



FOI informerar om

Telekrig



FOI
Totalförsvarets
forskningsinstitut

Forskningsområdet telekrig syftar till att skapa förutsättningar för att behärska det elektromagnetiska spektrumet för att skydda egna förband, plattformar och personal. Området spänner över bland annat störning, signalspaning och skydd. I Sverige utgör Totalförsvarets forskningsinstitut, FOI, en nationell expertkompetens avseende telekrig.

Den här skriften är framtagen för att ge en introduktion till området och är avsedd att användas som litteratur för utbildning i telekrig inom totalförsvaret. Den riktar sig särskilt till dig som har en yrkesroll där telekrig ingår, men även andra vars verksamheter kan påverka eller påverkas av telekrigföring. Skriften ger en sammanställd bild som annars inte återfinns i litteraturen.

Skriftserien "FOI informerar om" är författad och faktagranskad av forskare och experter vid Totalförsvarets forskningsinstitut. Skrifterna erbjuder läsaren överblick och ökad kunskap inom olika områden relevanta för totalförsvaret. Besök gärna vår webbplats foi.se för att läsa mer om vår forskning.

FOI informerar om

Telekrig

Titel	FOI informerar om Telekrig
Rapportnummer	FOI-R--5989--SE
Månad	Oktober
Utgivningsår	2026
Antal sidor	132
ISSN	1650-1942
Uppdragsgivare	FOI
Forskningsområde	Telekrig
Projektnummer	I530146
Godkänd av	Christian Jönsson
Ansvarig avdelning	Telekrig
Redaktion	Lars Berglund, Göran Kindvall, Gunnar Marcusson
Illustration	Eken Bild & Animation AB
Omslagsbild	Getty Images, Stephen Dalton/Oxford Scientific
Tryck	Multiply Solutions Sweden AB, Järfälla 2026

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bland annat innebär att citering är tillåten i enlighet med vad som anges i 22§ i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Innehållsförteckning

Inledning	4
Elektromagnetisk vågutbredning.....	14
Telekrig mot radiokommunikationssystem.....	24
Telekrig mot radarsystem.....	46
Telekrig mot elektrooptiska system.....	74
Telekrig mot laserkommunikationssystem	94
Tillämpningar.....	100
Närliggande verksamheter.....	106
Skapa kunskap och insikt.....	120
Avslutning.....	124
Bilagor.....	126

Inledning

Introduktion

Syftet med denna skrift är att ge teknisk information om telekrig (Electromagnetic Warfare) och sätta ämnet i sitt sammanhang. Läsaren ska inte behöva ha teknisk bakgrund för att kunna tillgodogöra sig innehållet. För att underlätta förståelsen innehåller skriften både förklarande bilder och faktarutor med fördjupningar.

Med telekrig avses militär verksamhet som utnyttjar det elektromagnetiska spektrumet för att påverka en motparts förmåga att inhämta, bearbeta eller dela information. Telekrig innefattar även skydd mot att en motpart använder spektrumet på ett sätt som skadar den egna verksamheten.

Telekrig är en förmåga som kan användas tillsammans med andra för att uppnå operativa mål. Huvudmålen med telekrig är att försämma effekten hos motståndarens lednings-, underrättelse- och vapensystem. Samtidigt ska de egna systemen fortsätta att fungera trots motståndarens åtgärder samt ge underlag till lägesbild. Telekrig kan delas in i tre huvudområden. I denna skrift använder vi Natos beteckningar:

- Elektromagnetisk stödverksamhet (ESM, Electromagnetic Support Measures) – att upptäcka, identifiera och lokalisera elektromagnetiska källor.
- Elektromagnetisk attack (EA, Electromagnetic Attack) – att använda elektromagnetisk energi för att störa, vilseleda eller slå ut motståndarens system eller stridsförmåga.

- Elektromagnetisk protektion (EPM, Electromagnetic Protective Measures) – att minska effekten av motståndarens telekrigföring samt förhindra elektromagnetiska konflikter.

Andra benämningar är ES (Electronic Support) eller ESM (Electronic Support Measures), EA (Electronic Attack) eller ECM (Electronic Counter Measures) och EP (Electronic Protection) eller ECCM (Electronic Counter Counter Measures).

Elektromagnetiska signaler påverkas av vågutbredningsförhållanden och miljön där de används. Detta behandlas kortfattat i avsnittet om elektromagnetisk vågutbredning.

Skriften fokuserar främst på telekrig riktat mot kommunikations- och sensorsystem. Dessa system beskrivs översiktligt, därefter presenteras telekrigsåtgärder inom ESM, EA och EPM.

Skriften tar också upp tillämpningar av telekrig på förbandsnivå och för egenskydd. Även närliggande verksamheter beskrivs, utan att dessa klassas som telekrig. Därutöver beskrivs hur telekrig kan tränas och övas för att skapa kunskap och insikt.

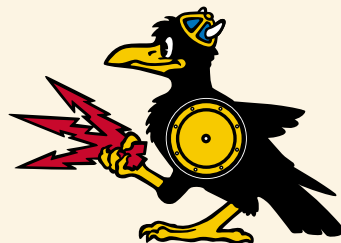
Avslutningsvis kommenteras omvärldsutvecklingen och tillämpningar av telekrig, både avseende nya tekniska lösningar och nya sätt att använda tekniken. Det omfattar också potentiella hot mot civila system.

Symboler

Såväl internationellt som i Sverige har "kråkan" (egentligen en korp) kommit att bli en symbol för telekrig och telekrigare. Bakgrunden är att amerikanska flygvapnet under andra världskriget använde varnar- och motverkanssystem mot radar. Systemen gavs kodnamnet "Raven" (korp) och operatörer för systemen kallades för "Ravens". Efter kriget skapades ett utbildningsprogram i USA för telekrigsoperatörer. Samtidigt började man använda namnet kråka i stället för korp för motmedelsoperatören.



Figur F1. Internationell telekrigssymbol.



Figur F2. Svensk telekrigssymbol.

Telekrig i naturen

I naturen finns många fenomen som kan jämföras med telekrig. Den vanligaste sensorn i djurriket är ögat och ett vanligt sätt att skydda sig är att anpassa sitt utseende till omgivningen. Många bytesdjur har kamouflagefärgad päls eller fjäderdräkt. Kameleonten är känd för att kunna ändra sin färg efter omgivningen och skorpionfisken – en av världens giftigaste fiskar – använder samma förmåga när den jagar.

Det finns även djur som försöker lura angriparen genom att se ut som något helt annat. Svalstjärtsfjärilslarven efterliknar fågelavföring för att inte bli uppäten. Ett annat exempel är kungssnoken, som är ofarlig, men liknar den giftiga korallormen. När ett ogiftigt djur imiterar ett giftigt kallas det för batesisk mimikry.

I naturen förekommer också motmedel. Bläckfiskar kan till exempel släppa ut bläck när de hotas samtidigt som de gör en snabb undanmanöver. Vissa djuphavsbläckfiskar kan dessutom avge ett fluorescerande ämne för att förstöra mörkerseendet hos angriparen.

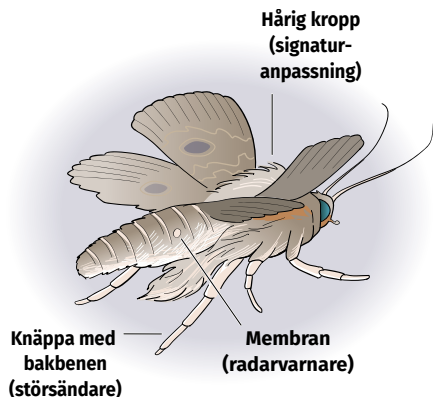
Naturen visar även exempel på "signalkrigsföring". Ett rovdjur kan närma sig bytet mot vinden för att undvika att avslöjas av sin lukt. Skunken använder sensormättning genom att sprida en så kraftig lukt att angriparen tvingas retirera. Katter smyger och ugglor flyger tyst för att inte avslöjas av sina ljud. Kanske påminner kampen mellan fladdermus och nattfjäril mest om telekrig även om den utspelar sig inom akustiken.

Duell mellan fladdermus och nattfjäril

Följande exempel beskriver hur fladdermus och nattfjäril använder både sensorer och motmedel på ett sätt som liknar modern telekrigföring.

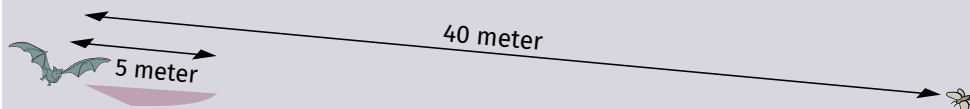
Fladdermusens främsta jaktvapen är ett avancerat ekolod som använder ultraljud med en våglängd på cirka en centimeter. Med detta kan fladdermusen upptäcka ett byte på ungefär fem meters avstånd.

Nattfjärilen har hår på kroppen som är ungefär en fjärdedel av ultraljudets våglängd. Detta gör att ekot från fjärilen minskar, vilket är ett biologiskt exempel på signaturanpassning.

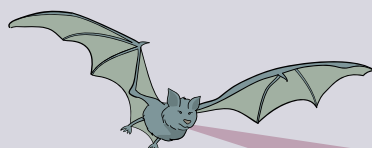


Avstånd

Avståndet mellan nattfjärilen och fladdermusen kan vara upp till fem meter för att fladdermusen ska kunna detektera nattfjärilen. Nattfjärilen har membran som känner av ljudet från fladdermusen på ca 40 meter.

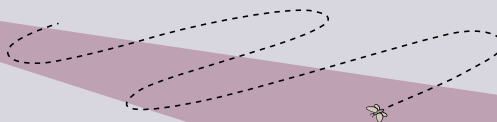


1. Manövreringsteknik mot doppler

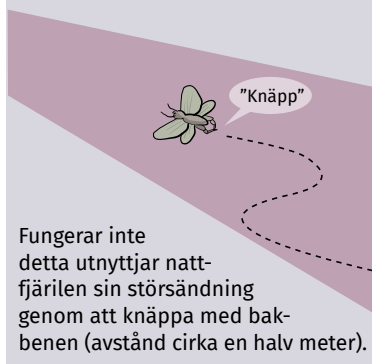


Genom att använda sig av doppler kan fladdermusen höra om nattfjärilen rör sig bortåt.

Nattfjärilen kontrar med att flyga rakt åt sidan i förhållande till fladdermusens radar. Dopplerskiftet försvinner.

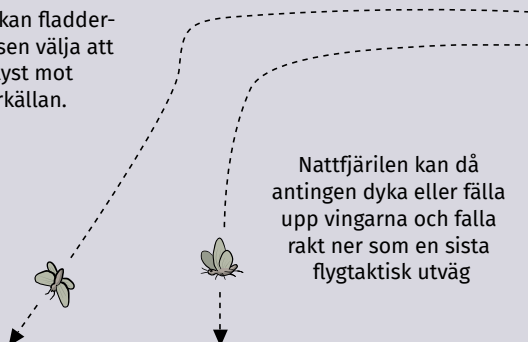


2. Störsändning



3. Flygtaktik mot radartystnad

Nu kan fladdermusen välja att gå tyst mot storkällan.



Figur 1. Duellen mellan fladdermus och nattfjäril.

Exempel på telekrig i krig och konflikter

Den första duellen

Ett av de tidigaste exemplen på telekrig inträffade under det andra boerkriget i januari 1900. Den brittiska flottan försökte uppmuntra den omringade garnisonen i Ladysmith (nuvarande uMnambithi i Sydafrika) genom att sända meddelanden i morsekod med strålkastare mot molnen. Systemet fungerade bara i ungefär en halvtimme innan boerna började använda en egen strålkastare för att störa signalerna. Genom att blinka, flimra och korsa ljusstrålen försökte de förväxla prickar och streck, vilket är ett tidigt exempel på telekrig.

Användandet av remsor

Under andra världskriget arbetade briter med att hitta metoder för att störa tyska radarstationer. En av lösningarna var att släppa metallbelagda pappersremsor i luften för att skapa falska radarekon. På engelska kom det att kallas "chaff". Försök genomfördes under 1941 i största hemlighet för att tyskarna inte skulle få veta om tekniken.

År 1942 var remsorna färdigutvecklade, men ledningen under Churchill vågade inte använda dem av rädsla för att Tyskland skulle börja använda samma metod. I Tyskland pågick samtidigt liknande forskning under namnet Düppel. Även där genomfördes tester 1942 och även där stoppades utvecklingen. Göring fruktade att briter annars skulle svara med samma teknik.

Först den 23 juli 1943 gavs tillstånd i Storbritannien att använda remsor i samband med bombningen av Hamburg. Signalen för insatsen var "Open the Windows". Under räden deltog 795 bombflygplan och sammanlagt släpptes 92 miljoner aluminiumremsor (cirka 40 ton). Förlusten blev 12 flygplan eller 1,5 procent jämfört med ett normalt förväntat bortfall på cirka 6 procent.

Falklandskriget

Remsor kom åter till användning under Falklandskriget 1982, då de användes av brittiska fartyg för att avleda radarsökande sjömålsrobotar av typen

Exocet. Den 26 maj avfyrares två Exocetrobotar mot fregatten HMS Ambuscade. Fregatten hade redan hunnit skjuta ut remsor före avfyringen och robotarna läste i stället på remsmolnet. Därmed klarade sig Ambuscade oskadd. När robotarna hade passerat remsorna gick de tillbaka till sökfase och träffade i stället ro-ro (roll on/roll off)-fartyget Atlantic Conveyor, som saknade telekrigssystem. Förlusten av fartyget innebär att mycket viktig materiel gick förlorad.

Bekaadalen

Slaget om Bekaadalen 1982 lyfts ofta fram som ett exempel på telekrigets potential. Den israeliska sidan använde skenmålsrobotar för att aktivera syriskas luftvärnsradarsystem. När radarsystemen väl sände kunde de lokaliseras och bekämpas med signalsökande robotar.

Israeliska stridspiloter utnyttjade dessutom att de syriskas jaktplanens radarvarnare hade "blinda" sektorer. Samtidigt stördes kommunikationen mellan de syriskas flygplanen och stridsledningen, vilket ökade effekten av de israeliska insatserna. Konflikten var telekrigsmässigt asymmetrisk med en tydlig israelisk överlägsenhet.

