[redacted]

COPY NO. 32

Navy Department - Office of Naval Research

[redacted]

NAVAL RESEARCH LABORATORY
Washington, D.C.

* * *

ELECTRONIC SPECIAL RESEARCH DIVISION -
SECURITY SYSTEMS SECTION

12 September 1946

FR-2972

CODING AND SECURITY OF ELECTRONIC RECOGNITION AND IDENTIFICATION SYSTEMS

by

C. E. Cleeton

[redacted]

- Report R-2972 -

[redacted]

[redacted]

Approved by:

C. E. Cleeton, Section Head
Security Systems Section

Dr. J. M. Miller - Superintendent,
Electronic Special Research Div.

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

Preliminary Pages..... a-c
Numbered Pages..... 20
Distribution List..... d

Problem Number S1234X-S

ADDRESS REPLY TO
DIRECTOR, NAVAL RESEARCH LABORATORY
WASHINGTON 20, D. C.
AND REFER TO:

[redacted]

NAVY DEPARTMENT
OFFICE OF RESEARCH AND INVENTIONS
NAVAL RESEARCH LABORATORY
WASHINGTON 20, D. C.

S-S67/89(1350)
S-1350-23/46
Ser. 6017
lb

SEP 27 1946

To: Chief of the Bureau of Ships.
Attn: Code 938(918).

Subj: NRL Report - Coding and Security of Electronic Recognition and Identification Systems - Forwarding of.

Encl: (HW)
(A) NRL Report R-2972 above subject by C. E. Cleeton dated 12 September ~~1946~~.

1. Subject report is forwarded herewith in connection with the studies being made under Problem S1234X-S.

By direction of the Director.

J. J. Bartko
Project Officer

Distribution:
BuShips 938(918) - #2 thru #6
ONR - #7
ONR, Boston - #8
CNO, Op-413 - #9
CNO, Op-20N - #10
BuAer, AER-EL-32 - #11
BuOrd, Re4 - #12
NEL - #13
SNLO, Ft. Monmouth - #14
OCSigO - #15
ESL - #16
AAF, AFDRE - #17
AMC, TSELC7 - #18
AMC, WIENA - #19
AMC, Cambridge Field Sta. - #20
ASA, Attn: Lt.Col. Leo Rosen - #21

Transmission by Registered Guard Mail or U. S. Registered mail is authorized in accordance with Article 76-15 [illegible]

Page 1 of 1 page.
Copy 15 of 25 copies.

Copies 32 + 33 of Report

ABSTRACT

The problem of coding an electronic recognition and identification system is analyzed. General principles and methods are discussed. The direction which future developments must follow in order to produce a practical coding system is indicated.

CONTENTS

INTRODUCTION

1. Much has been said concerning the coding of an IFF system. In many cases the treatment has been applied to a specific set of conditions or has been colored by political opinions. Very little of the thought which has been given the subject has been recorded in available reports. No attempt is made in this paper to sort out the historical developments, the purpose being to analyze the problem of coding of electronic recognition and identification systems and to state the pertinent facts which must be considered when the time comes to specify the coding of a future system. References are made to existing reports which give further details on methods and techniques. While it is realized that the ideal system is one that positively recognizes the enemy, no practical solution is known; therefore, since we must continue to recognize the enemy by subtracting the friends from the total until a better proposal is advanced, and since we will very likely in any case require a system for identification of friends, this paper is presented as a study of the subject of coding of a system to be carried by friendly craft for recognition and identification purposes. It is restricted to electronic systems of the same general character as have been widely used in the past and such techniques as use of absorbent materials[1], infra red, etc., which may be useful for special applications but which do not at this time show promise for the general solution, are not discussed.

CODING FUNCTIONS

2. A system of electronic recognition and identification, that is, a system applied to our own units (planes, missiles, ships, troops, etc.) to enable ourselves to determine the friendly character of such units and certain additional detailed information as may be desired, uses coding for the following functions:

(a) Security against enemy use.
(b) Detailed information concerning an individual unit or units.
(c) Improvements in the operation of the system.

Security Coding

3. It may be hoped to provide protection, by means of security coding, against

(a) Enemy use of the system to appear as a friend.
(b) Enemy use of the system to interrogate our units, thereby securing such information as

    (1) Recognition of our units.
    (2) Location of our units.

Ideally it is desired to be able to continue to use the system without fear of compromise even though the enemy has an amply supply of our equip-

ment and fully understands its operation. The ways in which an enemy could use the system to appear as a friend are:

(a) Equipping a complete unit to conduct an offensive operation deceiving us as to their real identity.
(b) Equipping isolated units to conduct intruder operations.
(c) Equipping their units to appear friendly in order to avoid offensive action by us.

Information Coding

4. Informational coding is considered here as including all coding which provides information concerning friends, other than his friendly nature. Ideally it is desirable to know the identity of each individual unit, his location, what he is doing, and his future plans. Such extensive information may well be impractical and much of it may be supplied by other systems. Particular items which have been associated with IFF systems of the past and appear to be of sufficient importance to consider in a future identification or special system are:

(a) Distress signal. Has been used on airborne IFF transpondors to call attention to an emergency condition of the plane.

