

Lärobok i telekrigföring för luftvärnet

Radar och radartaktik



Lärobok i telekrigföring för luftvärnet

Radar och radartaktik

Lärobok i telekrigföring för luftvärnet – Radar och radartaktik

Lärobok i telekrigföring för luftvärnet – Radar och radartaktik 2004 års utgåva (**M7741-850101 Telekri Rr Tak Lv**) fastställs för tillämpning fr o m 2004-09-01.

Beslut i ärendet har fattats av generalmajor Alf Sandqvist. Deltagit i den slutliga handläggningen har varit överste Kent Samuelsson, överstelöjtnant Björn Jacobson samt fördragande major Per Gerdle.

Alf Sandqvist

Per Gerdle

© 2004 Försvarsmakten

Boken är publicerad i samarbete med
Mediablocket AB

Tryck: Elanders Berlings, Malmö

M7741-850101 Telekri Rr Tak Lv

Central lagerhållning: Försvarets bok- och blankettförråd

Förord

Boken behandlar telekrigföring mot främst luftvärnets spaningsradarstationer. Avsikten är att visa hur tekniken påverkar radartaktiken och ibland gränser för vad som kan vara taktiskt lämpligt.

Boken är avsedd för främst luftvärnets taktiska program, TAP, samt MHS termin 3–4, delar kan användas vid utbildning av befälselever. Boken ställer inga förkunskaper förutom gymnasieutbildning. Avsiktligt har förekomsten av matematiska uttrycks minimerats.

Per Gerdle

Innehåll

Förord 3

1. Inledning 11

Informationsoperationer (IO)	11
Ledningskrigföring	13
Telekrigföring	15

2. Historik 17

Inledning	17
Rikttningsbestämning	18
Passiv spaning	18
Övrigt	18
Telemotmedel i insektsvärlden	19
Tekniska motåtgärder	19
Taktiska motåtgärder	20
Första världskriget	20
Andra världskriget	20
Invasionen i Normandie	22
Teknik för störsändning under 1950-talet	25
Koreakriget	26
Vietnamkriget	27
Yom Kippurkriget 1973	29
Bekaadalen 1982 och invasionen av Libanon	32
Gulfkriget	34
Luftförsvarssystemet Kari	34
Underrättelser	35
Planen	36
Desert Storm	39
Elektronisk krigföring under Gulfkriget	43

3. Radarlära 45

Faktorer som påverkar radarns räckvidd	47
Antenn- och målhöjd	49
Konstruktionsprincip	50

Radarns arbetsprincip	51
<i>Avståndsmätning</i>	51
<i>Upptäcktssannolikhet</i>	52
.....	62
<i>Radarantenn</i>	62
<i>Helikopterkanal</i>	73
Faktorer som påverkar radarns prestanda	77
<i>Störningar och falska radarekon</i>	77
<i>Blinda sektorer och falskekon beroende på reflektion i närliggande objekt</i>	77
<i>Sidolobsekon</i>	77
<i>Andragångenrunt ekon (andrasvepsekon)</i>	77
<i>Interferens</i>	78
Radarns funktion – PS-70	79
<i>Sändning</i>	79
<i>Mottagning</i>	80
<i>Måldatasändaren – MDS</i>	80
<i>Funktion</i>	82
<i>Eldledningsradar</i>	94
Fördjupning	96
<i>Elektromagnetiska vågor</i>	96
<i>Egenskaper hos elektromagnetiska vågor</i>	98
Signalanalys	105
<i>Modulation och bandbredd</i>	105
<i>Amplitudmodulering (AM)</i>	106
<i>Frekvensmodulering (FM)</i>	113

4. Telekrigföring 121

Signalspaning	121
<i>Information från signalspaning</i>	124
<i>Riktningsbestämning och triangulering</i>	128
<i>DDOA-mätning av dopplerskillnad</i>	135
<i>Att kombinera flera lägesbestämningsmetoder</i>	136
<i>Prestanda</i>	136
<i>Slutsatser för luftvärnet</i>	139
Signalsökande robotar	140
<i>Målsökaren</i>	141
<i>Banfas</i>	142
<i>Slutfas/dykning</i>	143
<i>Stridsdel</i>	144
<i>Användningsprinciper</i>	144

