ALLIED FORCE HEADQUARTERS
OFFICE OF THE CHIEF SIGNAL OFFICER
APO 512, U. S. ARMY

X419

TO: Chief Signal Officer, War Department, Washington 25, D. C.
Attn: SPSIS

SUBJECT: Fixed Call Signs.

Included herewith for your information is a copy of memorandum on fixed call signs prepared by a member of the local YNA committee.

For the Chief Signal Officer:

R. E. SCHUCRAFT
Lt Col, Sig C

1 Incl:
Memo dtd 13 Apr 44, file B.39/753/6

Declassified and approved for release by NSA on 01-26-2015 pursuant to E.O. 13526
A copy of Sigma 9 telegram No 85270 dated 8 April has been circulated to this section with regard to REDACT Manual of Signal Security.

Appendix B, which I submitted to X Branch, is characterised as an "Attack on Far Office policy governing major circuits". It seems that I should therefore put on record its origin and reasons.

The original REDACT Manual of Signal Security which is described as "excellent" in para 4 of telegram 85270 contains similar words at the beginning of the paragraph on fixed call signs (cf. chapter III para 9 "the system of allotting fixed call signs to certain long range stations is inherently insecure") as the equivalent para in the printed for 19% edition (chapter III para 9 'the system of allotting fixed call signs to certain static \# stations working between and within commands in inherently insecure').

During the visit by the 3 0 in 0 to our station at REMICELI, I mentioned the difficulty we are experiencing in recasting by traffic analysis diagrams of GORDA networks and of sorting traffic, owing to the fact that the O.O. L. use changing call signs for all their stations whether static or mobile, and constantly make changes devised to hinder the task of our interception service. I expressed the opinion that our methods seemed to be deteriorating since previously the use of fixed call signs was restricted to the "FAST MAIN between commands and theatres. and not their use had been expanded to fixed stations.

I was subsequently asked to redraft para 5 of chapter III since the reasons justifying the statement that the system was "inherently insecure" were felt to be indifferently expressed. This I did and para 5 was altered and the Appendix B was added.

Chapter I para 4 of the Manual contains the following: "a distinction has been made between the procedures into which "will be adhered to, and that which should be aimed at if circumstances permit in order to obtain as great a degree as possible". If despite this, the repetition of the statement in the revised edition that the "system is inherently insecure" is regarded as an "attack on Far Office policy governing major circuits" would it not be fair to suggest that the first duplicated edition which referred to "certain long range stations" contained the attack rather than the subsequent printed edition where the phraseology was changed to "working between and within commands".

The Y intercommunication network has been directly affected by this expansion in the use of fixed call signs. Then the necessity for 4 links between NET stations was first experienced, charging call signs were allotted; now all our main stations including remote NET stations use fixed call signs. The size and activity of our Y strategical network is thus laid bare to the enemy.
8. For the reasons given in para 7, and because I am convinced that it is my obligation to call attention to any apparent failure in our methods as compared with those adopted by the enemy, of which I become aware, I hope the question will be further considered.

9. I see that para 1 of SME 9 states that the K& arguments with reference to fixed callsigns are ungrounded. I have not had an opportunity of seeing the detailed reply to which reference is made.

10. The planning of para 5 and of Appendix B were not intended to be arguments, but reasons for the statement that the "system is inherently insecure" and to encourage consideration of how far our signal security could be improved without prejudicing practical and speedy traffic disposal.

11. **REMARKS ALIEN CODES**

I understand that our present Army system of call-sign allotment is

(1) all fixed stations, above the level of Army By, are allotted fixed four letter calligns. They use double calligns occasionally, then clearly showing the originating and receiving stations.

Taxes such as Algiers, Constantine, Philipwville (there are about thirty such allotments in E.A. and seventeen in Italy) are given a fixed callign and any NT station operating in that area uses that callign, unless they have a special callign which may them be used as a callign eg. BG. In addition certain Bks or other units may be used. At 0 in 0 000 AD MAP, GB, and Rhodes are given delivery groups composed of the same two letter letters. Those may appear in the preamble. Operational reserve units such as Corps Bks, Div Bks and units within a Division, AA units, that have, although geographically behind Army N4, are allotted calligns (changing daily).

(11) all calligns allotted to stations in a particular command or theatre start with the same two letters, and are easily distinguishable from those of other commands.

E.g.  

<table>
<thead>
<tr>
<th>Callign</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>JA</td>
<td>UK</td>
</tr>
<tr>
<td>JB</td>
<td>America in UK</td>
</tr>
<tr>
<td>JU</td>
<td>MDEHAT</td>
</tr>
<tr>
<td>JD</td>
<td>NORTH AFRICA</td>
</tr>
<tr>
<td>JJ</td>
<td>ITALY</td>
</tr>
<tr>
<td>JP</td>
<td>Persia</td>
</tr>
<tr>
<td>JG</td>
<td>India</td>
</tr>
</tbody>
</table>

(ii) operational units are allotted daily changing calligns, letters only (except for fig affixes below in level).

12. **R.A.F.** uses fixed calligns, allotted to their Bks and aerodromes. These do not change when one unit on an aerodrome replaces another.

When an advance to an place, and new aerodromes are opened, new calligns are allotted. When an aerodrome ceases to be used callign lapses.

I am told that the NS and NN calligns can generally be distinguished; the former are composed of letters, the latter of figures. The ground to air calligns are not under discussion.