(b) Personal identity. Used to isolate one craft of a group of friendlies for purpose of giving control vectors.

(c) Group or type designation. Used to distinguish between types of planes or ships, or to mark special missions or group arrangements.

(d) Reporting of tactical situation. Has been used by reconnaissance planes to report sighting of enemy craft.

(e) Identification of individual transpondors. Coding has been used to isolate particular beacons for homing purposes in connection with return of planes to their base, rendezvous of planes and ships, and dropping of troops and supplies.

It is possible to transmit position information concerning a moving craft and convert such information into the desired coordinates at the interrogation station. The altitude coordinate may be rather easily determined by the plane and converted into the angular coordinate of elevation, where needed, by less complex equipment than required for elevation scanning at the interrogator. Proposals for such features have been made in connection with navigational systems[2,3].

Coding for Improved Technical Operations

5. Coding has been used in the past for obtaining improved performance

of an IFF system. Examples are:

(a) Reduction of transpondor triggering due to noise and to other systems transmissions by use of a signal having special characteristics.

(b) Reduction of unwanted signals by recognizing a code for special functions and allowing only these wanted signals to appear.

(c) Channeling of various functions to increase the traffic capacity of a system.

Summary of Coding Functions

6. In summary, the functions which coding may be called upon to serve in an electronic recognition and identification system are:

(a) Security coding

(1) Against enemy use to appear as a friend.

i. For offensive operations.
ii. For intruder operations.
iii. To avoid our offensive action.

(2) Against enemy use to obtain information.

i. As a positive recognition system.
ii. Location of our units.

(b) Informational coding

(1) Distress signal.
(2) Personal identity.
(3) Group or type designation.
(4) Reporting of tactical situations.
(5) Identification of individual transpondors.
(6) Position data.

(c) Improvement in the technical operations

(1) Reduction of undesired transpondor triggering.
(2) Reduction of unwanted signals.
(3) Channeling.

CODING PRINCIPIES

7. All characteristics which may be changed, during the operational life of the system, in such a manner as to require corresponding changes in other portions of the system to enable it to operate, or which supply

different or additional information may be considered for coding purposes. The specification of the exact values of these characteristics is said to constitute the code. The code may be varied as required to suit the particular purpose. This section outlines those broad principles which control the coding system design.

System Characteristics Suitable for Coding

8. An electronic system may be coded by varying either the signal frequency or a modulation of this frequency. The particular means for doing this are well known and the detailed combinations are numerous[4]. It may be expected that the designer of any new system would give consideration to utilization of the following basic methods:

(a) Use of one or more signal frequencies which may be varied including simultaneous and interlaced channels.

(b) Use of continuous wave signal frequencies in which the type, degree or other characteristic of the modulation may be varied.

(c) Use of pulsed signal frequency whose characteristic may be varied including recurrence rate and pulse groups with pulse width, spacing, shape and arrangement critical.

Technical Requirements

9. In addition to meeting the operational requirements of security and supply of information, the method finally chosen for coding the system should meet the following technical requirements:

(a) Decoding should be completed in time to make sweep by sweep comparison with the radar signal, permitting electronic comparison with the radar information. (Benefits may be derived by delay of one or more sweeps in certain systems but this should apply only to particular installations).

(b) Traffic capacity should not be reduced. In fact consideration should be given to means of increasing the traffic capacity by coding.

(c) The coding should not interfere with proper operation or reduce the reliability of the system, nor should it require special consideration as to siting.

Master Codes

10. In many cases it is possible to cause the decoder to operate upon reception of codes which are different from the one nominally considered correct. In fact, it is often times possible to generate a "master code" which will operate the decoder in any of its conditions. Most coding

methods lend themselves to a choice between decoding which offers protection against use of a master code and decoding which does not offer this protection. In the first case, it is necessary to recognize the signal as the true code when it appears independent of certain other signals. In the second case, the code must appear only as a component of the signal. In addition to protection against use of a master code, the first method of decoding may be necessary in order to obtain the required number of informational codes in a minimum time interval; also, one may gain protection against some forms of enemy jamming and reduce unwanted triggering. On the other hand, it may be more susceptible to other forms of jamming and more complex. Also, in forms of coding which are time critical, multiple paths[5] may introduce additional signals which would interfere with proper operation. Similar trouble would be encountered by overlaping of signals from different sources[5].

False Code Radiation

11. The radiation of signals other than those specified as the true code may be used to confuse the enemy or to protect against compromise. The following facts must be considered in any decision regarding their use:

(a) Interrogation with false codes may be used to detect enemy transpondors using a master decoder but only if a method is provided for recognizing replies to the false code.