<i>Exempel på signalsökande robotar</i>	145
<i>Exempel på SSARB-taktik</i>	146
<i>Robottyper</i>	149
Varnar- och motverkanssystem	156
<i>Allmänt</i>	156
<i>Robotskottvarnare</i>	158
<i>Laservarnare</i>	160
<i>Radarvarnare</i>	160
<i>Signalspaning</i>	161
<i>Åtgärdsval</i>	167
<i>Motverkansutrustning</i>	167
<i>Antenner</i>	169
Olika störmetoder	172
<i>Passiva störmetoder</i>	172
<i>Vad händer då en elektromagnetisk våg träffar ett föremål?</i>	191
<i>Metoder att minska målaren</i>	198
<i>Aktiv radarabsorption- plasma stealth</i>	205
Aktiva störmetoder	209
<i>Maskerande störning</i>	214
<i>Vilseledande störsändning</i>	230
<i>Störformer mot eldledningsradar</i>	242
Högeffekt pulsad mikrovågsstrålning (HPM)	263

5. Ledningsystem **277**

Nätverksbaserat försvar	277
<i>Kampen om snabbaste beslutscykeln</i>	277
<i>RMA (Revolution in military affairs)</i>	278
<i>Syftet med NBF</i>	280
<i>Nätverk för vapenstyrning</i>	281
<i>Organisation</i>	283
<i>Motmedel</i>	291
<i>Civil teknik</i>	293
<i>Utvecklingen av NBF</i>	293
Ledningssystemutveckling inom luftvärnet	295
<i>Utformningen av taktiska ledningsverktyg</i>	295
<i>Utveckling av luftvärnets ledningsplatser</i>	296
<i>Hotbildsstudie 1990-talet</i>	299
Ledning av luftvärnsförband	300
<i>Samordning</i>	301
<i>2003-års syn på Luftvärnsledning</i>	302
<i>Luftvärnsunderrättelseområdeschef</i>	302

<i>Begrepp vid sensorledning</i>	<i>305</i>
<i>Uppgifter att reglera vid sensorledning</i>	<i>306</i>
<i>Ledningsverktyg 2003</i>	<i>307</i>
<i>UndE 23 (PS-23) och LvUndC</i>	<i>313</i>
<i>Konceptet LvPlus</i>	<i>320</i>
<i>Om ledning</i>	<i>321</i>

6. Taktik 325

Faktorer som styr radartaktiken	325
<i>Spaningsshotet</i>	<i>325</i>
<i>Telestörning</i>	<i>326</i>
<i>Sammanfattning</i>	<i>327</i>
Att störa ett luftförsvar	327
<i>Sensorkedjan</i>	<i>328</i>
<i>"Home on jam" (HOJ)</i>	<i>329</i>
Att hitta den svaga punkten – förhindra systemkollaps	330
<i>Orsaker till systemkollaps</i>	<i>331</i>
<i>Sammanfattning</i>	<i>335</i>
Några störtaktiska begrepp	336
<i>Bakgrundsstörning</i>	<i>336</i>
<i>Sammanfattning</i>	<i>342</i>
<i>Medstörning (eskortstörning)</i>	<i>342</i>
<i>Egenstörning</i>	<i>350</i>
<i>Förgrundsstörning</i>	<i>353</i>
Luftvärnsjägare	356
<i>Allmänt</i>	<i>356</i>
<i>SEAD-utveckling i USA</i>	<i>357</i>
<i>SEAD i Europa</i>	<i>366</i>
<i>SEAD-utveckling i Ryssland*</i>	<i>367</i>
Passiva spaningsmetoder	370
<i>Signalspaning för luftväret</i>	<i>370</i>
<i>IR-spanare</i>	<i>371</i>
<i>Akustisk helikopterdetektering</i>	<i>372</i>
Skyddsåtgärder mot signalsökande robotar	372
Använda terrängen för att förbättra räckvidden	377
<i>Minska sidoloberna</i>	<i>377</i>
<i>God geometrisk sikt kan ge sämre räckvidd</i>	<i>378</i>
Krysspejling	379
<i>Störbärningar</i>	<i>380</i>
<i>För- och nackdelar med passiv spaning</i>	<i>381</i>
<i>Att krysspejla rätt mål</i>	<i>383</i>

