H10

HEMLIG
Enligt 4 § ... 1937:249
21 SEP. 1956
Flygstaben

OTEL

ORIENTERING I TELETJÄNSTEN

Delgivning: Off och uoff i signaltjänst. I övrigt enl fljch bestämmande.

Nr 14-21, 56, 60 utdelas ej.
Nr 66-68 tilldelas resp Flybo S, W, N.

KRYPTOTJÄNST

Erfarenheter från FVÖ 1956.

A. Allmänt.

1. Under FVÖ har kryptotjänst bedrivits i betydligt större omfattning än vid tidigare övningar. Antalet kryptobiträden, som utgjordes av repövande vpl, var under övningen endast omkring en tredjedel av i krigsorg upptagna. Å andra sidan torde antalet kryptomeddelanden och använda kryptonycklar (normalt endast F-X nyckel under FVÖ) öka under krig. Erfarenheterna måste anses vara någorlunda representativa, även om de icke helt kunna omsättas till verkliga förhållanden.

2. Kryptobiträdenas arbetsbelastning var genomgående stor. Vid basbat- och depåstaber fanns i regel endast ett krybitr (3 enl F-plan), varför sigoff, sigförv och siguoff i stor utsträckning måste ägna sig åt kryptering och dekryptering.

Kryptoberedskap måste finnas dygnet runt och tjänsten fordrar stor uppmärksamhet och vakenhet för att felprocenten skall kunna hållas nere. Det är därför viktigt att personalen kan beredas erforderlig vila. Erfarenheterna tyda på, att antalet krybitr enl F-plan vid de flesta staber och förband är för litet.

3. Kryptopersonalens berättigade krav på arbetsro, sekretess och möjligheter till betryggande förvaring av kryptomateriel och handlingar har endast i undantagsfall varit tillfredsställande tillgodosedda. Frågan om lokaler för kryptoarbete måste i framtiden ägnas större uppmärksamhet.

Jfr GBKK mom 215, 218, 232-234.

B. Befordringstider.

1. Genomsnittstiden för kryptering resp dekryptering av ett meddelande om ca 50 grp var 10-30 min. I övnledn (chiapp m/40 T) var tiden för dekryptering + utskrift i medeltal 13 min (statistik från 4 dagar med 90 meddelanden om i genomsnitt 43 grupper).

Tiderna för kryptering och dekryptering visade sig vara relativt konstanta. Med nuvarande arbetskrävande mtrl får de anses vara godtagbara. Under förutsättning att större fel icke göres i kryptcarbetet, visar det sig att längre fördröjningstider till stor del uppstå vid stockningar och fördröjningar längs befordringsvägarna.

2. Ex på tider för överbringande av flygvapenorder:

Tid	Inlämnat och kry	Sändning	Dekry och överlämnat x)	S:a	Anm
9/4					
Bästa	15m	12m	13m	40m	Tråd
Sämsta	20m	1t	20m	1t40m	
14/4					
Bästa	12m	51m	12m	1t15m	Radio
Sämsta	20m	1t	1t	2t20m	
Bästa	12m	13m	11m	36m	Tråd
Sämsta	20m	55m	20m	1t36m	

x) Kontrollerat med MB.

3. "Corr" till och "rep" av kryptomeddelanden måste ges så hög företrädesrätt, att dekryptering av det ursprungliga meddelandet icke onödigt fördröjs. Härvid bör ej meddelandet sändas om omedelbart utan den "avsändande" kryptören bör först undersöka om meddelandet kan lösas. (Anledningen till att mottagaren begär "corr" el "rep" kan vara fel från kryptörens sida). Härigenom kan avsevärd tid vinnas.

C. Redigering.

1. Den totala tiden för attöverbringa (krypterade) meddelanden kan väsentligt nedbringas om till signalstationen inlämnade order, underrättelser m m avfattas kortfattat och på ett för kryptering lämpligt sätt. Så vanli regel icke fallet under FVÖ. Det åligger visserligen signalpersonalen att redigera inlämnade meddelanden före avsändning, men detta tar onödigt lång tid om dessa äro olämpligt avfattade. Särskilt vid stora krav på entydighet (t e order) blir redigeringsarbetet tidsödande.