"Desert Storm"

Operation Desert Storm 1991 innebär ett tekniskt genombrott. För första gången användes rymdbaserade system i stor skala för övervakning och navigering. Andra centrala tekniker var kryssningsrobotar, signaturanpassning (stealth) och avancerade radarsystem för markövervakning och luftförsvarsbekämpning. Styrda vapen (laserstyrda, elektrooptiska och signalsökande) fick stort genomslag.

Amerikanska stridsvagnar hade sensorer med betydligt längre räckvidd än de irakiska, även i mörker. De kunde därför bekämpa mål innan motståndaren ens upptäckte dem.

Telekrig spelade en stor roll. Flygplan som F-4G Wild Weasel, EA-6B Prowler och EC-130H störde radar- och kommunikationssystem. Stealth-flygplanet F-117A flög alltid med

understöd av EA-6B. En önskad bieffekt var att irakierna ofta började skjuta intensivt med luftvärnskanoner när störningen startade, eftersom telekrigsinsatsen uppfattades som en signal om att ett flyganfall var på gång.

Signalsökande robotar hade mycket stor effekt. Mer än 1 000 HARM-robotar avfyrades, vilket resulterade i att endast fem procent av de irakiska radarsystemen var aktiverade efter sex dagar. Alla var aktiva vid konfliktens början.

Kosovokriget

Under Kosovokriget blev vädret en avgörande faktor. Det ihållande regnet försvårade användningen av elektrooptiska sensorer och laserstyrning, som fungerat mycket väl under Desert Storm. I stället fick radarsystem, som är mindre känsliga för väder, en större roll. En viktig erfarenhet från konflikten var behovet av GPS-styrning för att få hög träffsäkerhet i dåliga siktförhållanden.

Nato lyckades inte slå ut det serbiska luftförsvaret, bland annat på grund av att serberna använde skenmål och höll sina radarsystem

avstängda. Luftförsvaret var dessutom redundant och bemannat av vältränad personal med disciplinerad taktik, sannolikt efter lärdomar från Desert Storm.

Eftersom luftförsvaret aldrig neutraliserades behövdes löpande insatser som ISR (Intelligence, Surveillance and Reconnaissance) och SEAD (Suppression of Enemy Air Defences) under hela det 78 dagar långa kriget. Nato fick inte flyga under 15 000 fot (4 500 meter). Uppgiften blev särskilt krävande för besättningarna i EA-6B, som också understödde stealth-bombaren B-2. Bekämpningen av den serbiska markarmén blev effektiv först sedan Kosovos befrielsearmé (UCK) inlett sin offensiv.

Ukrainakriget

I den öppna rapporteringen från kriget i Ukraina framgår att telekrig används av båda sidor, både offensivt och defensivt. Exempel från Ukraina visar inte bara bredden inom telekrig, utan även hur avgörande det är att ha korrekt och aktuell information om operationsområdet och om motståndarens system.

Svenska erfarenheter av telekrig

Telekrig har länge varit en del av svenska militära insatser. Ett tydligt exempel är telekrigsbataljonens oavbrutna deltagande i utlandsmissioner från 1990-talet på Balkan till insatser, bland annat i Mali, i början av 2020-talet, se figur 2.



Figur 2. Den svenska styrkan i Mali på patrull 2017. Foto: Mats Nyström/Försvarmakten.

Fokus för insatserna har främst varit:

- Force Protection – särskilt skydd mot fjärrutlösning av bomber.
- Taktisk signalspaning – för att samla in underlag och skapa en samlad lägesbild.



Figur 3. JAS 39 Gripen startar från Sigonellabasen på Sicilien. Foto: Johan Lundahl/Försvarmakten



Figur 4. HMS Gävle i Medelhavet under ML01. Foto: FMV.

Flyginsatserna över Libyen 2011 och korvettinsatserna utanför Libanon i mitten av 00-talet hade liknande upplägg, se figur 3 och 4. Plattformarna fick systeminställningar anpassade till aktuella hot och bidrog med signalspaning för den gemensamma lägesbilden.

Dessa insatser visar hur telekrig i modern tid används på marken, i luften och till sjöss.

Samtidigt måste de data som återrapporteras från insatsmiljön behandlas så att de snabbt kan omsättas till praktisk nytta i mark-, luft- och sjöstridskrafter. I många fall krävs hög precision i

signaldata för att egna system ska fungera som avsett. Det ställer krav på:

- noggrann analys
- bearbetning och produktion av stora mängder data
- kontinuerlig uppdatering till förbanden.

Här fungerar Telekrigstödenheten (TKSE) som ett nav. Enhetens arbete pågår året runt och syftar till att förse insatsförbanden med rätt data-satser, så att telekrigssystemen kan upprätthålla förmåga till spaning, varning, skydd och verkan.

Samarbete och övningar

När system ska användas tillsammans med andra nationer ökar behovet av gemensamma tester och övningar. Sverige har inom Natoramverk – även före det fulla medlemskapet – deltagit i aktiviteter med målet att skapa gemensam förmåga inom telekrig.

Samverkan mellan nationer och försvarsgrenar utvecklas fortlöpande. Samtidigt växer kraven på samordning, eftersom allt fler avancerade kommunikations- och spaningssystem kräver att telekrigsförband kan fungera ihop med andra förband.

Det finns dessutom gemensamma utmaningar. Allt fler system har dual-use-karaktär, vilket innebär att de används både civilt och militärt. Det gör det svårt att öva i fredstid eftersom systemen kan vara samhällsviktiga. Ett tydligt exem-

pel är GPS och andra positioneringssystem, där det är svårt att öva med störsändning. Det påverkar i sin tur vilka områden det går att öva i och hur övningar med störsändning måste planeras och genomföras.

Frekvenser och vågformstekniker

Radiokommunikation och radar utnyttjar till stora delar samma frekvensband och liknande vågformstekniker. För att undvika upprepning tas de gemensamma delarna upp i detta avsnitt.

Frekvensband

Inom radio och radar används olika benämningar och frekvensomfång för de frekvensband som avses, se Tabell 1.

Vågformstekniker

Flera metoder har tagits fram för att använda frekvensspektrumet på ett mer effektivt sätt. Det ger också flera fördelar som beskrivs nedan.

Frekvenshoppsteknik

Frekvenshoppsteknik används för att minska inverkan av störsändning och minska interferens, men det påverkar även signalspaningen. Signalen är oftast momentant smalbandig och ändrar sin huvudfrekvens hundratals, ibland tusentals, gånger per sekund, enligt ett i förväg bestämt mönster som mottagaren redan känner till.

Tekniken användes ursprungligen i militära radiosystem för att undgå avsiktlig störning. I dag används den också kommersiellt för att minska risken för störningar på öppna frekvensband där många sänder.

Inom radarområdet är frekvenshopp främst dels ett störskydd, dels ett skydd mot interferens med andra sändare på samma frekvens.

Direktsekvensspridning

En radiosignal kan spridas över ett mycket stort frekvensband, vilket gör den mer robust och mindre känslig för störningar. Effekttätheten kan bli så låg att signalen döljs i det naturliga

bruset, vilket minskar sannolikheten för att den kan upptäckas. Mottagaren kan sedan använda samma kod för att ”avsprida” (despread) signalen och återskapa den ursprungliga informationen.

En av fördelarna med direktsekvensspridning är att den sända signalen ser ut som lågfrekvent brus för den som inte har tillgång till rätt kod. En signalspanare som tar emot signalen kan inte räkna med att se någon indikation av signalen enbart genom att titta på frekvensspektrumet för den mottagna signalen.

Pulskompression är en variant av detta med radar. Genom kodning kan en lång puls med låg energi komprimeras i mottagaren och omvandlas till en kort puls med hög effekt. På detta sätt kan radarn nå längre och ändå få en bättre upplösning.

Multicarrier-teknik

Den vanligaste varianten av multicarrier-teknik är ortogonal frekvensmultiplexering (OFDM), som delar upp dataströmmen i mindre bitar. Den används i många moderna kommunikationssystem som digital-tv, wifi och fjärde generationens mobila nätverk (LTE). Signalen består av ett stort antal smala underkanaler (bärvågor) som sänds samtidigt och tillsammans utgör en bredbandig överföring. Varje bärvåg bär en delmängd av den totala informationen och tack vare den ortogonala relationen, som gör att de inte stör ut varandra, kan mottagaren på ett effektivt sätt separera och återskapa dataströmmen. ■

Tabell 1. Benämning av frekvensband. Den vänstra tabellstapeln är benämningar enligt ITU (International Telecommunication Union) och används inom radiokommunikation. Den mellersta tabellstapeln är benämningar enligt IEEE (Institute of Electrical and Electronics Engineers). Den högra tabellstapeln är nomenklatur enligt Nato. De två senare tabellstaplarna används vanligtvis för radar.

Frekvens	GHZ			MHZ			våglängd
	300						1
	100						3
	60						
	30						5
							7,5
	10						3
	6						5
	3						7,5
	1						3
							6
	300						1
	100						3
	60						
	30						
	10						30
	6						
	3						
	1						300

Decibelbegreppet

För fysikaliska storheter vars mätetal vanligen varierar inom ett stort område, åtskilliga tiopotenser, finns det ett behov av att göra värdeskalen mer kompakt. Ett sätt att göra detta är att utnyttja ett relativt, logaritmiskt mått, som betecknas decibel, förkortat dB. En egenskap vid användandet av dB är att addition och subtraktion ersätter multiplikation och division vilket förenklar beräkningar och underlättar förståelsen av grafiska presentationer.

Grundläggande definition:

$B = \text{Bel} = \log_{10}(P_1/P_2)$, d.v.s.

$\text{dB} = \text{decibel} = 10 \cdot \log_{10}(P_1/P_2)$

där P_1 = den uppmätta eller beräknade effekten, och P_2 = referenseffekten.

Decibel uttrycker alltså förhållandet mellan två effektvärden. För att uttrycka en absolut storhet refereras denna till en baskvantitet. Ett exempel är dBm, som t.ex. används för att ange uteffekten från en generator. I detta fall ansätts att baskvantiteten, det vill säga referenseffekten P_2 är 1 mW. Om $P_1 = 1$ watt uttrycks alltså detta som $P_1 = 30$ dBm.

Dopplereffekt

Då ett målobjekt rör sig i förhållande till den detekterande sensorn blir vanligen frekvensen hos den mottagna signalen en annan än hos den utsända. Fenomenet kallas dopplereffekt och uppträder för alla slags vågor.

Dopplereffekt uppstår både då sändaren rör sig, då observatören rör sig och då bägge rör sig (så länge inte den relativa rörelsen är noll).

Det kanske allra lättast iakttagbara exemplet på dopplereffekten är sirenerna från utryckningsfordon. Ljudet från dessa minskar i frekvens då fordonen passerar observatören. Allmänt gäller att då avståndet minskar uppfattar observatören en högre frekvens än den utsända medan observatören då avståndet ökar uppfattar en lägre frekvens än den utsända.

För fallet aktiv sensor med sändare och mottagare (observatör) på samma plattform (och således med samma rörelse) kan frekvensförskjutningen skrivas $\Delta f = 2vf/c = 2v/l$ där f är den utsända frekvensen, l våglängden, v målets rörelse relativt sensorn längs siktlinjen och c vågens utbredningshastighet. Beroende på om målet närmar eller fjärrar sig kan dopplereffekten bli positiv eller negativ.

Dopplereffekten har mycket stor betydelse eftersom frekvensförskjutningen hos ett eko dels gör detta lättare att uppfatta, dels ger uppgifter om målets rörelser.

Elektromagnetisk vågutbredning

Hur elektromagnetiska vågor breder ut sig har avgörande betydelse för hur radio-, radar- och elektrooptiska system fungerar. Den elektromagnetiska vågutbredningen blir en begränsande faktor i större utsträckning än tidigare i takt med bättre prestanda och ökad komplexitet i moderna system. Det krävs god kännedom om vågutbredningen och störningsbakgrunden för att veta hur systemen fungerar i en verklig miljö. Hur en elektromagnetisk våg eller signal färdas genom atmosfären är generellt svårt att förutsäga på grund av dynamiken i form av variationer i höjd, luftfuktighet, tryck, temperatur,

turbulens samt även solens joniserande inverkan på mediet. Andra faktorer som är svåra att modellera och som påverkar vågutbredningen är topografi, markbeklädnad, markytans struktur och markens elektriska egenskaper. Dessa omständigheter inbjuder till enkla genvägar som kan resultera i orealistiska uppskattningar av systemprestanda, ibland som rena glädjesiffror eller i form av undervärderade systemegenskaper. Vågutbredningen genom atmosfärens dynamiska miljö är det som sätter gränser för dagens och sannolikt även morgondagens system inom radio, radar och elektrooptik.

Utbredning av radiovågor

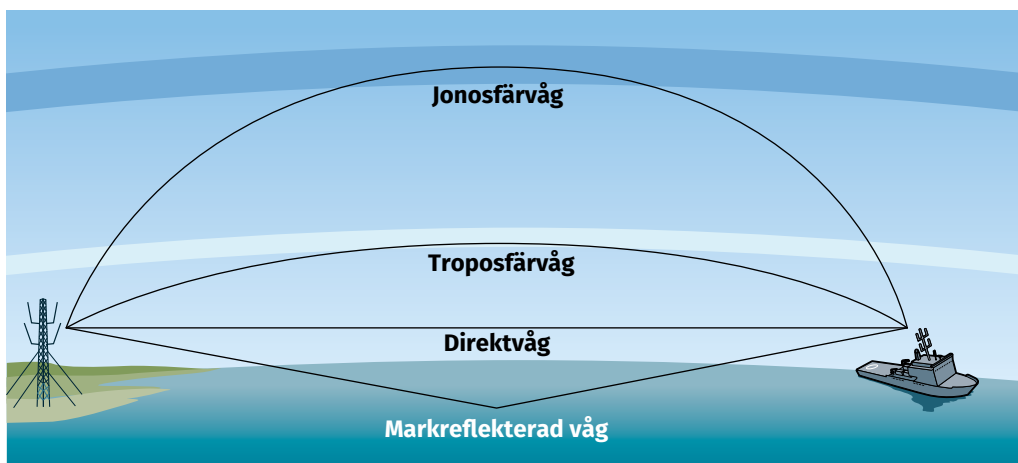
Radiovågor breder ut sig genom transmission, spridning, reflektion och diffraktion. Dessa utbredningsmekanismer påverkas i sin tur av terrängen, dess topografi, vad som finns på marken samt atmosfärens egenskaper, inklusive brus. Utbredningsmekanismerna ger alla upphov till fenomen som påverkar systemens prestanda.