<i>Att pejla starkaste störsändaren</i>	384
<i>När blir egenstöraren starkare än medstöraren?</i>	386
<i>Störsändare med variabel uteffekt</i>	387
<i>Pejling av repeterstörare</i>	387
<i>Antal störbärningar vid ett flyganfall</i>	389
<i>Det är inte säkert att en motståndare behöver störsända</i>	391
<i>Sammanfattning</i>	392
Grupperingsgeometri och sändningstaktik	392
<i>Radarsändning</i>	392
<i>LuLIS som förvarning</i>	398
<i>Alla former av förvarning ökar verkan</i>	399
Påverkbara störskyddsfunktioner i våra radarstationer	401
<i>Frekvensväxling</i>	402
<i>Brusvärde och minst störd frekvens</i>	404
<i>PRF-moder</i>	406
<i>Passiv spaning</i>	408
<i>Pulslängd</i>	410
<i>Stegdämpning</i>	411
<i>Intermittent sändning</i>	412
<i>Sektorsändning</i>	412
<i>Konstant falskalarmeringsnivå – KFA*</i>	414
<i>Detekteringskanaler</i>	417
<i>Målfångning</i>	422
<i>Sammanfattning</i>	425

Bilaga 1. _____ 427

Bilaga 2. Engelskspråkiga begrepp och förkortningar _____ 429

Källor _____ 436

Bildförteckning _____ 438

Inledning



Informationsoperationer (IO)

Under århundradernas lopp har krigföringen i allt mindre grad kommit att avgöras av enbart muskelstyrka, istället har förmågan att fatta snabba beslut och förmedla order blivit allt viktigare för krigets utgång. Den som snabbast kan skaffa sig information om motståndaren och omsätta detta till beslut kommer alltid att befinna sig steget före angriparen. Han kan då lyckas med det han annars behövt mångdubbelt större styrkor för.

Det blir därför nödvändigt att ha en planläggning för hur man själv ska kunna skaffa sig underrättelser och ge order, samt hindra motståndarens motsvarande beslutsprocess.

Informationsoperationer är samordnad verksamhet som genomförs i syfte att påverka motståndarens eller andra aktörers beslut. Detta uppnås genom att påverka beslutsfattare, information och informationsbaserade processer och system. Samtidigt ska man skydda egna beslutsfattare, information och informationsbaserade processer och system. Informationsoperationer stödjer aktivt egna defensiva eller offensiva syften.

I sin vidaste betydelse omfattar informationsoperationer användning av diplomatisk, ekonomiska och militära maktmedel med det yttersta syftet att påverka andra aktörers beslut. Försvarmaktens verksamhet kan utgöra en del i en större nationell informationsoperation. Övriga delar kan t ex vara insatser avseende utrikes- och säkerhetspolitik, diplomati, samordnad informationsberedskap vid kriser och informationssäkerhetsarbete.

Inom Försvarmakten utgör informationsoperationer ett stöd för att uppnå uppsatta militära mål på militärstrategisk, operativ eller taktisk nivå. Informationsoperationer leds på samma sätt som övriga operationer i Försvarmakten.

En viktig del i strävandet efter ledningsöverläge och initiativ är således åtgärder som riktar sig mot motståndarens förmåga att upptäcka, bedöma och fatta beslut. Här har informationsoperationer en nyckelroll. Genom att ge motståndaren vilseledande information eller förvägra honom tillgång till viss information kan vi påverka såväl förmågan till upptäckt som bedömning. Genom att bekämpa informationssystem och kommunikationer kan motståndarens förmåga att fatta beslut och sprida dem begränsas. Offensiva informationsoperationer är tydligt riktade mot motståndarens organisation, sammanhållning och moral. Defensiva informationsoperationer ger

oss bättre skydd mot motståndarens försök att bryta vår vilja att föra kampen vidare. Att behärska informationsoperationer är en viktig del av manövertänkandet, både för att nedsätta motståndarens ledningsförmåga och för att skydda den egna ledningsförmågan, inklusive tilltron till det egna ledningssystemet.