(b) Protection against enemy interrogation of our transpondors by not disclosing the true code to a monitoring system requires that all codes be treated equally as to duration, to time relations to other signals such as associated radars and to use with all interrogators. Also one must remember that the enemy can find the correct interrogation code by trying each possible code in succession until replies from one of our transpondors are obtained.

(c) Radiation of false reply codes to confuse an enemy monitor provides protection only if the enemy cannot use interrogators to induce the true reply.

(d) Radiation of false codes adds to the complexity of equipments, increases the average power requirement and adds to the general clutter of signals.

SELECTION OF CODING METHOD

In this section it is desired to examine the requirements imposed on the coding methods in carrying out the functions outlined in paragraph 6, and to bring out certain criteria for use in the selection of the coding method.

Security against enemy use to appear as a friend

12. It is required to deny the enemy use of transpondors, captured or fabricated, to reply to our interrogation. Real security comes only when such use is made so remote that we need never question the information furnished by the system. Such perfection may never be reached; therefore, we will examine to what extent the requirement may be met by various methods. In any coding method, security is obtained only by ability to change the code faster than the enemy intelligence can break it. His facilities in this respect are:[6]

(a) Captured or fabricated systems equipment to

(1) Monitor our interrogations.
(2) Induce responses from our transpondors.

(b) Special monitoring and measuring equipment to determine any or all characteristics of our signals.

(c) Other intelligence.

Items (a) and (b) above can be defeated only by a system design and operation which will make such efforts impractical. Item (c) falls into the same class as other information which must be kept from the enemy and it is assumed that appropriate security measures are carried out on advance information relating to coding, etc. The ratio of enemy effort to degree of compromise may be divided as indicated below starting with the smallest ratio and therefore the one which the enemy would be most likely to attempt. We should attempt to prevent such efforts in the order named. The effort required on our part to obtain this security is likewise indicated. The practical difficulties will require some compromise at the time a decision is made on the specifications of a new system even though theoretically we may operate at any level.

(a) Use of transpondors, captured or fabircated, at any time to appear as a friend being required only to be in good operating condition. Some systems of the past have dropped to this level when all coding for security purposes was eliminated. The simplest of security coding, if its use is enforced, will deny such use by the enemy.

(b) The enemy is required to determine the proper code setting at a time which may be in advance of his intended use of the transpondors. This level of security is the highest which has been used to date. Systems have been built which are technically capable of giving the maximum advantage in this respect by code changes which reduce the time between determination of the proper code and use of the quipment.

(c) The enemy is required to determine the proper code setting continually while using the transpondor. To force the enemy this degree of effort we must vary some characteristic of the system in such a manner as to set up new codes at intervals

short compared with the time of a single tactical operation. The control of the code variations must be through channels which are secure against enemy compromise to the extent that the future settings are not made available to the enemy before actual use.

(d) The enemy cannot under any circumstances use transpondors to appear as a friend. This represents the ideal in security and can be accomplished only by maintaining complete information on all friendly units such that other friendly units cannot appear in an area unidentified. This may appear fantastic but only in the extreme. Present practices go a long way in tracking, plotting, and assimilating information in large centers such as CIC. However, before a decision is made to expend great effort in perfecting such an organization to the extent indicated above, it must be considered that recognition of an enemy is the primary function, and that for this purpose detailed knowledge concerning friends is only indirectly applied to the solution of the problem and such effort might better be applied to a more direct approach,

Clearly, the effort which we must expend and the complexity of the system is increased by the degree of security desired. It is practical to go only as far as necessary in order to feel assured that our potential enemies will consider it impractical to attempt a compromise of the system. The answer to this question will, to a large extent, determine the complexity of the coding method to be used. As a concluding statement on this requirement, it may be said that security against enemy use to appear as a friend must be accomplished by varying a characteristic of the system (coding) at a rate faster than it is practical for enemy intelligence to follow or to use extensive operational procedures which in effect creates a surrounding wall within which all units are completely under control and across which no enemy can cross undetected.

Security against enemy use to obtain information

13. As a positive identification system for the enemy, he need only be able to interrogate our transpondors and receive a reply to take advantage of our system. It is interesting to note that while we must carry out a very great program of production and installation of a system before it can be of any use to us, the enemy can use it as a positive identification system as soon as he has one interrogator. Methods which may be applied to deny such enemy use are multiple interrogation frequencies, variable reply and interrogation frequencies and modulation of the interrogation frequency. In addition, reduction of transpondor range even to zero may be used to deny the enemy such use when the advantages gained outweigh those of having the transpondor operating for our own use. Such has been the practice in the past when flying over enemy territory. In any case such protection is important only if the enemy lacks a satisfactory system of his own and also it becomes increasingly less important as our superiority

increases to the point of his being able to recognize us merely by the numbers present.

