F'U' Ciphony

Jay

Mr Scott RAF
Mr Werfund

~~SECRET~~

EXTRACTS FROM RESEARCH & DEVELOPMENT PROGRESS REPORT - JANUARY 1947 ADMIRALITY SIGNAL ESTABLISHMENT

1. It has been found for example that to give communication during 60% of the 24 hours only medium powers are required. For the full 24 hours, however, the powers necessary increase rapidly. Again the present Naval requirements are for telephony and automatic telegraphy, both of which require much higher powers than does the existing form of hand operated morse signalling. It seems probable from the results of analysis made so far that powers of about 5 KW (radiated) may be needed to satisfy the requirements completely. It is the opinion of many of the Staff that the requirements in the future can best be met by a series of equipments operating within the frequency range 100 - 800 MC/s. One of the ruling factors in new designs is that the ability to work with the Americans must be provided, and a mission has been to the USA to establish a common technical foundation on which the future may be built. The report of this mission which is now returned will shortly be available.

AUTOMATIC TELEGRAPHY

For reasons of propogation, long distance automatic telegraphy working must be carried on in the part of the high frequency communication band lying between four and twenty-one megacycles. The congestion in this band is such that the maximum use must be made of each frequency allocation. This can best be done by employing the highest degree of frequency stability that the present state of development will permit, and by using high keying speeds or multi-channelling, high speeds and suitable for direct printing because of the mechanical characteristics of printing apparatus. Multi-channelling is, how-

~~SECRET~~

2.1

ever, quite practicable and will be considered in some detail. We speak of multi-channel time division and multi-channel frequency division. This five unit code is with minor variations in use as a standard teleprinted code in the USA, Great Britian and most Continental Countries and at the Bermuta Telecommunications Conference in November 1945 the five unit code with start-stop synchronizing was recommended as the World's Standard Teleprinted Code for Radio and Land Line Working. For these reasons it would be very difficult to produce an argument for any other teleprinted code, but there is little doubt that if a free choice of code could be made today, the six unit code would be adopted in preference to the five or seven unit. Using a six unit code 63 basic combinations will result (6 spaces are not used as a combination). Also for certain kinds of traffic such as stock market reports and the like where letters and numerals are mixed the speed of this code may actually be faster (that is requiring a narrow bandwidth for a given speed of signalling than the normal five unit code). Now a seven unit code is introduced because of its so called error detecting properties. Error detection finds its chief value in coded or ciphered messages where it might be expected to reduce the number of corrupt groups that would otherwise have to wait for decoding or deciphering before a repitition could be requested. The error rate on the better class radio teleprinted networks is frequently less than one error in ten thousand characters, and the value of error detection under these conditions is doubtful. For minor circuits where it is found impossible to obtain a lower rate an error detecting code would be of advantage but would involve the use of code converters for the exchange of traffic with other routes. The admirality in common with all other services is committed for the next five years to the start-stop synchronizing arrangements on its main track routes and this system is quite suitable for normal book ciphering arrangements. Recently, however, many advances have been made in machine or on-line ciphering which opens up possibilities of rapid transmission of secret information by simply feeding plain language tape into a ciphering machine which delivers a ciphered tape ready for transmission. The converse operation being performed at the receiving end. It will be seen at once that this system fits in admirably with the tape relay system but unfortunately start stop synchronism cannot be used because of the danger of mischaracters, which altho of no particular consequence in book cipher might with on-line ciphering make all the information after the lost character completely indecipherable. Where either of the synchronizing arrangements other than the start stop are used although the character itself may be lost its position in time is noted by the receiving apparatus and it is this that the ciphering machine requires to know to enable the coding to be changed. A possible compromise would be to send the start stop code synchronously in which case the advantage of synchronous working could be combined with the flexibility of the start stop system for the slight disadvantage of a slower code than is absolutely necessary. As for the teleprinter proper it seems to have before it a very great future, the ease with which a message in letter form may be transmitted and received and the facility with which copies may be taken make it the ideal form of communication wherever a record is required. In its essentials it is merely an extension of printing which has been with us for almost six hundred years. Altho this article has been given the broad heading of Automatic Telegraphy no mention has been made of the alternatives to the teleprinter, mainly the hellscriber and the various facsimile systems. These have been deliberately ignored because it is felt that while they may have a very extensive tactical application in the future they are not well suited for long distance telegraphing signalling on account of the relatively high baud rate required.