Då man avser att påverka motståndarens eller andra aktörers beslutsfattande med informationsoperationer, är det viktigt att förtydliga ansvar och roller från den politisk-strategisk nivå ned till den taktiska nivån. På de olika nivåerna finns olika sätt att verka inom IO-området enligt bild 1:1.

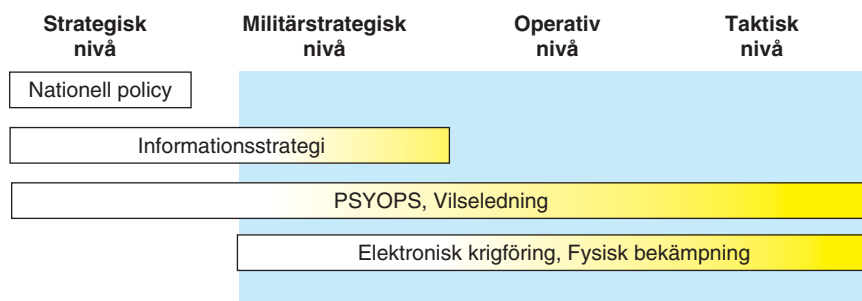


Bild 1:1. Verkansmöjligheter för olika ledningsnivåer.

Informationsoperationer sker t ex genom

- underrättelseskylld som hemligstämpling av viktig information, signaldisciplin m m
- politiska åtgärder för att t ex påverka potentiella allierade
- psykologisk krigföring för att påverka känslor, åsikter och opinioner hos motståndaren
- telekrigföring för att störa ut motståndarens kommunikationer och underrättelsesystem
- fysisk bekämpning av infrastrukturen t ex tv- och radiostationer, telenät m m.

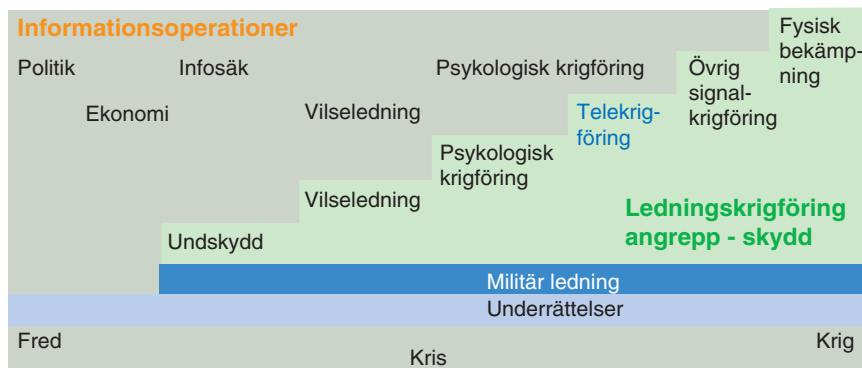


Bild 1:1. Exempel på informationsoperationer under eskalering från fred till krig.

Samhället blir mer och mer känsligt för påverkan på dess kommunikationssystem. Man kan leka med tanken vad en kvalificerad motståndare skulle kunna uträtta om han t ex med hjälp av aggressiva datavirus från internet påverkar

- ett lands kommunikationssystem,
- systemen för datorstyrning av elförsörjningen,
- bankväsendet,
- blockering av datorsystem med e-post.

Troligtvis skulle ett litet land kunna orsaka en stormakt mer skada på detta vis än vad som vore möjligt på konventionell väg. Det är därför troligt att s k hackers redan ingår eller kommer att ingå i framtidens arméer.

Stormakterna har dessutom tagit fram s k EMP-vapen vilka alstrar en elektromagnetisk puls tillräckligt stark för att förstöra alla elektroniska kretsar inom ett område.