2. Krybitr kunskaper i kryptotjänst har - trots bristande rutin - varit genomgående goda. Detta torde till stor del bero på att en speciell kryptokurs för samtliga vpl krybitr anordnades omedelbart före FVÖ. Särskilt i början av FVÖ förefanns vissa svårigheter att efter dekrytering tolka klartexten. Orsaken härtill synes vara ovana vid FV förkortningar och vukabulär.

3. Ett kryptomeddelande får ej omfatta mera än 50 grupper utöver kryptobeteckningS- och visargrupp. Kryptering av längre meddelanden blir extra tidsödande genom att dessa måste delas upp, ny grund- och arbetsinställning måste föras för varje del och hänvisning till första delen (tidsnumret) måste göras i de följande, ex: "Y DEL TRE TNR ETT TVA FYR FEM Y". Denna hänvisning omfattar ca 5 grp, dvs 10 % av meddelandet. Dessutom tillkommer i regel "Y HEMLIG Y", dvs ca 2 grp, ytterligare "lik i lasten". Detta minskar den praktiska längden av efterföljande delar till ca 40-45 grupper.

En flygvapenorder (nr Op 7), som efter snabbbredigering omfattade 7 st kryptomeddelanden, bearbetades senare ytterligare något av FS/S och kunde därvid förkortas med 1/3 (till 4 st meddelanden).

4. Personalen måste utbildas att avfatta order och meddelanden mera kortfattat och med större hänsyn till kryptoarbetet.

D. Brott mot gällande bestämmelser.

1. Kryptomeddelandena har huvudsakligen bestått av order och underrättelser, till största delen befordrade med fjärrskrift. Trots att order i regel gått med onormalt hög företrädesrätt ha de totala befordringstiderna varit för långa. Detta berodde huvudsakligen på den mycket begränsade kryptokapaciteten.

För att undvika de fördröjningar, som kryptoarbetet medförde uttelefonerades av övningsskäl under FVÖ ett stort antal order och hemliga meddelanden på klartext. Ett sådant förfarande är olämpligt och kan icke generellt tillåtas. Endast i undantagsfall om kravet på snabbhet har avgörande betydelse må sekretessen åsidosättas och metoden tillgripas.

I några fall sändes order såväl med fjärrskift (krypterade) som med telefon (klartext). Detta förfarande innebär ett allvarligt brott mot innebörden av gällande bestämmelser. Det kan underlätta fi forceringsverksamhet och äventyrar därigenom säkerheten hos använda krypton. Jfr GBKK mom 462.

2. Ett stort antal meddelanden har under FVÖ innehållit mer än 50 grp. Det längsta omfattade 89 grp. Tendensen får ses mot bakgrunden av för hög belastning och stabspersonalens ofta framförda krav på större snabbhet i kryptoarbetet.

Möjligheterna till forcering av ett meddelande ökar mycket snabbt om antalet grupper överstiger 50.

3. Ett allvarligt fel gjordes av ett krybitr, som i ett meddelande bifogade arbetsinställningens bokstavsgrupp och därmed röjde aktuell nyckel. Felet upptäcktes och rapporterades snabbt av flera mottagare varefter övergång till annan nyckel beordrades.

E. Lösensystem för stridsledning.

Mot missledande signalering utarbetades inom E 3 ett lösensystem att användas mellan stridsledare och flygplan i luften. I stället för täcktermer användes en enkel matematisk formel. På ff begäran om lösen svarade stridsledaren med en siffergrupp (siffra), som med hjälp av formeln snabbt kunde kontrolleras av ff.

Även om detta system kan förefalla bra - inga täcktabeller i fpl - torde det vara ganska lätt för fienden att snabbt vinna insteg i det. Formeln, som visserligen kan ändras då och då, måste vara så enkel att ff snabbt kan kontrollera erhållen lösen, varigenom fiendens forceringsmöjligheter underlättas.

Frågan om lösensystem för stridsledning skall bearbetas av flygledningen.