14. Location of our units. Protection against location of our units by IFF is of use to the enemy only when we are concerned with keeping our location concealed which may be to prevent detection or to prevent collection of firing data. The first case may be associated with radio silence conditions which would likely require the system to be inoperative. In general it is the interrogation signal frequenc which must be transmitted in such a manner as to avoid interception, however under certain conditions it may be desirable to maintain "silence" of the transpondor transmitter. If radio silence is not imposed, thereby permitting him to obtain intercept information, it may be desirable to avoid giving him range information by our IFF system. The collection of information for fire control would require a planned and coordinated fire control system which the enemy would not be likely to provide based upon use of equipments which we would have to provide for him. Obviously such protection as is provided must be accomplished on the interrogation path. The same methods as enumerated in the above paragraph apply here. To be effective, master codes must not exist and the number of codes used must be very large to prevent breaking by simple trial and error procedures. In addition a coded transpondor delay could be used to protect against use of range data for firing. In these connections it is well to remember that due to the uncertainty connected with such use the enemy would undoubtedly be equipped with radar and intercept equipment.

Information Coding

15. Information coding may be produced by two general methods:

(a) Channelized method. This is used where there is interest only in a portion of the units and it is desirable to eliminate all others from the picture while this information is being collected. Functions which could benefit by this method are personal identity, group or type designation, and beacon identification.

(b) Non-channelized method. This method is used where it is desired to impress the information upon any active interrogation station. The distress function and report of tactical information may be better performed by this method.

Certain operational conditions may require a combination method. As an example, it may be desired to present a series of beacons channelized as a group but each beacon identified by a non-channelized code. It is obvious that the signal frequencies and interrogation modulation coding lend themselves to channelized coding in particular, while reply modulation coding is particularly applicable to non-channelized methods. Also, it may be noted that a non-channelized reply code is easily converted to a channelized code at individual responsors by proper decoding equipment.

The problem is primarily one of providing a sufficient quantity of information in an easily assimilated form without overloading or deteriorating the system in other respects.

Improvement to Technical Operation

16. Electronic systems have suffered from triggering by radiation from other sources such as ignition noise, radar and communication equipment (fundamental, harmonic and image frequencies). Also, interference is always experienced on non-triggering paths due to the usual sources. Such interference may be reduced to a large extent by coding methods which recognize a characteristic of the signal which does not exist in the interfering signals. Oftentimes coding for other purposes may provide this function. Attention to such detail as well as channeling out special functions may materially increase the traffic capacity of a system.

DEVICES AND TECHNIQUES

17. Numerous devices and techniques have been used or suggested[4,7] for coding IFF systems and no doubt additional ones will be developed. It is the purpose of this section to examine a number of the basic techniques, pointing out their advantages and disadvantages in order that their relative merits may be assessed.

Signal Frequency Coding

18. The signal frequency of a system may be made critical as in the majority of electronic systems or may be made non-critical as in the Mark III IFF system or wide band amplifiers may be used as transpondors such as "Peter"[8]. The former impose stability requirements such that unattended equipment will not drift out of the assigned channel under all expected operating conditions. Frequency-critical techniques are particularly suitable for channelized coding methods since the unwanted signals are removed by the receiver input circuits. However, a large number of discrete channels would not be expected due to the necessity of remaining within a definite allocated band and the requirement for considerable separation between channels as a result of frequency variations which must be accommodated and the large variations of signal strengths experienced in operating equipments at extreme range while at the same time operating nearby equipments. Also, in general, rapid code changes would require considerable increase in complexity of equipment. Non-frequency-critical systems provide channeling which serves to increase the traffic capacity, offers freedom in shifting away from interfering signals (deliberate or otherwise) and decreases the stability problem. However, in scanning systems, the counting down effect (IFF information not supplied as frequently as the radar information) may be objectionable.

19. Use of two or more interrogation frequencies either simultaneoulsy or in sequence has been considered[9,10,11] on various systems to provide security against unauthorized interrogations and for obtaining improved performance. Additional unlocking information may be transmitted on these

carriers such that various portions of the information must appear on a particular channel or channels and not appear on the other channels. The major objection to such systems has been the additional complexity introduced by adding more radio frequency components which in the past have contributed to our difficulties of design to no small extent. We may hope that some time in the future radio frequency techniques may be so highly developed that they may compete with video techniques on the basis of reliability and simplicity.

Pulse Patterns

20. Pulse patterns have been used not only for coding IFF systems but for radio control and synchronizing signals on communications equipment. Although the complete characteristic may be expressed as a relation between amplitude and time for one complete cycle, in which peculiar shapes may be used to vary the code, it is more practical to consider a number of individual characteristics which may be combined to form the code. Characteristics which are suitable are:

(a) Pulse width. Rather broad tolerances are required due to distortion by multiple paths and the electronic circuits which, with the increase in duty cycle for the wider pulses, restrict the number of discrete widths which are practical.

(b) Pulse number. The total number of pulses in a group may be used for forming critical codes.[9,12] Methods are available for counting such pulses electronically at very high rates. Although the duty cycle increases with the number of pulses, the individual pulses may all be held to a minimum in width with the result that several pulses may be used in the code. The chief difficulty is the error introduced by extra pulses produced by multiple paths and extraneous signals. In some applications, gating of the decoder has been used to reduce the time it is exposed to the extraneous signals.

