~~SECRET~~

COPY

FROM: HELSINKI (JMA)
TO: TOKYO (SUMMER)
#042 (Seven parts)
January 18, 1943

(Translated (B.) Jan.30,1943)

Recently all countries have been devoting great energy to cryptanalysis, and they have made remarkable progress. For instance, Finland is now reading Russian, American, and Turkish codes, and now they are starting on the French. Moreover, to judge by what Lt. Col. HARAMA says ("it is not impossible to read machine ciphers"), we may expect that they are also reading the Swedish and German codes.

In view of these facts it seems necessary to take the utmost precautions to preserve the security of our present codes and therefore for your information I give you my opinions regarding the military attache's code now in use.

1. Every country is collecting great quantities of dispatches for cryptanalysis. The number of our dispatches that Germany or England accumulates in one day must amount to 40 or 50 (SU JU). In considering the additive book, over a long period of time the dispatches using the same additive must also amount to a considerable number.

2. Every country, having confidence in its own security, believes that as a matter of common sense its own code messages cannot be read, but the natural phenomena of code operation or errors give an entry into breaking the code. By studying a number of copies of dispatches sent and received by this attache's office the position of the serial numbers and the keys can be ascertained and if the research is pushed further we cannot be confident that the system of the primary code could not be conjectured.

3. Each country, using much time and personnel, first carries out all kinds of statistical analysis, then, by comparison with previous systems, progressively reaches the result of reading the code in present use. Therefore for the security of the present code it is necessary to consider its relation to the former system.

4. Judging by the experience of the decipherment of the Russian code we may suppose there is a possibility that identical additives were used in Finland. This kind of composite decipherment (is not difficult?). In view of this situation, if identical

COPY

~~SECRET~~

~~SECRET~~

additives are used in different places it will be necessary for the basic code to have a high degree of security, and it will be necessary to change the indicators and position of the keys from time to time.

5. There is much duplication in Navy Department announcements and in DOMEI dispatches of material which is contained in the dispatches from the attache in (Lisbon?). It must be considered that this gives much material for contrast and analysis to the enemy.

6. There is no doubt as to the high degree of security of our present code and I believe Staff Headquarters are studying how to preserve its security. Moreover, as I suppose that is hazardous to instruct the higher authorities, I will cut this short, but once more I would like to ask that you exercise the utmost precaution and study analytically our messages sent and received.