SPEECH SECRECY SYSTEMS

The fact remains, however, that the original speech elements themselves must be transmitted in some form and they may be capable of being extracted from the scramble without previous knowledge of the code. In all interception of scramble or partially scrambled speech the training and experience of the interceptors are of the greatest importance. A practiced operator can often extract some sensefrom the elements of the transmitted speech, altho to a casual listener the signal appears to be a completely unintelligible noise. An assessment of the security of any speech scrambling system is a very difficult process and without making a number of qualifying statements it is usually quite impossible to estimate how long an interceptor will take to obtain a knowledge of the contents of scrambled messages. The most pessimistic estimate is obtained by assuming (1) that the enemy can receive messages either directly or by relay at Interception Stations provided with recording equipment associated with all known cracking devices. (2) Spare no expense in material and man power to perfect these stations. (3) Captured appropriate receiving equipment or that information from intelligence sources has allowed him to construct it. Under these conditions only the system which makes use of a number of difficult codes or which uses a non-repeating code can give any useful security and the system must of course be proof against the possibility of extracting the sense of the speech by partial descrambling without the use of the proper code. Scrambling equipment under these conditions and given a security period of at least some hours can certainly be built but its bulk would probably preclude its use in ships except for a few important radio circuits. For traffic of immediate operational importance there is use for a scrambling system of a security time of upwards of 15 minutes and this appears to be within reach with moderately compact equipment which might for example be carried in an aircraft. The average security can be increased by the common methods of saturating the enemy's interception station with dummy traffic. If it can be assumed that the enemy will not use his resources to deal with all such traffic the average security may be much better. There will always be a risk, however, that he may be fortunate in quickly determining part of a code. They speak of inversion and the use of the "secret telephone". In this sytem the range of frequencies say 250 to 2500 cycles is reversed so that 250 cycles becomes 2500, 300 becomes 2450, 350 becomes 2400, etc. This system gives no security at all on the radio link, as it is only necessary for an eavesdropper to set his receiver hetrodyne to 2750 cycles to reinvert one of the side bands which then gives clear speech to a mask by the hetrodyne whistle and the other side band. The whistle may be reduced by filtering. In the same class with inversion sometimes combined with it is the process of shifting all the speech frequencies up or down by constant amount. This process again offers no real security, altho plain inversion and frequency shift gives more measurable security than when used alone. Both methods conform equal parts of other more elaborate systems. For example both inversions in band shifts form parts of split band shifts discussed below and with the addition of a time variation to the frequency shift on the basis of German devices developed at the Feuerstein Laboratories. The next systems of importance to be considered are those which employ band splitting and scrambling as exemplified by the GPO modulator 2C developed for Naval use in speech control outfits, and from what has been said about it it will be clear that the long time security of the 2C is negligible. An example of more complicated band scramblers are to be found in the Bell Telephone A1A2 and A3 equipments used on the London New York Circuits at various dates. If these systems beside the large number of alternatives of automatic switching is provided to switch periodically from one condition to another in a coded sequence which again is periodically changed. As a primary switching code allows for 20 seconds on each condition interception can be effected if the intercepter keeps separate equipment set up, etc.

TIME DIVISION SCRAMBLING

The best known examples of this method of scrambling are the Western Electric TDS machines of which model PF may be taken as typical. In this system the original speech is broken up into successive elements on a time basis instead of into frequency band. The duration of each of these time elements is approximately 40 mil. seconds and the scrambling consists in rearranging the order in which they are transmitted. In the PF machine 20 such elements form a cycle in the code used beside the order of the rearrangement of these 20 elements. In the method of time switching employed is the double series of 732 codes available, giving about a half million possible codes, changeable by means of punch cards supplied by the machine. The security of the system is not classed as high as that of the modulated 2C. It is possible from a recorded message and appropriate equipment to discover the code used and subsequently scramble the message and any further ones made with the same code. More recently Western Electric have designed an attachment to the PF equipment to provide continuous code changing over a long secondary cycle. It is no doubt that this considerably increases the security and will result in greatly increasing the time in scrambling and require the continuous use of the enemies decoding recourses. These methods of scrambling are exemplified in the modulated type 90 now being developed by the G P & O on an air administered contract for common use of the services. This system is a combination of band scrambling and TDS and if the speech is first divided on a frequency basis into three bands which are then transposed with or without inversion according to a code which changes five times in one cycle of operations and then repeats. The resulting 15 speech elements comprising one cycle are then scrambled on a time basis so that in the final scramble any one of the original elements can occupy any one of the 15 positions, three in frequency and five in time beside possibly being inverted in frequency. The security of this system could be classed as moderate. The time required to determine the code for recorded sample has been estimated at 3 to 4 hours to maintain reasonable security. The possibilities of the vocoding in a speech secrecy system are well known in the U. S. where the vocoder originated. Post war interrogations have shown that the Germans were all so fully aware of its advantages but they had not completed development of their system at the end of hostility. In this country the GPO have undertaken the development of an experimental equipment which may also fulfill a requirement for the war office. For the pulse type radio teletype; presumably similar to our pulse code modulation equipment.