(c) Pulse spacing. The space between a pair of pulses may be varied for coding or the pattern may be expanded to include a chain of pulses in which the spacing is uniform or non-uniform.

(d) Pulse amplitude. Signal strength variations make coding by amplitude less attractive. However, it may be practical to utilize the relative amplitudes of the pulses within a group of short duration.

In the generation and electronic decoding of pulse patterns, extensive use is made of delay lines, time constant circuits and coincidence circuits. In general, the first pulse of a group serves as a zero time reference and the decoding is performed by examining the signal at specific times following this pulse or by using it to initiate the generation of a local pattern against which the incoming pattern may be compared. Cathode ray displays are extensively used for visual reading of codes. This method

is primarily applicable to the reply path and where an operator is present. A common type of coding which has been used on radar beacons and is decoded visually is "range coding" where the number of pulses and their relative spacing make up the pattern.

Extended Patterns

21. The pattern of the individual groups may be varied in a sequence which in turn form the code. Such extended patterns cover several repetition periods which is its practical limitation since the antenna rotation rates must be decreased until the pattern can be generated during the sweep of the beam; in some cases, it is even necessary to searchlight in order to read the complete code. A simple form of this type of coding is a keying of some characteristic of the signal (frequently in Morse fashion) such as pulse widening, spacing variations or an on and off switching of a pulse. Characteristic symbols[13,14] may be generated by changing the composition of the groups in the proper manner. The symbol is then made up by the presentation of proper dots within a rectangular area where one side of the rectangle is measured along the range direction and the other side along the azimuth. The limitation of this type of code is the area taken up for its presentation. It becomes practical only when the pattern can be condensed, by use of short pulses and close spacings, until it is no longer objectionable. Reading of such a pattern will of course require some form of local expansion of the picture.

Interrogation Controlled Reply Coding

22. It has been proposed that a coding system be used which at any one time may have several proper interrogation codes each of which would produce a different reply code.[15,16] Such a system offers the following advantages:

(a) Security. An emeny monitoring our replies would receive several codes which would force him to also monitor the interrogation and properly associate the two codes. This could be made very difficult if we used several interrogation codes at all times. However, if he possessed an interrogation equipment he could readily produce a response from one of our transpondors and thereby learn the proper combination. To make such information less useful, there should be no simple relation between the interrogation and reply codes such as the sum of two numbers equal a constant, use of image patterns, etc., and also it should be made difficult for the enemy to obtain all combinations by a simple trial and error process. This means either a very large number of codes or frequent change of the combinations. This type of coding offers no additional protection against unauthorized interrogation since any number of interrogation codes would produce operation.

(b) Defruiting. Such a code system offers possibilities in

removing the reply signals produced by other interrogators, called "fruit", by the simple process of decoding the replies and displaying only those that correspond to the interrogation code in use. It would not remove fruit due to other interrogators in the area using the same code. However, by proper doctrine, a major increase in traffic capacity over an unde-fruited system might occur.

Code Changes

23. Change from one code to another should only be required for security purposes or when it is necessary to alter the information being transmitted. The latter needs little discussion as it is merely a question of operational requirements being fulfilled by appropriate switching devices. The change of security codes is more involved and, in fact, is the key for obtaining security. As pointed out in paragraph 12, security is achieved when the code is changed at such a rate that it is impractical for the enemy to attempt to compromise the system. Obviously the advantage which the enemy could derive by use of the system is enhanced by an increase in the length of time between obtaining knowledge of the code and his intended use and by reduction of the uncertainties which he may have concerning the proper code to use during the operation. If the code is varied continuously in a random fashion, the enemy would be forced to obtain his information at the time he was making use of the system. If he were attempting to appear as a friend and the coding was on the transpondor reply path, he must also have available a signal from one of our transpondors for monitoring purposes. The random cycle generator[17] by means of its extremely long cycle and large number of different cycles will accomplish such security. The code and cycle phase may be varied to protect against capture and the cycle variation forces the enemy to monitor at the time of use. Such devices are of less use for protection against unauthorized interrogation since he could interrogate with the possible codes in succession or employ a master code (unless protected against) to induce replies and thereby obtain the desired information. While the continual changing between a few reply codes provides considerable security against enemy use of transpondors to appear as a friend, to obtain security against unauthorized interrogation a large number of individual codes are required such that the enemy will find it impractical to use trial and error methods.

SYSTEM SECURITY

24. The discussion of factors which must be considered in the choice of coding for security is incomplete without a consideration of other possible means for obtaining security. Complete security of an IFF system implies that.

(a) The enemy cannot interfere with our use of the system and

(b) The enemy cannot use our system to his advantage.

