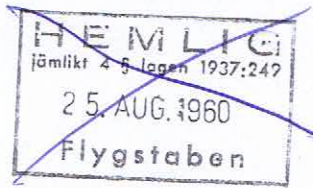




H46



ORIENTERING I TELETJÄNSTEN

26/8 1960

Delgivning: Enl esk- och fljch (motsv) best.

Särskild utsändningslista: Nr 7-23, 28, 30, 31, 63-67 utsändes ej.

Kontroll av kryptoberedskap.

Vid av ÖB anbefalld kontroll av kryptoberedskapen vid FV staber och förband (CFV tpr 262100) har följande iakttagits.

1. Beredskap.

2107	Meddelande (krypterat) utsändes från CFV.
2114	Samtliga adressater hade kvitterat meddelandet. (Bra passning!)
2131	Meddelandet först löst (F 18)
2147	" löst av 40 % adressater.
2204	" " " 70 % "
2330	" sist löst (F 15).
2202-2400	Svar på meddelandet inkom från alla utom en adressat (F 15).

En jämförelse med tidigare kontroller visar en genomsnittligt förbättrad beredskap. Härvid fästes enbart vikt vid tiden från när meddelandet avsänts från CFV tills att det dekrypterats.

Dekrypteringen har genomgående utförts av dagbefäl (dagoff/stf dagoff) och synes visa på en tillfredsställande färdighet hos denna personal i detta avseende. Däremot är förmågan att redigera och kryptera meddelanden sämre (jfr p 2).

CFV avser föreslå ÖB förenklad kryptotjänst i samband med kupp. Detta skulle medföra en högre beredskap samtidigt med minskad kryptobelastning för dagbefälet.

2. Krypteringsfel.

I inkomna svar har följande allvarliga fel förekommit:

svar i klartext (på signalmedel): 3 fall,

olösligt meddelande: 3 fall.

Övriga (lindrigare) förseelser:

meddelandet ej kuperat,

utelämnad sekretessgrad,

utelämnad eller onödig ordskillnad.

Helt utan anmärkning var svaren från F 11 och F 13.

3. WARNING!

Det har inträffat att felaktiga kryptomeddelanden - såväl lösbara som helt eller delvis olösbara - föranlett samtal på klart språk mellan avsändare och mottagare varvid felens art behandlats. Genom avlyssning av dylika samtal kan obehöriga erhålla sådan kännedom om inställningsförfarande, redigering, m m för aktuellt krypto att textskyddet allvarligt äventyras. Risken härför ökar med antalet adressater för meddelandet i fråga. Ett antal samtal i anslutning till ett dylikt meddelande med var för sig till synes oväsentliga upplysningar och påpekanden kan i sammanställning röja hemliga och för textskyddet viktiga uppgifter.

Rapportering av upptäckta fel i kryptomeddelanden - vanligtvis från mottagare till avsändare - bör äga rum. Den är önskvärd från utbildnings- och kontrollsynpunkt. Tidsödande felsökning kan även härigenom underlättas eller elimineras. Dylik rapportering måste dock ske enligt gällande bestämmelser.