13. **REMARKS GERMAN CODE**

(1) All stations with few exceptions, use daily changing calligns composed of mixed figures and letters. They are usually used as link and not double calligns.
Δε γεννά 

Προσεχτικά, το 1/3 της παραγράφου είναι κομματισμένο και δεν έχει μονογραμμάτιστη εστίαση. Ανυπολογιστικά, ο μεγαλύτερος μέρος της παραγράφου μειώνεται σε 1/3 της εκλειπόντως κεκομισμένης παραγράφου. Αυτό προκαλεί σημαντικά δυσλειτουργίες στην απόδοση της μηχανής και καθιστά δυσκόλα την αναγνώριση της επικεφαλίδας και των λεπτομερείων.
enable them to estimate concentrations and observe moves.

Any change in the "codesign - fixed callsign junction point" of the above will assist, and also probably reveal changes of subordination. The number of messages that require retransmission between a Corps or Div I., in reserve and during repositioning, to higher formation H.Q. is probably higher than when operationally employed.

19. The use of fixed callsigns for ports, railheads, important towns, Districts and billeting areas will tend to give similar information in view of the inevitable changes in the volume of traffic, consequent on concentrations or departures.

The allotment of additional fixed callsigns to towns or other stations, and the lapsing into silence and non-use of others will also provide information of infiltration and increased or decreased concentrations. The existence of BRITISH AT stations in TURKEY was mentioned by an ITALIAN cryptographer and was probably disclosed by the use of JU callsigns of new stations communicating with UAFFRO (JGFO).

The GERMAN police used to use fixed callsigns. In 1941, the GERMAN infiltration into ROUMANIA was spotted as a result of this, and caused search to be made for Army stations using changing callsigns in that area. Owing to the inaccuracy of T/F and the difficulty of the callsign procedure, this search was not conclusive but confirmatory.

We are aware from captured documents that GERMAN intercept stations render a daily return of formations or units subordinated to senior formations. This assists their records of our order of battle. Our callsign system facilitates this.

There are probably other compromises of direct military value, based on the background knowledge acquired by persistent interception and traffic analysis.

20. Chapter III para 5 sub-para (b) "It provides aids to enemy cryptographic attack on cipher traffic".

There can be no doubt that the enemy has a large cryptographic organization. Unless our high grade machines and book ciphers are absolutely secure, we must expect our codesign system enables him

CALL

(i) to determine the originating station and the receiving station without doubt from day to day of each message;

(ii) to sort all traffic accordingly;

(iii) to follow the course of re-transmitted messages and from the T or 3G instruction in the prefix to try cut possible re-transmitted re-enveloped of the same message.

If a message addressed from a station within the fixed callsign area to a station in the daily changing codesign zone is not re-enveloped, the changing codesign is compromised with the fixed callsign and possibly from day to day. I gather that shortage of cipher staff renders this latter callsign compromise inevitable. The alternative seems to be two cipher versions of one message.

21. The system seems to facilitate enemy cryptographic attack in that

(i) any indiscretion and compromise can be worked on

(ii) routine messages can be collected from day to day;

(iii) captured films of telegram or cipher documents can be examined against earlier cipher traffic intercepted.
22. The present system presents fewer difficulties than the "old wave code call sign system" where each terminal at a large station had a different call sign. In the summer of 1941, the writer with two receivers and one 3SS produced a diagram of MIDDLE EAST static stations in the area OTTOM, SYRIA, PALESTINE, EGYPT, and SUDAN when the wave code system was in force.

23. Illustration of the above statements comes from prisoners and co-belligerent ITALIANS. The latest arrival "ARNOLD", ref SSM/35/39, was employed for 4 weeks only on low grade traffic classification, and as a teleprinter operator. The case with which enemy intercept is controlled is shown by the organisation of the service into 5 REGIONS, No. 4 at BELGRADE being responsible for BALKAN area, No. 7 for ITALY.

24. No 6 BALKAN has

K6 at BELGRADE
Intercept station No. 5 at SALONIKA (30 watches)
No. 6 at ATHENS (30 watches)
Mobile Intercept Day 9th June PACK 2
3 D/F stations.

25. The prisoners worked at No. 6 intercept station at ARGOS, and states that all types of traffic analysis and cryptanalysis are done there. His opinion was that BRITISH signals security was poor, that groups using fixed call signs are particularly easy to intercept. He said that JUNO (CAIRO) was treated as a priority. The full report (SSM/35/39 dated 4 Apr 44) is worth reading.

CONCLUSION

26. It is difficult to explain to anyone not versed in traffic analysis the results that can be achieved.

In the appendix there are imaginary reports from the GERMAN intercept station at ATHENS

(i) For the year 1943 whilst BRITISH used fixed call signs

(ii) and (iii) for two successive weeks in 1943 after a change to daily changing call signs.

It is hoped personnel of these may assist.

27. The practical difficulties of adapting changing call signs to fixed networks are said to be great, if delay in routing traffic is not to result. The GERMAN, however, overcome this. An up to date analysis of their call sign methods and traffic routing from GERMANY might solve the problem.

28. Compilations of call sign books used by operational units could be overcome by the provision of a new book for fixed stations. If well designed, a very long time would elapse before the enemy could reconstruct it, particularly if all figures as well as letters were used throughout.

I suggest that the SIS/FRS staff working on GERMAN traffic obtain a very full insight into the interpretation of signal and cipher security and of start times of IT procedures are measure or assess. May I suggest that the officers of Sign 9 confer with SIS/FRS officers doing traffic analysis, on the subject.

A. FISHER
Colonel, S.S.

Copy to: GBO AIRHQ
30th June 1944

TOP SECRET