SECRET

The former include such things as jamming, producing false information, etc., which in effect serves to decrease the efficiency of our system rather than to compromise it. While this may be serious, it is more a system design problem than a security coding problem. On the other hand, prevention of enemy use of the system may depend solely upon the coding. The only other approach is that of preventing him from obtaining equipments, captured or fabricated, which he may use. Efforts which we might make in this direction are:

(a) Secrecy of System. This has been practiced to a certain extent in the past. The intention is to make it impossible for the enemy to fabricate equipment due to his lack of knowledge of what to build or how to build it. The results are that many of our own people are denied the information which is necessary for proper operation and use of the system, thereby lowering its efficiency. Even if such security were practiced, it would be undone should equipment be captured, assuming that he could understand the operation and apply it to his planes. This assumption is the only safe one as scientific advances in principles and techniques have never been the property of one nation only, and we may expect others to make these discoveries in about the same way we do. The system might be compromised by the time our forces had become sufficiently familiar with it to be of real operational use.

(b) Use of Destructors. Destructors have been used to destroy portions of equipment when planes crash over enemy territory. They serve to reduce the number of equipments which the enemy may accumulate for his use by capture. Destructors which have been used have not succeeded in destroying the equipments to the extent that knowledge of their characteristics cannot be determined from a few samples, but rather serve to render the equipment unusable without extensive repairs. It is doubtful that much more than this can be accomplished when used with piloted craft because of the necessity of confining the destruction to avoid serious injury to personnel. In any case, sooner or later an equipment is likely to fall into enemy hands due to forcing a plane down over enemy territory without destruction, failure of firing circuit, etc. We may therefore conclude that destructors serve only to make the problem more difficult for the enemy and offers no guarantee of security for any specific time.

25. We are forced to the conclusion that lasting security cannot be accomplished by attempting to keep knowledge of our system and equipment a secret from the enemy. However, should there be no satisfactory security coding solution at the time it becomes necessary to determine the specification of a new IFF system, it will be necessary to weigh the partial coding solution against the other means for obtaining security for a limited time. Therefore, it is in order to discuss such possibilities. We may start with a system in use or available for use at the time. If we assume

that the system is compromised due to other nations having knowledge of its characteristics and possibly even having equipment, we may ask to what extent the system must be changed in order that it is no longer compromised. We are likely to be misled by the argument that a change which requires a long time for us to carry out would likewise be difficult for the enemy to carry out, thereby giving security over a considerable period of time. The fallacy lies in the fact that we must carry out the change on a large scale which may require a long period of time in production and installation after it is developed in the laboratory, making these changes on a large number of equipments - possibly both transpondors and interrogators, while the enemy can modify a few transpondors only, in the laboratory, use them to appear as friends and thereby shake our confidence in the system to the extent that we can never feel sure in any particular instance that the enemy is not deceiving us. We therefore must take steps to protect ourselves against what, in the majority of cases, will turn out to be friends.

26. As pointed out above, it would be relatively easy for the enemy to modify existing equipment of similar characteristics and compromise our IFF system by using a few such equipments to appear as a friend. If the enemy has compromised a system he has equipments which may serve as his models for modification. A mere modification of the equipment such as a frequency shift would hardly be worth the effort. To gain security we must either make an extensive system change - a new system which gives only limited security as discussed in the paragraph above, or we must make a modification which will enable us to retain our security by coding methods. Our conclusion is that the security of a system by its novelty is short compared to the reasonable life of a system of such magnitude and that security can be obtained only by coding properly designed into the system, other modifications or changes of a system being made only when they are warranted by increased operational and technical performance.

DOCTRINE

27. The doctrine which is practiced may materially affect the security of the system. The reduction of range or switching off of transpondors when over enemy territory to avoid enemy use of our transpondors for positive identification or as a means for extending his detection range has already been mentioned.

28. The frequent change of code by manual means will largely protect against compromise by capture. However, such changes are difficult to carry out on a large scale due to the great number of individuals who have to be informed and carry out the instructions at specific times. It is obvious that the more frequent the changes, the greater the burden on the personnel. Such changes have been very infrequent in the past. No one can say how frequent they would be made in the future. This will depend upon such things as the ease with which coding information could be disseminated, the effort required in terms of interference with other duties, the efficiency with which such changes are carried out, and the apparent necessity for change to protect against compromise. The question of code

changes while planes are in flight can be resolved either by recognizing an "old" and a "new" code during a certain period of overlap, or by equipment design which will permit easy change, while in flight, between two codes previously selected.