En radiovåg som färdas från en sändare kan nå en mottagare via flera olika utbredningsvägar, se figur 5. Nära jordytan kan man urskilja en direktvåg, en markreflekterad våg samt en ytvåg. Direktvågen och den markreflekterade vågen kombineras till atmosfärsvågen. Ytvågen kan bara existera tätt utmed marken och är enbart viktig om sändarantennens höjd är liten i förhållande till våglängden. De vågor som utbreder sig i atmosfären kan påverkas av skikt i troposfären, som sträcker sig från jordytan upp till cirka 10 kilometers höjd, och jonosfären, som sträcker sig från cirka 40 till 1 000 kilometers höjd.

Skikten i troposfären uppkommer genom vertikala förändringar i temperatur och fuktighet som påverkar elektromagnetiska vågor från cirka 30 MHz och uppåt i frekvens. Den reflekterade vågen från dessa skikt benämns troposfärvåg. De jonosfärskikt som uppkommer genom joniserande strålning från solen reflekterar främst vågor med frekvenser från 30 MHz och nedåt. Den reflekterade vågen kallas jonosfärvåg.

Markens inverkan

När en radiovåg träffar en yta reflekteras den på två olika sätt. En del av vågen reflekteras åt olika håll (diffus reflektion eller spridning) medan en annan del reflekteras mer som i en spegel. När ytan är ojämn sprids vågen åt olika håll beroende av ytans struktur och den infallande vågens riktning. Den spegelliknande reflektionen motsvarar den spegelreflektion som ytan skulle ge om den vore fullständigt jämn. Här gäller spegelvill-



Figur 5. De viktigaste utbredningsvägarna mellan en sändare och en mottagare i form av atmosfärvåg (bestående av direktvåg och markreflekterad våg), troposfärvåg och jonosfärvåg. Observera att jonosfärvåg och troposfärvåg inte uppträder samtidigt.

koret, det vill säga att den reflekterade vågens vinkel mot ytan är lika stor som den infallande vågens. För en plan yta kan man även ange en reflektionsfaktor. Den beskriver hur stor del av en inkommande radiovåg som reflekteras tillbaka, både avseende styrka och fas. Storleken på reflektionsfaktorn bestäms av infallsvinkel, frekvens och hur bra ytan leder elektricitet.

Vågutbredning i skuggan bakom till exempel byggnader och berg sker genom att radiovågorna böjs av (diffraktion) kring hindret. På så sätt kan kommunikation upprätthållas bakom hinder även vid höga frekvenser, se figur 6.

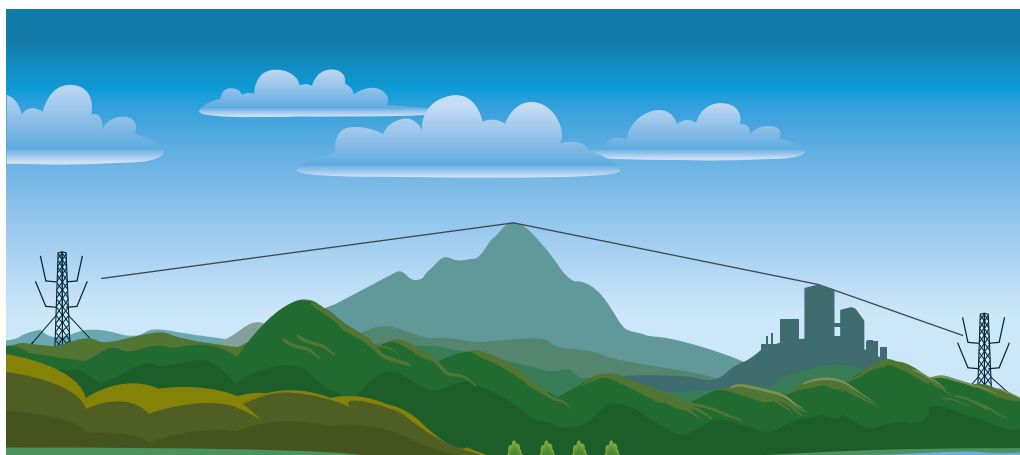
Skog och annan vegetation påverkar i hög grad hur de elektromagnetiska vågorna utbreder sig. Inverkan sker i form av ren dämpning, men även genom polarisationsvridning och att vågen utbreder sig samtidigt utmed flera utbredningsvägar (flervägsutbredning). Den totala effekten av olika vågutbredningsfenomen i kuperad terräng exemplifieras i figur 7.

I kuperad terräng påverkas de elektromagnetiska vågorna av reflekterande ytor som större stenblock, bergssidor, kullar, åsar och raviner. I stadsmiljö finns det rikligt med reflekterande objekt, både stora och små. Det kan vara hus, broar, stolpar, elektriska ledare, fordon samt träd.

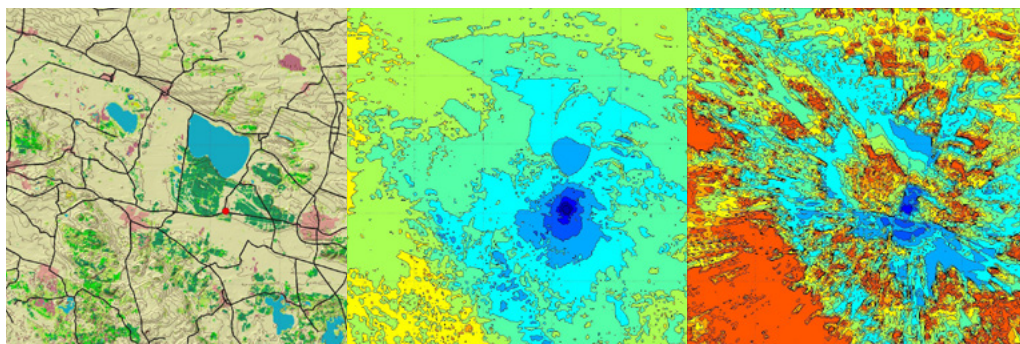
Om stationerna är högt placerade på kullar eller berg ger det en generellt minskad transmissionsförlust (utbredningsdämpningen mellan sändare och mottagarantenn), medan placering djupt nere i dalgångar ger förhöjd transmissionsförlust. Stora och jämna ytor ger upphov till flera distinkta och kraftiga utbredningsvägar som reflekteras medan mindre och ojämna ytor bidrar till spridningssignalen.

Signalstyrkan varierar om sändare och/eller mottagare flyttas i rummet. Man skiljer mellan två olika typer av fädning (amplitud- och/eller fasvariationer hos mottagen signal), dels en storskalig variation i rummet, dels en lokal variation. Den storskaliga fädningen bestäms huvudsakligen av hur terrängen ser ut mellan sändare och mottagare.

Vid förflyttning i rummet uppstår fädning med ett max-till-max-avstånd på en halv våglängd, vilket för höga frekvenser ger mycket snabb fädning vid små förflyttningar. Fädningen kan uppstå både om sändare eller mottagare flyttas och den kan vara mycket djup. Orsaken till denna fädning är att radiovågen i allmänhet är sammansatt av en direktvåg och ett stort antal flervägskomponenter, som har olika amplitud och fas, och som reflekterats från



Figur 6. Diffraktion över terränghinder och byggnader.



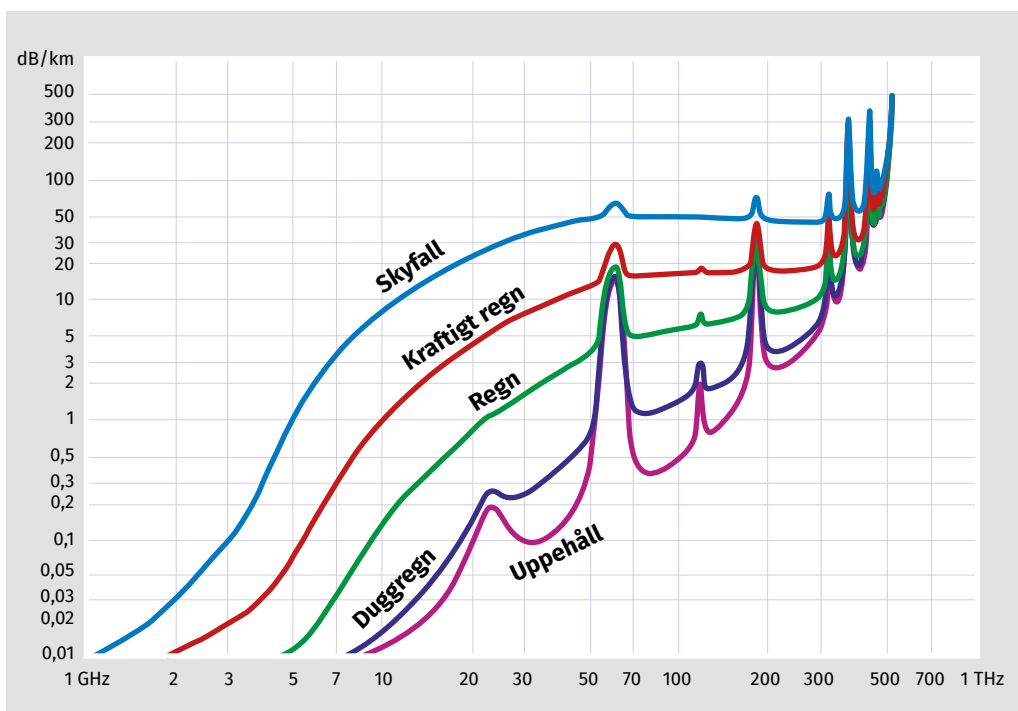
Figur 7. Exempel på hur terrängen dämpar radiovågens utbredning vid 50 MHz (mitten) och 1800 MHz (höger) i ett 25x25 kilometer stort terrängavsnitt på övningsfältet Revingehed. Sändaren är placerad vid den röda pricken på kartan till vänster. Höjderna för sändarna, 10 respektive 60 meter, motsvarar typiska höjder för radio Ra570 med högantenn (50 MHz) och för en 4G/LTE basstation (1800 MHz). Höjderna för mottagarantennerna är i båda fallen 3 meter. Färgskalan motsvarar en transmissionsförlust från 70 (mörkt blå) till 170 dB (mörkt röd). Bilderna är framtagna med hjälp av FOI:s beräkningsprogram för vågutbredning detvag90.

olika föremål i terrängen. Om någon eller flera av flervägskomponenterna färdas en betydligt längre sträcka än direktvägen uppstår dessutom utspridning i tiden av mottagen signal (tidsdispersion). Det gör i sin tur att radiokanalen påverkar signalens ingående frekvenser olika (frekvensselektiv fädnings). Det gör också att digitala symboler utsända vid olika tidpunkter kommer

fram till mottagaren samtidigt och stör varandra (intersymbolinterferens). Båda fenomenen gör det svårt för mottagaren att tolka signalen korrekt.

Troposfärens inverkan

Troposfärens inverkan ökar uppåt i frekvens från cirka 30 MHz. Detta kan ge stora ökningar av



Figur 8. Specifik dämpning från gaser och nederbörd i området 1–600 GHz. Kurvan med minsta dämpning motsvarar uppehåll och därefter i stigande grad duggregn (ca 0,25 mm/h), regn (ca 4 mm/h), kraftigt regn (ca 25 mm/h) samt slutligen skyfall (ca 150 mm/h).

räckvidden men även underräckvidder (betydligt kortare räckvidder) samt depolarisation och diverse spridningsfenomen. Dessutom uppstår flervägsutbredning som kan medföra att signalstyrkan ändras snabbt i tid och/eller rum.

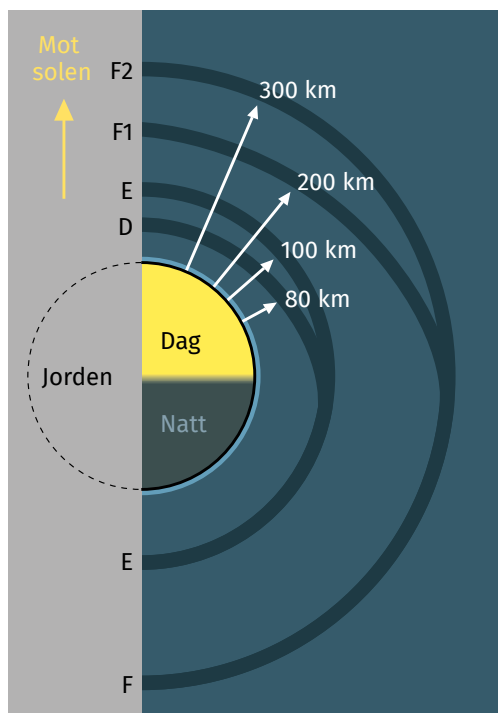
Effekten på mottagarsystem blir bland annat interferenser, fädning och påverkan på räckvidden. För ett radarsystem kan sannolikheten för upptäckt av ett mål minska och sannolikheten för detektion av falska mål kan öka. Även räckvidden för ett radarsystem kan påverkas kraftigt. Vidare uppstår diverse inmättningsfel där höjdmättningsfel i radarsystem dominerar.

Ledsikt har stor betydelse för radiovågors utbredning i troposfären. Dessa ledsikt kan bryta radiovågorna både mot och från jordytan. Skikten uppstår på grund av variationer av luftens brytningsindex i höjdd. Allmänt gäller att luftens brytningsindex avtar linjärt med höjden.

Avvikelser, så kallade anomalier, förekommer dock tämligen ofta inom vissa delar av den lägre troposfären, speciellt sommartid. Skikt med markant avvikelse är i regel relativt tunna, oftast 100 meter eller mindre. Ett ledsikt bildas när temperatur och luftfuktighet förändras mycket med höjden. För att det ska hända måste brytningsindex minska snabbt när man kommer högre upp. Det sker om temperaturen ökar och/eller om luftfuktigheten minskar.

Normalt sett avtar temperaturen med höjden. Det omvända kallas temperaturinversion och betyder att temperaturen ökar kraftigt med höjden inom ett begränsat intervall och bidrar till bildandet av ett ledsikt.