Ledningskrigföring

Ledningskrigföring (Command and Control Warfare – C²W) ingår som en del i informationskrigföringen och omfattar olika typer av åtgärder för att minska motståndarens möjligheter till effektiv ledning av sina stridskrafter samt säkerställa den egna ledningsförmågan. Syftet kan ofta vara att vilseleda motståndaren om den egna operativa avsikten.

Ledningskrigföring kan ske med ett antal olika metoder t ex vilseledning, psykologisk krigföring, telekrigföring eller fysisk bekämpning.

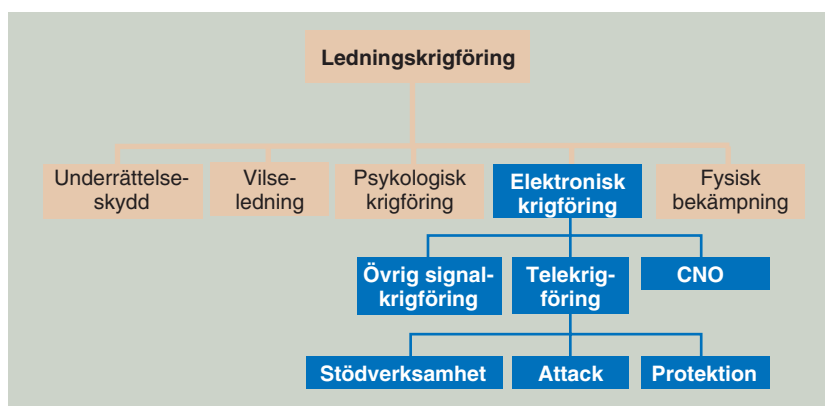


Bild 1:2. Omfattning av ledningskrigföring.

Underrättelseskydd är åtgärder för att hindra eller försvåra för motståndaren att inhämta underrättelser om våra stridskrafter och avsikter. Det omfattar också åtgärder för att minska vår sårbarhet om motståndaren lyckats inhämta underrättelseuppgifter från oss.

Vilseledning är verksamhet och åtgärder med avsikt att ge motståndaren en sådan bild av vår förmåga och/eller våra avsikter så att motståndaren agerar på ett för oss gynnsamt sätt.

Psykologisk krigföring är verksamhet som syftar till att påverka opinioner, känslor, åsikter och uppträdande på ett för oss gynnsamt sätt.

Fysisk bekämpning används för att sätta ledningssystemen d v s personal, organisation och teknik (sambands- och informationssystemen) ur spel.

Elektronisk krigföring omfattar

- bekämpning, förvanskning eller exploatering av motparters inhämtning, bearbetning eller delgivning av information,
- förhindrande av motståndares bekämpning, förvanskning eller exploatering av vår inhämtning, bearbetning eller delgivning av information.

Syftet är att skydda och försvara egna insatser, samtidigt som motståndarnas försvåras eller förhindras.

Elektronisk krigföring omfattar telekrigföring, CNO och övrig signalkrigföring.

Övrig signalkrigföring nyttjar detekterbara fysiska och kemiska egenskaper utom elektromagnetiska som ger upphov till tecken på eller signaler om militär verksamhet. Övrig signalkrigföring omfattar områdena akustik, hydroakustik, magnetik, seismik samt emission av främmande ämnen.

Dator och nätverksoperationer (Computer Network Operations – CNO) är en verksamhet som utnyttjar datorer och nätverk samt dess delsystem för offensiva och defensiva aktiviteter. Syftet är att skydda och försvara egen verksamhet på informationsarenan samtidigt som en motståndares verksamhet försvåras eller förhindras.

Telekrigföring

Syfte och mål med telekrigföring

Telekrigföring definieras enligt Överbefälhavaren som:

”Militär verksamhet som nyttjar det elektromagnetiska spektrumet för att bekämpa, förvanska eller exploatera motpartens inhämtning, bearbetning eller delgivning av information samt skydd mot för oss ogynnsamt nyttjande av det elektromagnetiska spektrumet.”

Telekrigföring avser kampen om det elektromagnetiska spektrat och syftar till att

- säkerställa effekten hos våra egna lednings-, underrättelse- och vapensystem
- hindra motståndaren att få full effekt hos sina motsvarande system.