29. Most any system which may be devised lends itself to use of a single security code at any given time over all areas or use of several codes distributed by area, function, or other plan. Previous systems have operated by both methods. The former method of use offers simplicity while the latter may provide additional security or additional information. Should our system be one which was secure except for enemy monitoring at the time of his intended use, we could gain considerable security by use of a different code for a number of geographical areas. For example, the enemy might desire to launch a surprise attack against a base where he was not assured of being in range of our transponders to provide the code to his monitor. He could obtain the necessary information and relay it from some other locality where activity was assured, and possibly even so disposed that he could monitor from the ground where greater facilities were available, if the same code were used in the two areas. In other cases compromise by capture may be more probable in one area than another and therefore it would be advantageous to use different codes. When the areas are widely separated, such as the European and Pacific areas during the past war, there is little difficulty with overlap but when the areas become much smaller and closer together, the problem of one craft going from one area to another, and the problem of the interrogator covering more than one area give rise to operational difficulties. Such problems may be solved by recognizing codes of adjacent areas so assigned as to be equivalent for decoding when the areas are in close proximity but to vary outside the decoder limits in a random manner for the more remote areas. One might imagine a system in which the code varied with latitude and/or longitude in much the same manner as the random cycle generator varies the code with time. The information for code change might be supplied by some natural phenomenon or by highly developed navigational aids.

GENERAL SUMMARY OF PROBLEM

30. This section summarizes the coding requirements and furnishes an outline which may be used as a guide in the technical development of coding methods and devices.

Primary Requirement

31. In any system for electronic recognition, the primary function of coding is the recognition of the enemy (direct or by elimination of friends) with assurance that he cannot deceive us by appearing as a friend. It must be assumed that (except possibly for short initial periods) the enemy will have at his disposal complete equipment and technical information concerning the system. The solution of the problem is one of changing the codes in a random manner at a rate which makes it impractical for the enemy to attempt breaking them. Prevention of compromise must for the complete solution cover the general cases of:

(a) Approach of enemy units in independent formations on offensive missions.

(b) Approach of enemy units associated with our units in intruder operations.

(c) Defensive uses by the enemy to avoid attack.

It is not essential that a single method be applicable to all cases. Coding on the reply path is to be preferred in that enemy monitoring requires the presence of our transpondors which may or may not be present during his attack while our interrogators must furnish him signals by the very nature of such a system, and also since interrogation coding requires radiation of false codes and display of their responses in order to guard against a master decoder.

Secondary Security Requirement

32. The preventions of unauthorized interrogation is of secondary importance to security against use to appear as a friend since, should the system be compromised to the extent that we were unable to recognize the enemy, discontinuance of use of the system for secure recognition would follow, defeating the enemy's use to

(a) Positively identify our units.

(b) Detect our units without use of radar.

With the exception of reply signal-frequency variations, such protection must be provided on the interrogation path and sufficient number of codes must be supplied to avoid breaking by simple trial and error methods.

Non-Security Codes

33. Should operational requirements dictate that in addition to the function of recognition, the system should also perform other functions of the nature of transmitting specific information, additional coding will be required to the extent of the number of messages which the system must handle. Security of such messages may be contained in their translation. The requirement will be merely to provide for the expressed needs to the extent that it is practical when complication of the equipments and possible interference with performance of the recognition system are considered. Items of information which have been transmitted by other systems and illustrate the type of information involved are:

(a) Distress Signal.

(b) Personal Identity.

(c) Group or type designation.

(d) Reporting of tactical situations.

[redacted]

(e) Identifications of individual transpondors.

In general, the problem will be one of compressing more and more information into shorter and shorter intervals. Channeling by interrogation and/or response frequencies and interrogation coding serves to increase the overall traffic and is desirable for many functions.

CONCLUSIONS

34. Definite conclusions which give the answer to the problem of security and coding for electronic recognition and identification systems can be formed only when operational requirements are established, which requirements are closely related to many problems of future warfare, and which are a matter of opinion and judgment rather than fact. Tentative practical requirements will therefore change as additional information becomes available and progress is made in techniques. The ideal is clear but its practical accomplishment is remote. Undoubtedly there must be a compromise agreement when specifications are fixed. In spite of this uncertainty there are sufficient facts upon which to base a program and which may serve as a working guide. These facts are:

(a) The ideal IFF system should at all times recognize the enemy, supply operational information as required, and should not permit the enemy to obtain information by means of the system.

(b) High degree of security can be assured only by cryptographic coding methods.

(c) The high cost of production, installation and training associated with equipment modification compared to the limited security accomplished by such changes make such methods for obtaining security of questionable value.

(d) Complexity of equipment increases with the amount of security and information desired. There is a limit to the complexity which is practical; therefore, development of new techniques which simplify the devices, reduce their size and weight, and improve their reliability will materially aid in the practical accomplishment of increased security and capacity for handling information.

(e) In order to keep pace with improved weapons, coding methods and devices will be required to supply more and more information in shorter and shorter times.

RECOMMENDATIONS FOR RESEARCH AND DEVELOPMENT

35. Effort on coding techniques and devices should be toward accomplishment of the following objectives with the importance approximately as listed:

(a) Automatic means for carrying out code changes at a rate fast compared to possible breaking by the enemy.

(b) Determination of a suitable characteristic to be coded which is capable of rapid variation together with the necessary development of techniques and devices to enable this process to be carried out reliably and with a minimum of complication.

(c) Means for transmitting a large number of messages in such a manner as to feed information to the necessary centers as rapidly as the radar information is received.