Den vanligast förekommande inversionen är havsinversionen (även kallad maritim inversion), som under en stor del av året förekommer över havsytan, och kan ge upphov till så



Figur 9. Jonosfärskikt; typiska höjder dag och natt. Skiktet F1 existerar ungefär i höjdiintervallet 150–220 km och F2 i höjdiintervallet 280–800 km.

kallade avdunstningsskikt med höjder upp till några tiotal meter. Dessa skikt har i regel mycket homogen fördelning över stora havsytor, vilket gynnar uppkomsten av ledskikt.

Strålningsinversion (även kallad markinversion) är den absolut vanligaste typen av temperaturinversion. Den uppstår endast över land under klara nätter, då utstrålningen medför kraftig avkylning av markytan. Strålningsinversioner förekommer i likhet med havsinversioner inom relativt tunna skikt närmast jordytan.

På vissa av svenska marinens fartyg används mjukvaran LBM (Lokal BrytningsindexModell) för att beräkna om det finns ledskikt eller inte genom att mäta ytvattnets temperatur, lufttemperatur, luftfuktighet samt vindhastighet. Eftersom ledskikt påverkar radar- och radiosignaler kan fartygets uppträdande delvis anpassas baserat på resultaten av en LBM-beräkning.

Gaser i atmosfären och olika former av nederbörd ger extra dämpning som i allmänhet ökar med stigande frekvens, se figur 8. Vid frekvenser under 10 GHz kan man oftast förbise denna dämpning. Absorption i vattenånga och syre ger kraftiga dämpningstoppar vid 22 respektive 60 GHz. Ökad regnintensitet ökar dessutom dämpningen.

Jonosfärens inverkan

Radiovågor under en viss frekvens kan inte tränga igenom de joniserade skikt på höjder mellan 40 och 1000 kilometer som utgör jonosfären. Den s.k. plasmafrekvensen är ett mått på tätheten av fria elektroner i jonosfären. Dessa fria elektroner bildas när solens joniserande strålar träffar atmosfären. Det handlar främst om ultraviolett ljus (UV), extrem ultraviolett strålning (EUV) och röntgenstrålning. Även partikelstrålning som kommer från solen med solvinden, bidrar till att skapa fria elektroner. Maxvärdet för plasmafrekvensen kallas för den kritiska frekvensen och ligger vanligen inom 3–30 MHz. Radiovågor på lägre frekvenser än den kritiska frekvensen är alltid instängda under jonosfären. Reflektion och avböjning i jonosfärsskikten gör att radiovågen kan utbreda sig längs med jordytans krökning.

Det sker variationer av den kritiska frekvensen eftersom solens strålning varierar med årstid, tid på dygnet och solaktivitet. Variationen är flera tiopotenser större för den joniserande strålningen än för strålningen inom det synliga bandet. Strålningen bildas i samband med utbrott på solens yta, vilket oftast sker i områden nära de mörka ytorna, som kallas för solfläckar. Solfläckstalet anger förekomsten av dessa fläckar på solen. Talet varierar under en period med en cykel på cirka 11 år.

Atmosfärens och solstrålningens sammanställning gör att jonosfären får en struktur som består av ett antal joniserade skikt med något olika egenskaper, se figur 9. D-skiktet (cirka 70–90 kilometers höjd) svarar för de direkta förlusterna för radiovågen medan E-, F1- och F2-skikten (på cirka 90–800 kilometers höjd) ger den avböjning som möjliggör utbredning bortom

horisonten. F2-skiktet är det skikt som är mest signifikant för radiokommunikation. HF-vågor (3–30 MHz) kan utbreda sig över stora avstånd via jonosfären under de flesta tider på dygnet, men frekvensen måste anpassas till rådande förhållanden. Den högsta frekvens som kan användas får inte vara högre än att radiovågen säkert reflekteras ner till mottagaren. Utbredning med en enda reflektion via E-skiktet ger en maximal räckvidd på cirka 2 000 kilometer och motsvarande via F-skiktet cirka 4 000 kilometer. Med flera reflektioner kan man få räckvidder som täcker hela jordytan.

Förlusterna vid jonosfärutbredning beror dels på avståndet, dels på dämpningen i jonosfären. Ju högre frekvens man använder desto lägre blir den senare dämpningen.

Reflektioner från de olika skikten (flervägsutbredning), liksom vågor som utbreder sig genom flera reflektioner i samma skikt (flerhopsutbredning), ger interferens mellan dessa vågor. Det jordmagnetiska fältet gör dessutom att jonosfärplasmat blir dubbelbrytande och man får två vågor som utbreder sig på något olika vägar. Vågorna sätts ihop till en våg vid utträdet ur jonosfären. Den här vågen har en varierande, vanligen elliptisk, polarisation som kan fädas på grund av rörelser hos jonosfären.

Vid större avvikelser från den normala jonosfären talar man om jonosfärstörningar. Dessa har sin uppkomst i händelser på solen och kan vid

kraftig ökad absorption slå ut all HF-kommunikation, fenomenet vid klart väder kan observeras som norrsken. Exempel på detta:

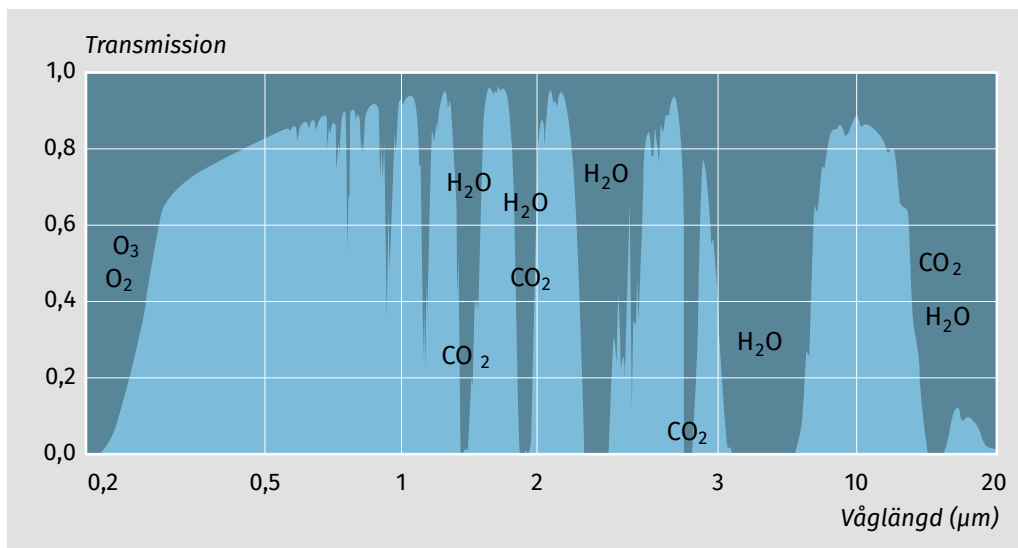
- Jonosfärstörningar är långvariga störningar på flera dygn som gör att F-skiktets kritiska frekvens först ökar något under en dag och sedan sjunker kraftigt följande dag för att sedan återhämta sig under ett antal dagar. Samtidigt kan absorptionen på låga frekvenser öka kraftigt. Fenomenet förknippas ofta med norrsken som i detta fall kan nå ner till de södra delarna av landet.
- SID (Sudden Ionospheric Disturbance) yttrar sig på HF-bandet som en snabbt uppträdande ökning av absorptionen, som kan sträcka sig från några minuter upp till någon timme. Absorptionen beror på ökad UV-strålning från solen och uppträder bara på den solbelysta sidan av jorden.
- PCA (Polar Cap Absorption) ger en mycket kraftig ökning av absorptionen, vilken kan slå ut all HF-kommunikation. Den uppträder några gånger per år på höga latituder och mest vid högt solfläckstal.

Förutom jonosfärstörningar påverkas HF-system mycket kraftigt av de interferenser som beror på att många radiostationer världen över måste dela på ett relativt litet frekvensutrymme. Det är därför svårt att hitta frekvenser som är ostörda under längre tid.

Optisk vågutbredning

Optisk vågutbredning i atmosfären påverkas av en mängd fysikaliska processer. Det innebär att räckvidd och prestanda för optiska system beror på tillståndet i atmosfären, det vill säga vädret och variationer i höjd, luftfuktighet, tryck, temperatur och turbulens samt förekomsten av partiklar. Atmosfärens transmission är också i högsta grad beroende av våglängd, vilket framgår av figur 10. Vissa våglängdsband (fönster) har låg dämpning och används av elektrooptiska system som skall verka i atmosfären.

I figur 10 syns från vänster UV-bandet som övergår i det visuella området (VIS) vid våglängden $0,4\ \mu\text{m}$ och som i sin tur övergår i det nära infraröda (NIR, $0,7\text{--}1,1\ \mu\text{m}$). Därefter följer det kortvågsinfraröda bandet (SWIR, $1,1\text{--}2,5\ \mu\text{m}$), det mellanvågsinfraröda bandet (MWIR, $3\text{--}5\ \mu\text{m}$) och det långvågsinfraröda bandet (LWIR, $8\text{--}12\ \mu\text{m}$). Man kan se att de är tydligt avgränsade i olika spektrum. MWIR- och LWIR-banden har delvis olika egenskaper, men framför allt stora likheter. De utnyttjas i



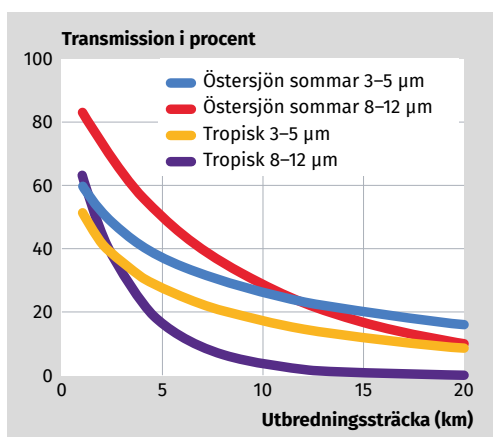
Figur 10. Exempel på en beräknad transmissionskurva inom det optiska området för en sträcka på 1 km, 10 m över markytan. De gaser som orsakar dämpning anges i figuren.

mycket stor utsträckning för sikten och övervakning. När man väljer våglängd för ett avbildande system bör hänsyn tas till geografisk plats och vädret. Anledningen är att transmissionen starkt dämpas av vattenånga, vars koncentration varierar både på grund av geografi och årstid. För att illustrera detta visas i figur 11 transmissionen i MWIR och LWIR för Östersjön respektive tropiskt farvatten. Detta visar att ett elektrooptiskt system som ska användas i Sverige kan vara direkt olämpligt i miljöer med annan atmosfär.

Absorption, spridning (och reflektion), emission, turbulens, brytning (refraktion) och polarisation är fenomen som påverkar prestanda hos elektrooptiska system.

Atmosfären innehåller gaser och partiklar som dämpar den elektromagnetiska strålningen genom absorption och spridning. Inom optiken sammanfattas det i begreppet extinktion (utsläckning). Dämpningen beror på atmosfärens tryck, temperatur och koncentrationen av gaser och partiklar. Var och en av dessa parametrar kan variera kraftigt beroende på höjd, tidpunkt och geografiskt läge.

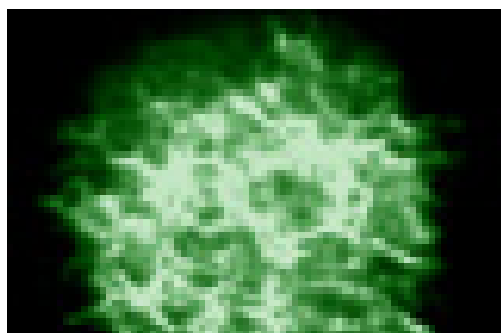
Spridningen sker antingen via molekyler (Rayleighspridning) eller aerosoler. Aerosoler är partiklar som svävar i atmosfären och påverkar dämpningen inom hela spektrumet, men kraftigast i UV-området (0,1–0,4 μm) och det visuella området (0,4–0,7 μm). Spridningen av molekyler är oftast så liten att den går att bortse från, förutom när det gäller UV-ljus.



Figur 11. Transmission för Östersjön och tropiskt farvatten vid två olika IR-band.



Figur 12. Bilder av upplösningstavlor vid låg (a) respektive hög turbulens (b).



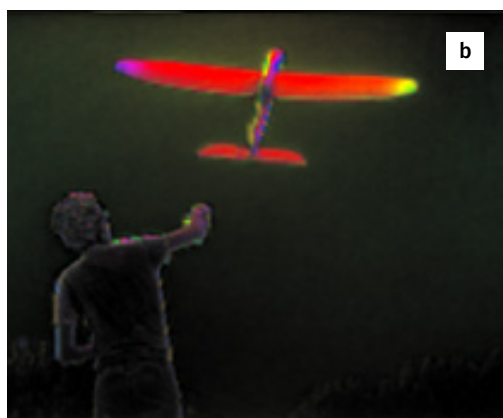
Figur 13. Intensitetsfördelning för en initialt symmetrisk laserstråle efter utbredning genom en turbulent atmosfär.

Absorptionen kan delas in i linje- och kontinuumabsorption. Gaserna i atmosfären, som till största delen består av kväve (N_2) och syre (O_2), absorberar strålning i olika grad. De flesta gasers andelar av atmosfären är ganska konstanta, men vissa kan variera starkt, speciellt vattenånga och ozon (O_3). Koncentrationen av koldioxid (CO_2) varierar med årstiderna och den långsiktiga trenden visar en ökande koncentration.

Vattenånga är den gas som påverkar mest eftersom mängden varierar mest i atmosfären. Vattenånga och koldioxid absorberar mycket infraröd strålning (IR-området 0,7–14 μm). Inom IR-området gör mängden vattenånga i atmosfären att mindre strålning släpps igenom. Mängden ozon i atmosfären är mycket liten, men den begränsar ändå UV-strålningen. Högre upp i atmosfären finns mer ozon som är av stor betydelse eftersom gasen hindrar solens skadliga UV-strålar från att nå marken. Vid korta våglängder dämpas strålningen även av syre som begränsar transmissionen längst ner i UV-området. Generellt kan atmosfärstransmissionen sägas avta exponentiellt med avståndet.