Telekrigföring ska t ex förhindra motståndaren att få underrättelser, fatta beslut och förmedla beslut eller hindra funktionen hos något vapensystem. Med telekrig menas inte bara störning på radio- och radarbanden utan alla delar av det elektromagnetiska spektrat, t ex störning mot IR och förmågan att se vanligt ljus.

Telekrigföring (Electronic Warfare, EW) indelas i

- elektronisk stödverksamhet (ES)
- elektronisk attack (EA)
- elektronisk protektion (EP)

Elektronisk stödverksamhet – Electronic support (ES)

Elektronisk stödverksamhet utgörs av åtgärder för att stödja pågående verksamhet genom att upptäcka, klassificera, identifiera och lokalisera elektromagnetiska källor.

Det omfattar bl a

- signalspaning mot kommunikationsnät inklusive att fysiskt ansluta i dessa
- signalspaning mot övriga typer av elektromagnetiska emitterar.

Elektronisk attack – Electronic attack (EA)

Elektronisk attack nyttjar den elektromagnetiska energin i syfte att ned-sätta eller förstöra motpartens systemfunktioner eller stridsförmåga.

Det omfattar bl a

- störning och vilseledning inklusive nyttjande av elektromagnetiska skenmål
- nyttjande av icke nukleära elektromagnetiska pulsvapen (NNEMP) och mikrovågsvapen (HPM)

- nyttjande av laservapen
- logiska attacker mot informationssystem t ex virus, dataintrång, och mailbomber.

Elektronisk protektion – Electronic protection (EP)

Elektronisk protektion syftar till att minska effekten av motståndarens telekrigföring samt åtgärder för att undvika elektromagnetiska konflikter.

Det omfattar bl a

- åtgärder för att behålla egna systemprestanda
- åtgärder för att minska risken för upptäckt, identifiering, lokalisering och avlyssning
- åtgärder för att undvika konflikter i det elektromagnetiska spektrumet
- taktisk ledning och kontroll av egna emissioner i det elektromagnetiska spektrumet.

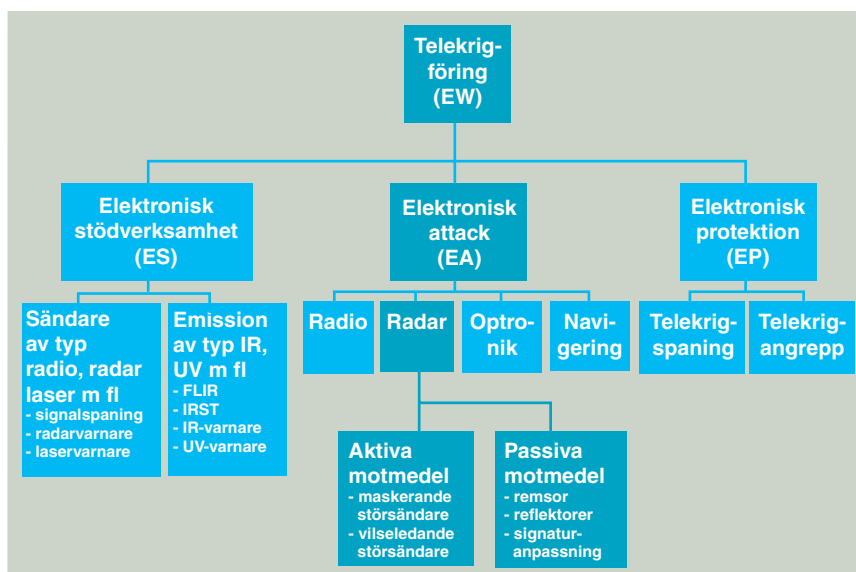


Bild 1:3. Indelningen av telekrigföring.

Äldre begrepp

Andra begrepp som ofta används är

- varnare och system för lokalisering– Electronic Support Measures, ESM
- motmedel (ofta i betydelsen störutrustning) – Electronic Counter Measures, ECM
- störskydd – Electronic Counter Counter Measures, ECCM
- signalspaning – Signal Intelligence, SIGINT.