(d) Development of simple devices for generating and decoding compact pulse patterns.

ACKNOWLEDGMENT

It is desired to express appreciation to present and former associates with whom the problems of security and coding of IFF systems have often been discussed and in particular to Mr. C. V. Parker for many valuable suggestions and clarification of topics in this paper as a result of their discussion during its preparation.

REFERENCES

1. Radiation Laboratory Report S-10, "Detection of Propeller and Sambo Modulations", by James L. Lawson, Editor, dated May 16, 1944.

2. Federal Telephone and Radio Corporation proposal 233 "Universal Communication, Airport Control, Traffic Control, and Aerial Navigation System".

3. Hazeltine Electronics Corporation Report CB-348-A "Lanac, Air and Marine Navigation".

4. CRG Technical Memorandum 3 and 3A "Partial Outline of Coding Elements" by H. M. Brown dated 12-5-42 and 1-11-43.

5. CRG Technical Memorandum 50 "Some Possible Defects in the Coding System Outlined in CA/R/RI 8/3" by R. H. Brown dated 12-14-43.

6. CRG Technical Memorandum 44 "Monitoring the Fast Codes" by H. M. Brown dated 11-22-43.

7. CRG Technical Memorandum 4 "Suggestions on Coding" by H. M. Brown dated 12-7-42.

8. OSRD Div. 15 Report 931-25 "Project Peter" by Siegfried Hansen dated November 16, 1945.

9. NRL ltr S-S67/33, Serial 111 of 17 January 1939 to BuEng. "Pulse System of Recognition, Special Progress Report on".

10. T.R.E. Report L/10, "Proposed Policy for Responder Beacons" dated 26 April 1942.

11. CRG Technical Memorandum 10 "IFF System with Simultaneous Two-Frequency Interrogation" by E. A. Jackson dated 12-16-42.

12. NRL Report R-1794 "Ship to Ship Pulse Recognition System" by E. H. Krause and M. W. Rosen dated 10-24-41.

13. CRG Tech. Memorandum 14 "Summary of Discussions on Type of Display" by H. M. Brown dated 15 January 1943.

14. Memorandum for file "A Proposed Method for Generating and Displaying IFF Code Letters" by L. W. Peay and C. C. LeGrand dated 18 January 1946, NRL report in preparation.

15. Bell Telephone Laboratories Technical Memorandum "Considerations of the IFF Problem in the Navy's Integrated Fire Control Program - Case 25653" by S. C. Hight dated December 21, 1945.

REFERENCES (Cont'd.)

16. "Proposed Operational Characteristics for a New IFF System" by Comdr. A. D. Hart, Enclosure B of BuOrd ltr to CNO of 22 March 1946.

17. NRL ltr report S-F42-6(1350), S-1350-8/46 Serial 5804 "Non-Recurring Mechanical Cycle Coding - Summary Report on" by Charles H. Doersam dated 14 March 1946.

DISTRIBUTION

5 Chief of the Bureau of Ships, Navy Department, Washington 25, D. C. Attention: Code 938(918).

1 Office of Naval Research, Navy Department, Washington 25, D. C.

1 Commanding Officer, Office of Naval Research, Branch Office, 150 Causeway Street, Boston 14, Mass. Attention: Comdr. R. W. Hart.

1 Chief of Naval Operations, Navy Department, Washington 25, D. C. Attention: Op-413.

1 Chief of Naval Operations, Navy Department, Washington 25, D. C. Attention: Op-20N.

1 Chief of the Bureau of Aeronautics, Navy Department, Washington 25, D. C. Attention: AER-EL-32.

1 Chief of the Bureau of Ordnance, Navy Department, Washington 25, D. C. Attention: Re4.

1 Naval Electronics Laboratory, Point Loma, San Diego 25, California.

1 Senior Navy Liaison Officer, USN Electronics Liaison Office, Fort Monmouth, New Jersey.

1 Office of the Chief Signal Officer, Chief, E & T Service, Pentagon Building, Washington 25, D. C.

1 Commanding Officer, Signal Corps Engineering Laboratory, Bradley Beach, New Jersey. Attention: Director Evans Signal Laboratory for Mr. Stokes.

1 Commanding General, Army Air Forces, AC/AS-4, Research & Engineering Division, Washington 25, D. C. Attention: AFDRE-2F, Mr. Harry Mulkey, 5D926 Pentagon Building.

1 Commanding General, Air Materiel Command, Aircraft Radiation Laboratory, Engineering Division, Wright Field, Dayton, Ohio. Attention: Code TSELC7.

1 Commanding Officer, Watson Laboratory, AMC, Red Bank, New Jersey. Attention: Code WLENA.

1 Commanding General, AMC, Cambridge Field Station, 230 Albany Street, Cambridge, Mass. Attention: Dr. O'Day.

1 Director of Intelligence, War Department General Staff, Washington 25, D. C. Attention: Lt. Col. Leo Rosen, Army Security Agency.

[redacted]