En gas kan både absorbera och stråla starkt vid samma våglängd. När gaser emitterar strålning ger det en bakgrundsstrålning inom det optiska området. För att kunna detektera ett mål fordras en viss kontrast mot bakgrunden. Om bakgrundsstrålningen är stark eller innehåller stor intensitetsvariation, försvåras måldetektionen. Så är fallet t.ex. vid sjöklotter, där rörelser i havsytan fläckvis reflekterar solstrålning in i detektorn.

Turbulens är luftrörelser som skapar en icke-enhetlig struktur med celler av olika storlek där luften har olika brytningsegenskaper. Strålningen som passerar dessa celler påverkas både i riktning och i intensitet. Turbulensen varierar kraftigt med tiden på dygnet och årstiden samt den geografiska platsen. Turbulens ger sämre bildskärpa i avbildande optiska system, se figur 12, och gör att objekt i en bildserie ser ut att röra sig slumpmässigt (bilddansning). Detta syns även tydligt i figur 3 i kapitlet Inledning där turbulensen orsakas av flygplanets jetstråle. Turbulensen ger också upphov till scintillation där inten-



Figur 14. Fotografi av en drönare tagen med en polarisationskänslig LWIR-kamera. I (a) visas en intensitetsbild och i (b) graden av polarisation på strålningen.



Figur 15. Hägringseffekter över hav. Foto: Carolina Ståhlberg.

sitetsfördelningen hos en laserstråle får slumpmässiga variationer, se figur 13.

Hur ljuset polariseras efter att det har spritts, reflekterats eller emitterats kan ge extra information om geometri hos avbildade mål. Den informationen kan komplettera intensitetsbilder, som mäter ljusstyrkan från konventionella kamerasensorer. Skrovlighet och lutning (ytorientering) är två egenskaper hos fasta objekt som starkt påverkar hur ljuset förändras när det reflekteras från eller passerar ett objekt (polarimetrisk signatur). Detta kan användas för att särskilja konstgjorda (ofta släta) föremål mot en naturlig (ofta oregelbunden) bakgrund. Ett exempel visas i figur 14 som är tagen med en polarisationskänslig värmekamera som mäter infrarött ljus (LWIR-kamera). I (a) visas en intensitetsbild från en konventionell kamera och i (b) är områden med hög grad av polarisation färglagda. Värmestrålningen (termisk strålning) som kommer från drönarens släta yta är polariserad. Det skapar en kontrast mot den mer opolariserade bakgrunden.

Att en stråles utbredningsriktning ändras (refraktion) beror på att luftens brytningsindex varierar, se figur 15. I det optiska området är det framför allt temperaturen som påverkar den så kallade brytningsindexgradienten. Temperaturen kan ibland förändras mycket på olika höjder. Vid mirage (hägringsfenomen) kan extra mål framträda som en spaningsutrustning felaktigt kan låsa på. ■

Telekrig mot radio- kommunikationssystem

Radiokommunikationssystem

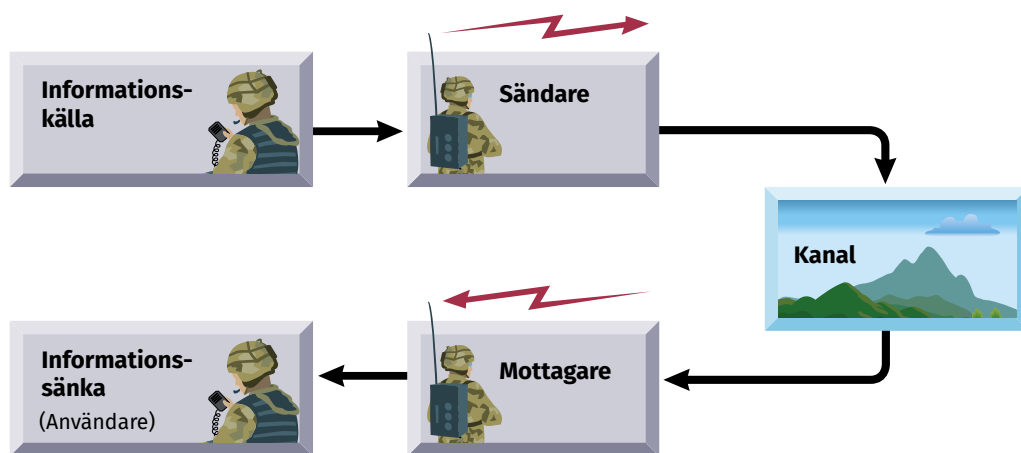
Ett generellt kommunikationssystem består av fem delar; informationskälla, sändare, kanal, mottagare och användare (informationssänka), se figur 16. Systemets uppgift är att överföra information från källan till användaren så fel-fritt som möjligt. Ett radiosystem kännetecknas av att informationen skickas med elektromagnetiska vågor över kanalen. Tabell 2 visar några viktiga egenskaper för ett antal militära och civila kommunikationssystem.

Sändare

En elektromagnetisk våg kan beskrivas med fyra parametrar; amplitud, frekvens, fas och polarisation. Om alla fyra parametrarna hålls konstanta blir vågen en ren oscillerande ton som kan representeras med en sinussignal. En sådan

ton innehåller ingen information, men genom att variera en eller flera parametrar kan information överföras. Detta kallas att modulera signalen. Det är emellertid ovanligt att polarisationen varieras. Den rena sinussignalen kallas vanligtvis för bärvåg eftersom den "bär" informationen.

Med analog modulation menas att den signal som modulerar bärvågen (basbandssignal) är analog, t.ex. signalen från en mikrofon. I processen ändras amplitud, frekvens eller fas hos den högfrekventa bärvågen proportionellt mot basbandssignalens svängning vid en viss tidpunkt (momentan amplitud). Beroende på vilken egenskap som ändras kallas det för amplitudmodulation (AM), frekvensmodulation (FM) eller fasmodulation (PM - Phase Modulation). AM och FM är de mest använda analoga formerna för



Figur 16. Generellt kommunikationssystem.

Tabell 2. Några systems egenskaper. Frekvenshopp och direktsekvens förklaras i avsnittet Frekvenser och vågformstekniker i kapitlet Inledning. OFDM (Orthogonal Frequency Division Multiplex) innebär att informationsmängden som sänds delas upp i flera parallella dataströmmar, där var och en sänds på en egen bärvåg med en lägre datatakt än den ursprungliga. Var och en av dataströmmarna moduleras med amplitud och/eller fas på en egen bärvåg och alla bärvågor skickas sedan samtidigt över kanalen. Resultatet blir en signal som är speciellt tålig mot flervägsutbredning och fädning.

System	Frekvensområde	Bandspridning	Kanalbandbredd	Högsta dataakt
HF2000 (kortvåg)	1,5–30 MHz	–	3 kHz	3,6 kbit/s
2G (GSM 900)	D: 935–960 MHz U: 890–915 MHz	–	200 kHz	14,4 kbit/s
Ra 180 (truppradio)	30–88 MHz	Frekvenshopp (FH) 100 hopp/s	25 kHz	16 kbit/s
RAKEL (Tetra)	D: 390–400 MHz U: 380–390 MHz	–	25 kHz	28,8 kbit/s
DRM	1,5–30 MHz	OFDM (228)	9 kHz	55 kbit/s
Ra90 (flygradio)	960–1 215 MHz	FH, 77 000 hopp/s Direktsekvens (DS)	3 MHz	115,2 kbit/s
Bluetooth gen 1	2 402–2 480 MHz	FH	1 MHz	723,2 kbit/s
Ra570	30–512 MHz	FH	50 kHz eller 1,2 MHz	–
DAB	174–240 MHz	OFDM (1 536)	1,536 MHz	1,7 Mbit/s
RL371 (radiolänk)	1 350–1 850 MHz	FH, adaptiv	125 kHz	2 048 kbit/s
RL 373	1 350–2 690 MHz	–	0,8–10 MHz	34 Mbit/s
3G (WCDMA)	D: 2 110–2 170 MHz U: 1 920–1 980 MHz	DS	5 MHz	42 Mbit/s
4G (LTE)	Flera frekvensområden mellan 450 MHz–3,5 GHz	OFDM	1,4–20 MHz	≈ 300 Mbit/s
5G NR	Flera frekvensområden mellan 450 MHz–28 GHz	–	3–100 MHz	≈ 10 Gbit/s
WiFi (IEEE802.11)	2 400–2 484 MHz 5,180–5,825 GHz 5,925–7,125 GHz	Orthogonal Frequency Division Multiplex (OFDM) (64)	20–320 MHz	23 Gbit/s

modulation. PM används främst när signalinnehållet är digitalt, det vill säga en bitström. Vid digital modulation består basbandssignalen av en ström av bitar, där varje bit antingen är en etta eller nolla. Flera bitar kan då bilda symboler, till exempel kan en grupp om tre bitar anta åtta olika värden ($2^3 = 8$). Symbolvärdet används för att karakterisera bärvågen.

Digitala sändare innehåller oftast också källkodare och kanalkodare. Källkodning plockar bort överflödiga information för att minska mängden information som måste överföras till mottagaren. I en digital bild är värdena i två på varandra följande bildelement ofta mycket nära var-

andra. Det tar då mindre plats att koda skillnaden mellan värdena i stället för att koda varje del för sig. Kanalkodaren tillför extra information till signalen så att eventuella störningar kan upptäckas och korrigeras i mottagaren. Enklaste formen av kanalkodning är att upprepa signalen tre gånger och låta mottagaren ta majoritetsbeslut för varje databit. Med hjälp av avancerad matematik kan bättre kanalkoder skapas.

Det finns ytterligare sätt att filtrera och optimera signalen. Ofta försöker man begränsa signalens effekt utanför sitt tilldelade frekvensband för att inte störa andra signaler. Det är vanligt med en kombination av amplitud-, frekvens- och

Radiolänk

En radiolänk är en radioförbindelse mellan två punkter. Ofta används antenner med mycket kraftig riktningsverkan. Det ökar inte bara kvaliteten på länken, utan minskar även risken för störning och avlyssning eftersom strålningsenergin koncentreras i rummet. Fasta radiolänkar har ofta höga master som bildar kedjor som kan överbrygga stora avstånd bortom horisonten.

Om sändaren eller mottagaren är rörlig måste antennerna följa rörelserna. Detta kan göras mekaniskt genom att fysiskt rikta om antennen. Om flera antenn-element används går det att påverka strålningsriktningen elektriskt genom att förändra fasan individuellt för varje antennelement. En elektriskt styrd antenn följer rörelserna snabbare än en mekanisk.



Figur F3. Radiolänkantenn. Foto: Peter Krans, Försvarets Materielverk.

fasmodulation. Mottagaren kan avkoda bitarna i signalen om varje unik kombination av amplitud, frekvens och fas motsvarar en egen signal, som tydligt skiljer sig från alla andra kombinationer.

Antenn

Sändarantennen överför växelström (ledningsbunden energi) till radiovågor (icke ledningsbunden energi). När en antenn kopplas till en mottagare sker det omvända och växelström överförs till mottagaren. Antennens uppgift är således att avge eller uppta energi.

Sändarantennen påförs effekt från sändarens slutsteg via någon form av ledning. Den energi som inte blir förlustvärme lämnar antennen i form av elektromagnetisk strålning. Den enklaste tänkbara antennen (isotrop antenn) strålar lika mycket i alla riktningar. En isotrop antenn är endast en hypotetisk punkt i rymden och går inte att realisera i verkligheten, men används som en matematisk referens. Verkliga anten-

ner omges inte av ett homogent strålningsfält, utan har mer eller mindre fokuserande egenskaper på strålningsfältet, s.k. riktverkan. En verklig antens förstärkning definieras som förhållandet mellan antennens effekttäthet i riktning med maximal strålning och effekttätheten hos en isotrop antenn. För ideala konstruktioner är det relativt enkelt att beräkna strålningsdiagrammet, men i verkligheten är en antenn alltid monterad på någon form av mekanisk struktur. Det gör det svårt att beräkna hur antennen kommer att stråla för en given installation.

En tumregel för praktiska sändare är att antennens fysiska storlek bör motsvara våglängden för bärvågen som antennen matas med. Det gör att så mycket som möjligt av den inmatade energin övergår i elektromagnetisk strålning.

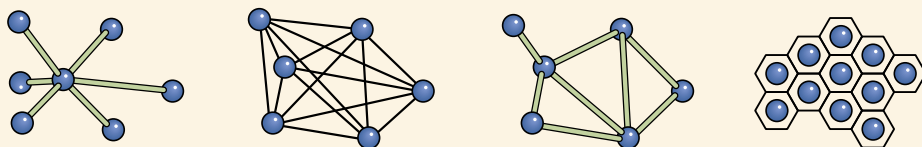
Mottagare

I radiokanalen kommer signalen att utsättas för oförutsedda störningar, som i huvudsak är brus,

Radionät

Ett radionät består av flera radionoder där varje nod oftast både kan sända och ta emot signaler. Nätets konfiguration beror på hur det tillämpas, se figur F4. Det centraliserade nätverket (stjärnnätet) har en centralt styrande nod. All trafik mellan två användare måste först passera centralnoden. Fördelen med ett sådant nät är att det är enkelt att styra och ger god yttäckning. Nätet är dock sårbart eftersom det är helt centralstyrt. Om den centralt styrande noden slås ut kommer nätet att sluta fungera.

I ett broadcastnät kan alla höra alla men bara en i taget kan sända. Det är ett fullständigt förbundet nät och alla noder i nätet har en koppling till alla andra noder. Nätet är relativt enkelt att styra och inte lika sårbart som det centraliserade, eftersom en centralt styrande nod saknas. Däremot kan det krävas att uteffekten är hög för att kunna nå en mottagare som befinner sig långt bort från sändaren.



Figur F4. Olika exempel på nätstrukturer. Från vänster stjärnnät, broadcastnät, flerhoppsnät och cellnät.

De ovan nämnda näten är av typen enkelhopp. Det betyder att kommunikationen sker direkt mellan sändare och mottagare. Nät som bara är delvis förbundna, men ändå kan förmedla trafik mellan godtyckliga noder, brukar benämnas mesh-nät eller ad hoc-nät. Trafiken förmedlas genom flera hopp mellan noder, vilket även kan benämnas flerhoppsnät. Då kan noder som är utom räckhåll för varandra ändå kommunicera genom mellanliggande noder som förmedlar informationen vidare. Den största nackdelen med ett flerhoppsnät är att styrningen av trafiken blir mer komplex.

Vårt mobiltelefonisystem är ett så kallat cellnät som är en hybrid mellan stjärnnät och flerhoppsnät. Varje cell är i sig ett stjärnnät och nätet som förbinder cellerna är ett flerhoppsnät.

fädning och interferenser. Brus kommer in från atmosfären och rymden via mottagarantennen. Dessutom alstrar de ingående komponenterna brus i mottagaren. Fädning innebär att signalens amplitud varierar över tiden, till exempel för att sändare eller mottagare rör på sig, så att radiokanalen förändras. Interferenser är andra signaler, antingen avsiktliga eller oavsiktliga, som

kommer in via mottagarantennen och påverkar nyttsignalen. Mottagarens uppgift är att ta emot den utsända analoga signalen även om denna innehåller störningar. Mottagaren är anpassad till den utsända signalen och ska omvandla den till information. Allt som görs på sändarsidan är till för att öka sannolikheten att mottagaren tolkar den mottagna signalen rätt.

Framtiden

Med hjälp av olika funktioner i mjukvaran kan radion anta olika profiler och kommunicera anpassat för skilda förutsättningar (mjukvaruradio). En radiosignals beskrivning (profil) brukar ofta benämnas vågform. Radiosystem med flera samtidiga vågformer ställer höga krav bland annat på kapaciteten hos processorn. Även arkitekturen hos hårdvaran måste vara flexibel om en sådan radio ska kunna implementeras. Samma hårdvara ska kunna återanvändas för flera olika kommunikationslösningar.

För att mjukvaruradion ska bli realiserbar krävs standardisering, öppna arkitekturer och gränssnitt, som är tydligt definierade. Samma

plattform ska kunna användas av militära, civila och kommersiella kommunikationssystem. Befintliga och nya radiosystem ska kunna existera på samma plattform. Det kräver genomtänkta lösningar, men också att befintliga resurser används mer kostnadseffektivt.

Det finns behov av att kunna kommunicera med lokala myndigheter och civila organisationer via olika kommunikationsnätverk och radiostandarder. Med en mjukvarudefinierad radio (Software Defined Radio, SDR) går det, liksom med en vanlig dator, att ladda ner olika applikationer. Det ger en flexibel och säker radiolösning som är väl anpassad för försvarets framtida kommunikationsbehov.

Elektromagnetisk stödverksamhet

Taktisk signalspaning mot radiokommunikation handlar om att lyssna på motpartens radiosändningar för att få fram så mycket information som möjligt. Även om innehållet är krypterat går det ändå att dra taktiskt viktiga slutsatser. Figur 17 illustrerar ett exempel när det geografiska läget för en soldat och en stab bestäms med hjälp av krysspejling. Vanliga uppgifter för ett taktiskt signalspaningssystem är:

- lägesbestämning av radiosändare
- typbestämning av radiosändare
- knytning av radiosändare till plattform eller plattformstyp och förband
- analys av motsidans kommunikationsstruktur
- analys av informationsinnehållet i sändningen.

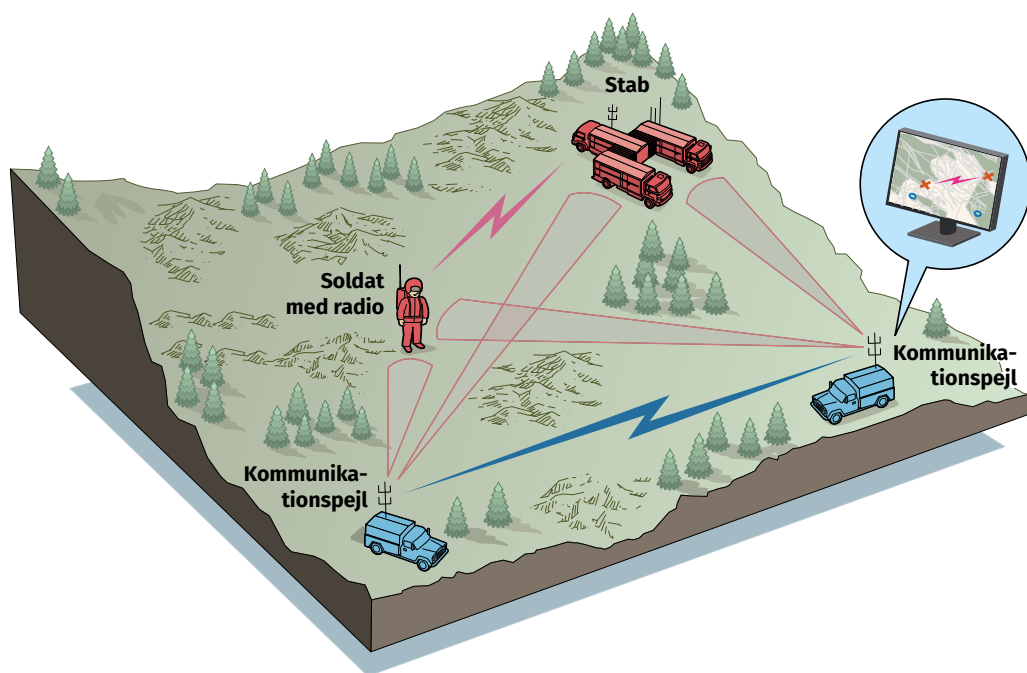
Det är vanligt att använda krypterad information i radiosändningar. Vid taktisk signalspaning mot radiokommunikation liknar arbetssättet signalspaning mot radar. I stället för att dra slutsatser om motsidans avsikter genom informationsinnehållet i sändningen tittar man främst på tekniska parametrar och sändningsmönster hos radiosystemet eller nätverket av radiosystem. I kombination med förkunskaper kan detta

bidra till en lägesbild som sedan ligger till grund för taktiska beslut.

Ett exempel på signaler som inbjuder till analys av kommunikationsstrukturer är då ett fartyg sänder information till övriga fartyg i samma grupp som i sin tur kvitterar det mottagna meddelandet med en kort sändning. En taktisk signalspaningsenhet kan med hjälp av radiopejling direkt se var fartygen befinner sig och hur många fartyg som finns i gruppen. Med hjälp av analys av radiosignalen och tidigare kunskap om sändarsystem på motsidans plattformar kan sändningarna även ge kunskap om typ av fartygsgrupp och vilket hot den utgör för egna enheter i närområdet.

Den taktiska signalspaningens bidrag till den gemensamma lägesbilden kan vara var motståndaren har sina enheter och deras rörelse, vilka förband och vapensystem det rör sig om samt var eventuella ledningsplatser befinner sig.

Signalspaning mot kommunikation sker även under strategiska tidsperspektiv (dagar, veckor, månader eller år), där tiden medger djupare analys av de mottagna signalerna. Här går gränsen mellan telekrig och signalunderrättelsetjänst då ett större arbete läggs på informationsutvinning, men även på karakterisering av nya



Figur 17. Lägesbestämning av motsidans radiokommunikation sker genom kryssspejling från samverkande pejlar. Detta ger information om enskilda enheters läge och eventuellt om sambandsnätets uppbyggnad. Om radiosändaren kan identifieras och knytas till plattform eller enhet kan hotet mot egna enheter bedömas.

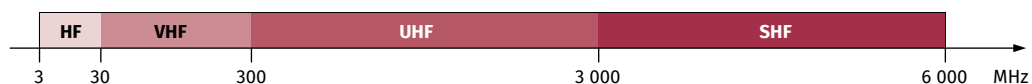
transmissionssystem samt analys av vilka plattformar sådana system är knutna till.

Räckvidder för radiosignalspaning

Taktisk signalspaning mot kommunikation bedrivs huvudsakligen mot frekvensbanden HF (kortvåg), VHF (ultrakortvåg), UHF (ultrahög frekvens) och på senare tid SHF (superhög frekvens). I figur 18 framgår hur dessa relaterar till varandra.

För VHF, UHF och SHF är antennhöjden avgörande för spaningsräckvidden då jordytans krökning skapar en radiohorisont, vid normal

atmosfärsutbredning. Vid flygspaning från hög höjd får man stor spaningsräckvidd. Från 3 000 meters höjd hamnar radiohorisonten på cirka 225 kilometer radie runt plattformen. Signalspaning från en obemannad flygande farkost på 500 meters höjd har i motsvarande fall möjlighet att upptäcka en radiosändare inom en radie av upp till cirka 95 kilometer. En markbunden signalspaningsenhet med pejlantennen i en 20 meter hög mast har ett avstånd på upp till 20 kilometer. Räckvidden kan bli längre om sändaren har en högre antennhöjd, men kan även vara lägre om bruset överröstar sändaren.



Figur 18. De vanligaste målfrekvenserna för taktisk signalspaning ligger i frekvensbanden HF, VHF, UHF och SHF.

Beroende på jonosfärens inverkan ser vågutbredningen på HF-bandet väsentligt annorlunda ut än på de högre frekvensbanden (se även vågutbredningskapitlet). Vid utbredning genom jonosfären bryts radiosignaler i den lägre delen av kortvågsbandet ner mot markytan igen. Det kan ge upphov till mycket långa förbindelseavstånd. Likaså kan en signalspanare på kortvågsbandet uppfatta radiosignaler på mycket långa avstånd, utan att för den skull behöva lyfta upp sin spanningsantenn från marken. Dock kan det uppstå en lucka utan mottagning från området nära mottagaren (ett antal tiotal mil) ut till reflektionen från jonosfären. Detta område ligger inom den så kallade skipzonen.

Uppbyggnad av ett radiosignalspaningssystem

Ett signalspaningssystem består av flera samverkande delar men i grunden finns en antenn, en radiomottagare och någon form av signalbehandling (analog eller digital). Moderna telekrigssystem för radiokommunikation är i stor utsträckning mjukvarubaserade och kombinerar oftast både signalspaning och störning i samma hård- och mjukvara.

I figur 19 illustreras ett telekrigssystem i olika block som utgår från ett modernt digitalt system som behärskar både signalspaning och störning. Beskrivningen är ett exempel och uppbyggnaden kan se annorlunda ut.

Antenn

Antennen omvandlar elektromagnetiska fält till växelström (och vid sändning sker det omvända). I ett system med pejling av radiokommunikation består ofta antennen av flera enskilda antenn-element. Dessa element är anpassade i längd och diameter samt inbördes placering till frek-

vensområde och vilken typ av inmätningss metod som ska användas.

Mottagare

Mottagaren i ett system för signalspaning har en begränsad bandbredd och digitaliserar växelströmmen från antennen. En mottagare som används för radiopejling har oftast lika många kanaler för digitalisering som enskilda antenn-element.

Hårdvarunära signalbehandling

Telekrigssystem har ofta en betydande bandbredd som behöver signalbehandlas. För att undvika flaskhalsar i dataöverföring görs först en hårdvarunära signalbehandling som förädlar informationen till en lägre dataakt som kan hanteras av senare mjukvarulager. Enskilda signaler separeras och ofta utförs signalbehandlingen på en programmerbar grindmatris (FPGA). Slutresultatet kan både vara en digital bitström och metadata i form av signaldeskriptorer. Dessa innehåller aggregerad information om en signal, till exempel bandbredd, sändningstid och ankomstriktning.

Ett exempel på reduktion är ett system med fyra antennkanaler med 200 MHz bandbredd som kan användas samtidigt (momentan bandbredd) och ett djup på 16 bitar. Datatakten blir då 25,6 Gbit/sekund innan signalen har behandlats. Anta att 15 olika sändare använder samma frekvensband, och varje sändare använder 50 kHz. Med hårdvarunära signalbehandling kan de 15 bitströmmarna skiljas ut från den totala bandbredden. Datatakten minskas till 96 Mbit/sekund. Om signaldeskriptorer används i stället reduceras informationen ytterligare till i storleksordningen 100 byte. Denna information kan skickas vidare till mjukvarulagret.



Figur 19. Exempel på schema över ett signalspaningssystem.

Mjukvara och kommunikation

I mjukvarulagret kan mer komplex signalbehandling utföras, men den kräver inte samma beräkningskraft som en grindmatris. Exempel på funktioner i mjukvarulagret är klassificering av radiosignaler, lägesbestämning med datafusion samt målföljning. Mjukvarulagret nyttjas också ofta till att styra och konfigurera ingående delar i systemet och hanterar även inspelning av signaler.

Mjukvarulagret hanterar även kommunikationen mellan sensorer som ingår i ett sensornätverk. En ensam pejlighet kan sällan lokalisera en sändare eftersom det endast i undantagsfall går att uppskatta avståndet till sändaren. Därför behöver pejligheter samverka med andra pejligheter för att kunna bestämma ett geografiskt läge. Inom ett mobilt, taktiskt signalspaningssystem upprättas sambandet oftast med hjälp av radiolänk.

Användargränssnitt

Ett väl utformat användargränssnitt gör det möjligt för användare att ta del av information och styra telekrigssystemet.

Användaren kan till exempel välja frekvensband, konfigurera detektorparametrar och skapa pulsfiler. Informationen som användaren ser kan till exempel vara en översikt över spektrumet och en karta över lägesbestämda sändare. Ofta finns även en möjlighet att skapa spaningsrapporter och interagera via ett ledningssystem.

Det förekommer också att telekrigssystemet kan fjärrstyras. I de fallen kan användargränssnittet köras på en separat dator som har en nätverksförbindelse med mjukvarulagret i systemet.

Figur 20 illustrerar ett exempel på utsnitt av ett användargränssnitt med ett frekvensspektrum som innehåller en LTE-basstation (Long-Term Evolution är en standard för mobiltelefoni).

Målsignaler för radiosignalspaning

Fixfrekvenstrafik

En vanligt förekommande typ av radiosignal är fixfrekvenssändare. Hit kan all radiotrafik som sker med signalering på en fast frekvens räknas.

För signalspaning mot fixfrekvenssystem med långa sändningstider kan ofta smalbandiga pejlar

med hög känslighet användas. I en smalbandig pejl blir signalen tydligare i förhållande till bruset, vilket gör att riktningen till signalen kan bestämmas mer exakt.

Frekvenshoppande radiosändare

Frekvenshopp ger ett skydd mot störningar, men det är inte ett effektivt sätt att undgå lägesbestämning med signalspaning. Även snabba frekvenshoppare har ett begränsat antal kanaler, där sändningen återkommer med till synes slumpmässiga intervall. En smalbandig pejl kan bevaka någon av de kanaler som används och samla på sig bäringsdata från de korta sändningar som faller inom kanalen. En modern bredbandig pejl klarar ofta även att lyssna på hela bandet samtidigt, dock med lägre dynamik än en smalbandig mottagare. Se även avsnittet Frekvenser och vågformstekniker i kapitlet Inledning.

Eftersom många frekvenshoppande sändare vid olika tillfällen använder samma band är det viktigt att samverkande pejlar är synkroniserade med varandra för att möjliggöra lägesbestämning. Synkroniseringen kräver precision på mikrosekundnivå.

Direktsekvensspridda radiosändare

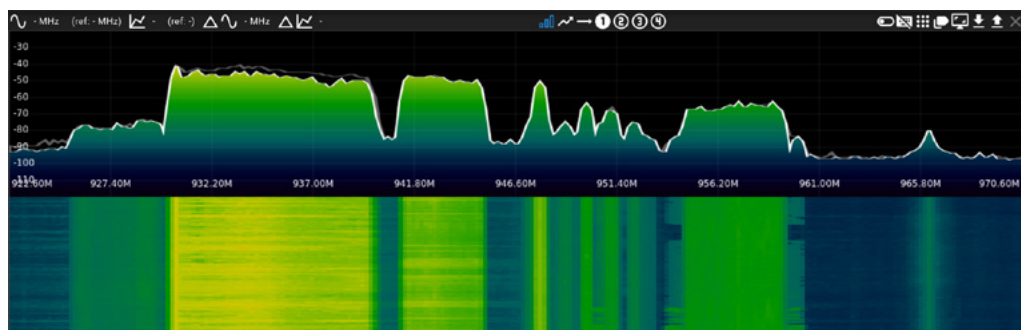
För att hantera den här typen av sändningar används ofta korrelationsteknik mellan två eller flera spaningsmottagare. Se även avsnittet Frekvenser och vågformstekniker i kapitlet Inledning.

Multicarrier

För signalspaning innebär multicarrier att en enskild bärvåg kan se ut som en kanal med låg datahastighet och låg effekt, medan hela multicarriersignalen framträder som ett block i frekvensspektrumet. Vid signalanalys kan spektrala korrelationsmetoder samt tids- och frekvensanalys vara nödvändiga för att skilja multicarriertrafik från annan bredbandig emission. Se även avsnittet Frekvenser och vågformstekniker i kapitlet Inledning.

Cellulära system

Cellulära kommunikationssystem, som GSM (2G), WCDMA (3G), LTE (4G) och NR (5G),



Figur 20. Exempel på användargränssnitt. I bilden syns ett effektspektrum med LTE-basstation.

använder ett nät av basstationer som täcker geografiska områden uppdelade i celler. Flera användare kan använda radioresurserna, utan att störa varandra, genom att dela en kombination av frekvenser, tider och koder. Moderna system som 4G och 5G använder OFDM-baserad modulation (metod för att överföra stora mängder digitala data) samtidigt som resurser för dataöverföring tilldelas dynamiskt. När två enheter kommunicerar med varandra går signalen via en eller flera av basstationerna.

Signalspaning mot cellulära system kräver ofta bredbandiga mottagare och protokollanalys i kombination med metoder för geolokalisering för att identifiera och följa mobila enheter.

Tekniker för att bestämma riktning och läge

Ett viktigt mål med taktisk signalspaning är att hitta riktning till – och läge för – sändare.

Riktningsbestämning

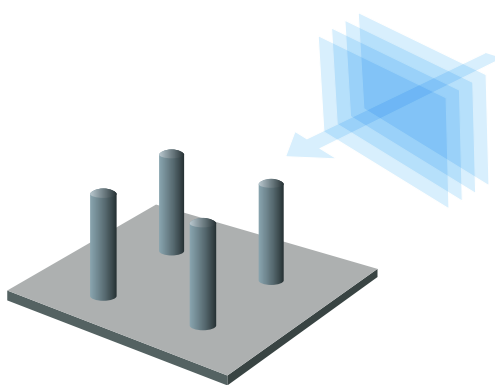
Ett enkelt sätt att bestämma riktning, som numera inte är så vanligt, är att vrida en riktanten mekaniskt tills den mottagna signalen är som starkast.

Genom att istället införa signalbehandling i systemet kan man med interferometri nyttja flera runtomstrålade antenner för att få riktningen till målet, se figur 21. Figuren illustrerar fyra vertikala antenner tillsammans med en infallande radiovåg. Radiovågen kommer att belysa antennerna med en liten tidsfördröjning som beror på infallsriktningen, ljusets hastighet och avstånden mellan antennerna. Tidsskillnaden ger en fasför-

skjutning av signalerna i respektive antennkanal. Genom att göra en uppskattning av fasskillnaden mellan kanalerna kan infallsriktningen beräknas. Metoden kräver att avstånden mellan antennerna är mindre än en halv våglängd för att ge en entydig riktning. Mer om detta finns i fakturatan om precisionsmetoder på sidan 35, under avsnittet långbasinterferometri.

Kryssspejling

Det enklaste och mest självklara sättet att bestämma ett läge är att pejla riktningen till sändaren från två olika punkter och se var linjerna som representerar riktningarna skär varandra. Metoden kallas för triangulering eller kryssspej-

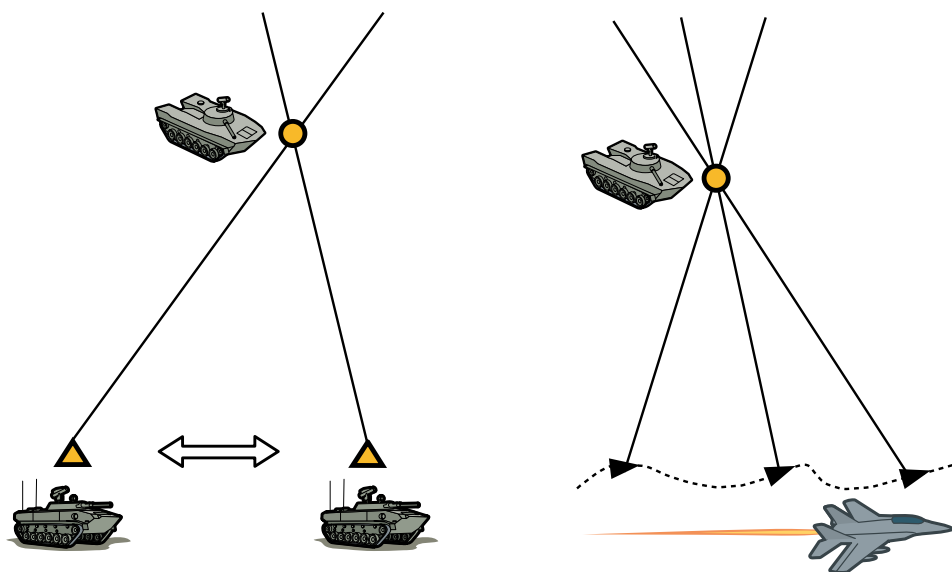


Figur 21. En infallande radiovåg och fyra vertikala antenner. Skillnaden i gångväg till respektive antenn skapar fasskillnader mellan kanalerna från vilka man kan göra en uppskattning av infallsriktningen för vågen.

ling, se den vänstra delen av figur 22. Osäkerheten i uppskattningen av läget varierar beroende på sändarens läge i förhållande till signalspaningsplattformarna. För att få en bra skattning av läget på långa avstånd bör avståndet mellan signalspaningsplattformarna (pejlbasen) vara så långt som möjligt. Enkel geometri visar att osäkerheten i inmätt sändarläge blir mycket stor nära pejlbasens förlängning. Det blir minst osäkerhet när skärningen mellan de inmätta riktningarna är 90° .

Egentriangulering

Det är möjligt att använda en ensam rörlig plattform för att bestämma en sändares läge. Detta kallas egentriangulering och bygger på att skapa en mätbas genom den egna förflyttningen. Det högra exemplet i figur 22 visar egentriangulering där flygplanets bana utgör mätbasen. En förutsättning är att signalkällan är stationär eller endast rör sig långsamt och att den sänder under en tillräckligt lång tid eller är återkommande.



Figur 22. Två sätt att triangulera. Till vänster sker trianguleringen momentant med två samverkande pejlar. Till höger sker en egentriangulering, där en pejl kan bestämma läget för en fast sändare genom att förflytta sig mellan mätningarna av infallsvinkeln.

Precisionsmetoder för lägesbestämning

I många fall önskas en bättre lägesbestämning än vad som är möjligt med triangulering från pejlar som bygger på interferometrar. Detta kan åstadkommas med högre precision i riktningsmätningarna, längre mättid eller genom att använda så kallade precisionsmetoder. Till dessa räknas TDOA (Time Difference of Arrival), DDOA (Doppler Difference of Arrival) samt LBI (Long Baseline Interferometry).

TDOA (Time Difference of Arrival) eller tidsdifferensmätningar mäter skillnaden i ankomsttid för en signal mottagen av två eller fler mottagarstationer som är skilda åt i rummet. Varje par av stationer ger en tidsdifferens och man kan då räkna ut en kurva (hyperbelgren) på vilken sändaren befinner sig. Dessa hyperbelgrenar skär varandra i den punkt som sändaren befinner sig i, men i många fall även i en punkt som ger ett falskt läge. Problematiken med ett falskt läge kan lösas med en extra inhämtningsenhet. Tekniken ställer höga krav på tidssynkronisering i signalspaningsplattformarna, något tiotal nanosekunder.

DDOA/FDOA (Doppler/Frequency Difference of Arrival) bygger på de frekvensförändringar som uppkommer när det finns en relativ rörelse mellan emitter och signalspaningsplattform. En dopplerdifferens mätt mellan två punkter resulterar i en skillnad på en isodopplerslinje. Denna beskriver alla punkter som kan ge upphov till skillnaden. Linjen kommer att ha olika form beroende på hastighetsvektorerna vid tidpunkterna för mätningarna. Med ytterligare en mätning kan en linje till skapas och skärningen mellan dessa pekar ut emitterns läge.

LBI (Långbasinterferometri) bygger på mätning av fasskillnaden mellan två mottagarkanaler. Till skillnad från annan, vanlig eller konventionell, interferometri är mätbasen – avståndet mellan antennerna – vanligtvis betydligt längre än en halv våglängd. Den långa mätbasen i kombination med att det inte är möjligt att mäta fas i ett större intervall än 360° gör att långbasinterferometern blir mångtydig. Det innebär att flera infallsriktningar ger samma skillnad mellan faserna (fasdifferens). Genom att mäta fasdifferensen med täta intervall, samtidigt som signalspaningsplattformen rör sig, kan en historik över fasdifferenserna skapas. Historiken kan användas för att hitta de fassprång, där läget byter från -180° till $+180^\circ$ eller vice versa. Genom att kompensera för fassprången kan fasens förändring beräknas och ett läge bestämmas.

Elektromagnetisk attack

Det går aldrig helt att förhindra kommunikation, men den går att försvåra och fördröja så mycket att den saknar relevans när den kommer fram.

Ett fungerande, men energikrävande, sätt att störa radiosystem är att sända en kontinuerlig signal inom mottagarens frekvensområde. Signalen måste vara så stark att den hindrar målsystemet från att ta emot nyttsignaler. För att störningen ska bli exakt och effektiv måste den anpassas till sändning och mottagare. Störaren måste då klara av att upptäcka signalerna, generera en effektiv signal och använda den på ett bra sätt.

För att en signal ska kunna störas måste den först upptäckas av störsändaren eller annan taktisk signalspaning. Om det inte finns någon signal eller kommunikation på en viss frekvens finns det ingen anledning att försöka störa. Detta är en av grundtankarna i smygradiokoncepten. Med hjälp av modulation och kodning försöker kommunikatorerna hålla nere signaleffekten så att den inte upptäcks av den taktiska signalspaningen.

När signalering påvisas eller antas pågå måste störsändaren skicka ut en störsignal som är tillräcklig för att kunna slå ut informationen i mottagaren. Med andra ord måste målet vara inom störsändarens räckvidd. En störsändares räckvidd är inget absolut begrepp, utan en fråga om ett styrkeförhållande mellan trafiksignalen och störsignalen. Relativ störräckvidd (RSR) visar hur långt borta en störsändare kan vara i förhållande till avståndet till två kommunicerande radiostationer. RSR räknas ut som förhållandet mellan störavståndet och avståndet för trafiken, då kommunikationen precis börjar störas. En störsändare minskar således endast radiostationernas förbindelseavstånd, men ambitionen är att minska det så mycket att radiokommunikationen blir taktiskt oanvändbar.

Det räcker dock inte med att skapa en stark och effektiv störning, utan den måste också sändas ut på rätt frekvens vid rätt tidpunkt.

Störning av fixfrekvenssamband

För att vara effektiv måste störningen sändas på rätt frekvens vid rätt tidpunkt och vara så nära

mottagaren att signalen överröstar trafiken. Hur stor effekt som behövs är beroende av hur trafiksignalen är modulerad. Olika modulationssätt är olika svåra att störa. För vissa modulationssätt kan det vara tillräckligt att ha den starkaste signalen för att helt omöjliggöra kommunikation. För andra modulationssätt kan båda signalerna uppfattas samtidigt på en viss nivå. Då måste störsignalen vara mycket starkare för att helt dölja trafiksignalen.

Det är naturligt att välja olika modulationstyper för kommersiella civila applikationer och militär kommunikation. I det förra fallet är en ren fin signal viktigast. När det handlar om militära applikationer prioriteras i stället förmågan till informationsöverföring även i svår miljö.

Olika typer av störningar påverkar trafiksignaler på olika sätt. Generellt gäller att ju mer störningen liknar trafiksignalen desto mer effektiv blir den.

Störning kan sändas till exempel som brus, pulser eller repetition. I det senare fallet sänds trafiksignalen ut igen fast vid fel tidpunkt, vilket skapar förvirring hos mottagaren.

En störsignal som är alltför unik går att extrahera i mottagaren och återmata i motfas, för att därigenom dämpa störsignalen. Förfarandet kallas för ”cancellering” och används även för att samtidigt kunna sända och ta emot med samlokaliserade radiostationer.

För att skydda sig mot störning använder kommunikatorn olika former av kodning, som kan upptäcka eller korrigera utstörd information. Ju mer störskydd som önskas desto kraftigare koder måste användas. Det gör att en allt större del av den överförda bitströmmen upptas av kodning. Det betyder i sin tur att informationsmängden per tidsenhet minskar eftersom tillgången på bandbredd oftast är begränsad. En minskad kapacitet för informationsöverföring är precis vad störaren är ute efter.

Det är således svårt att i förväg beräkna verkan av en störning mot en digital förbindelse om den inte är känd i detalj. Även om utrustningen är kartlagd under fredliga förhål-

landen kan den ha andra egenskaper under ett skarpt läge. Under en insats måste störverkan alltid följas upp. Detta kan göras med taktiska signalspaningsenheter som analyserar om den störda förbindelsen verkar fungera eller inte. Ett alternativt sätt är att studera motsidans agerande. Förväntade reaktioner är:

- frekvensbyte
- förändringar i sändareffekt eller sändnings-sätt
- signaleringen upphör eller repeteras
- minskade förbindelseavstånd
- byte av modulationssätt eller sambandsmedel.

I förlängningen vill man givetvis nå taktiska eller operativa fördelar med sin störning.

Det finns en möjlighet att motsidan inte ens förstår att den är utstörd, utan tror att den uteblivna förbindelsen beror på tekniska fel på utrustningen. Ett annat scenario är att de som blir utsatta för störning låtsas som ingenting och hoppas på att störaren väljer ett annat mål istället.

Störaren bör även komma ihåg att (1) varje störinsats utbildar motståndaren i att skydda sig mot störning och att (2) störsändaren kan upptäckas, positioneras och bekämpas av motståndaren. Störning bör därför sättas in mycket restriktivt och endast då den kan ha förväntad taktisk verkan.

Störning av frekvenshopp

Vid störning av frekvenshopp kan störaren antingen följa med och endast störa på den använda kanalen eller störa bredbandigt över hela eller delar av det använda frekvensbandet.

Om störaren följer med i ett frekvenshopp måste kanalen som används mätas in och en störsignal hinna levereras till radiomottagaren innan tillräckligt mycket information har sänts på den nya kanalen. Om störaren lyckas eller inte beror på hopptakt, kodning, störarens snabbhet och de geografiska avstånden mellan trafiksändare, trafikmottagare och störsändare. En tumregel för yttäckande system, till exempel en arméradio, är att en störare kan följa med upp till 500–1 000 hopp per sekund. Vid snabbare takter måste stör-

sändaren komma in i förbindelsestråket mellan trafiksändare och mottagare för att hinna med.

Störning av direktsekvens

Generellt är bärvågsstörning, eventuellt pulsad på lämpligt sätt, den mest effektiva metoden för störning mot direktsekvens. Den kan dock enkelt filtreras bort i mottagaren och därför breddas normalt störsignalen, till exempel med brus.

Smart störning

Modern radiokommunikation karaktäriseras av hög flexibilitet. Anpassning till rådande förhållanden kan ske på olika sätt, till exempel genom att reglera uteffekt eller ändra kodning och modulationsform. Ofta krävs också noggrann tidssynkronisering mellan kommunicerande enheter. Flexibilitet och tidhållning styrs genom kontrollinformation som skickas tillsammans med nyttodata. Det sker normalt inom fasta tidsstrukturer. En smart störare som kan identifiera och påverka kontrollinformation kan uppnå samma verkan som en klassisk störare, men med betydligt lägre energiförbrukning.

Principer för störsändning

Störsändare kan delas in i två grupper:

- Fjärrstörsändare – stör enstaka förbindelser över stor yta.
- Närstörsändare – stör ut all mottagning inom en begränsad yta.

Sekventiell störsändning är den vanligaste metoden vid fjärrstörning mot fixfrekvenssamband. Störsändaren lyssnar med jämna mellanrum och väljer varje gång ut de mest intressanta signalerna, vilka därefter störs sekventiellt. Förfarandet med lyssningsluckor brukar kallas "look through".

Det går fortfarande att sända ut från en yta som är störd eftersom det endast är mottagningen som är påverkad.

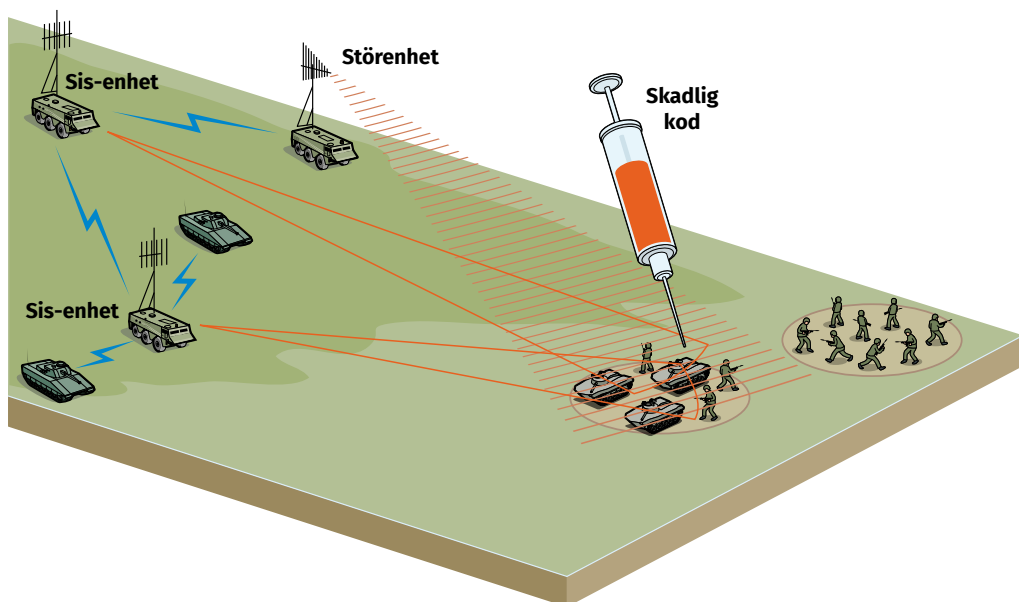
Samordning mellan telekrig och cyber

Cyber- och elektromagnetiska aktiviteter (CEMA) handlar om samordningen mellan telekrig och cyber. Den är inte enbart teknisk utan inkluderar också organisatorisk samverkan. CEMA på organisatorisk nivå kan handla om att telekrig- och cyberförband koordineras vid en insats. Ett exempel kan vara att en cyberoperation påverkar radioutrustning att sända med högre uteffekter så att spaning och positionering underlättas. På en teknisk nivå kan cyber och telekrig integreras för att ge ny förmåga. Ett exempel är att utnyttja information om detaljer i motståndarens radio-kommunikation för att uppnå en högre precision i både signalspaning och störning. Ett annat exempel på integrerad förmåga är att nyttja radiosignaler som bärare av nyttodata som exploaterar sårbarheter i IT-system.

För att ett modernt digitalt kommunikationssystem ska fungera krävs stora mängder administrativ kontrolltrafik, till exempel för tidssynkronisering, fysisk access, identitetshantering, autentisering, effektkontroll, förfrågningar och tilldelning av resurser. I kontrolltrafiken finns

information som kan överlagras på annan spänningsinformation och på så vis ge en mer högupplöst lägesbild. Informationen kan också inrikta störning mot särskilt känsliga delar av kommunikationen, se figur 23.

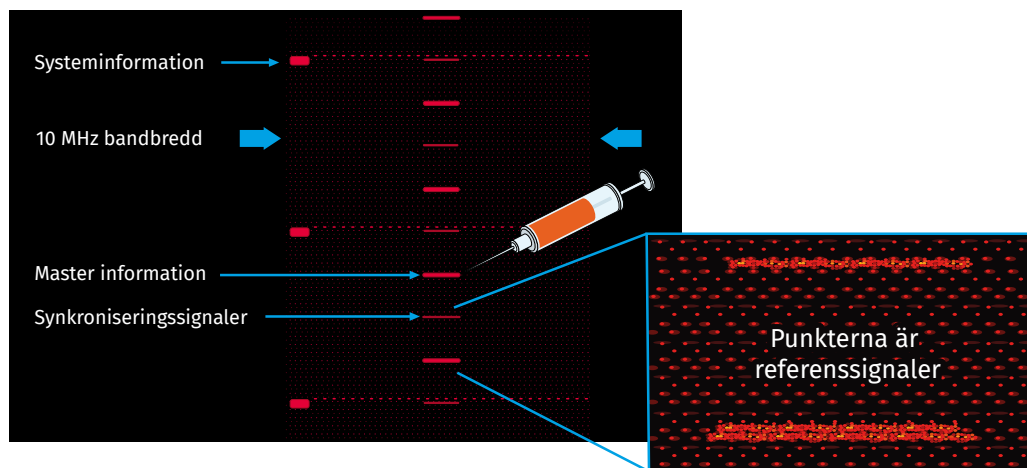
Ett mer konkret exempel på hur kunskap om en signal kan utnyttjas för att rikta in en störning ges i figur 24. Figuren visar en signal från en basstation i mobilsystemet 4G (LTE). Störsändare som endast har kunskap om frekvens och bandbredd lägger den största delen av sin energi på delar av spektrumet där de inte har någon effekt. En störsändare som kan avkoda och tolka signalen från basstationen får information om var referenssignaler finns och vilka synkroniserings-signaler som används. Genom att utnyttja denna information kan störsändaren fokusera sin energi på de mest kritiska delarna av signalen. Då kan nyttosignalen störas ut med en bråkdel av den effekt som skulle ha krävts om störeenergin hade spridits ut över hela frekvensbandet. En sofistikerad störsändare har även möjlighet att lägga in modifierad information i kontrolltrafiken för att påverka ytterligare.



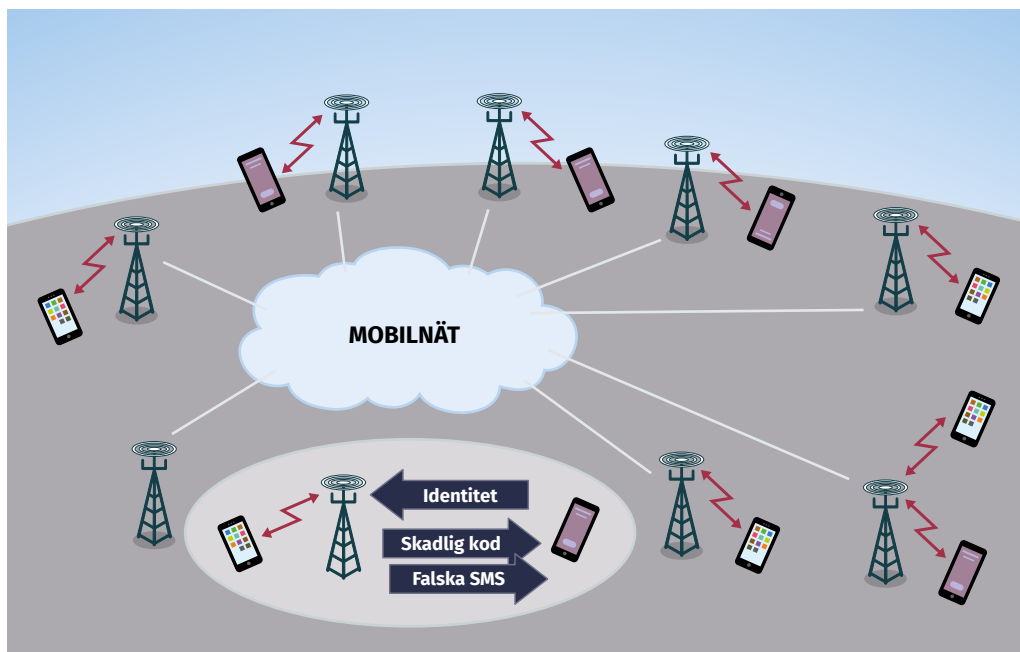
Figur 23. CEMA utnyttjar kontrolltrafik för att stödja spaning och inrikta störning.

Ett konkret exempel i LTE-fallet är när radio- och cyberförmågor tillsammans skickar förfälskade men korrekt utformade meddelanden med kommandon till mobila enheter för

att lura dem att sluta kommunicera med mobilnätet. Falska basstationer är ett annat exempel där radioförmågor kan nyttjas för att underlätta cyberattacker mot anslutna enheter, se figur 25.



Figur 24. Exempel från mobilsystemet 4G (LTE). En smart störning kan välja att endast fokusera på systeminformation eller synkroniseringssignaler



Figur 25. Falsk basstation med förmåga att läsa identitet från mobilen samt skicka skadlig kod och falska sms.

Protokoll och programvara kan sammanfattningsvis användas för att optimera störningar. Det är kunskap som normalt tillskrivs cyberområdet. Vice versa kan kunskap om att komma

åt systemens gränssytor, som annars är svåra att komma åt och som normalt brukar karakteriseras som telekrig, användas för att underlätta cyberattacker.

Elektromagnetisk protektion

Den utsända signalen kommer att utsättas för oförutsedda störningar, avsiktliga eller oavsiktliga. Det är viktigt att radiosystemet är robust mot störningar, vilket kallas för störskyddad kommunikation. Det är också viktigt att skydda kommunikationen från att upptäckas, till exempel av en signalspanare. Som för alla typer av skydd gäller att det alltid finns en grad av påverkan som kan bryta igenom skyddet.

Ett störskyddat kommunikationssystem är inte bättre än sin svagaste del. Det innebär att alla delar i radiosystemet (källkodning, kanalkodning, modulation och antenner) måste anpassas för störskydd. Dessutom behövs ofta komplettering med någon form av teknik för bandspridning för att skyddet ska fungera mot en intelligent störare. De vanligaste formerna av bandspridning är frekvenshopp och direktsekvens.

Frekvenshopp

Om frekvensbytena sker tillräckligt snabbt och systemet hoppar över tillräckligt stort frekvensband ger det ett gott skydd mot alla typer av störare. Med snabbt menas att hoppen måste ske ungefär lika snabbt som tiden det tar för signalen att gå mellan sändare och mottagare. Det hindrar så kallad följestörning där störaren först måste hitta aktuell frekvens och därefter ställa in och starta störaren. Tillräckligt stort frekvensband är då störaren inte har energi nog att störa så många frekvenser samtidigt att det skadar kommunikationen. Se även avsnittet Frekvenser och vågformstekniker i kapitlet Inledning.

Direktsekvens (Direct Sequence, DS)

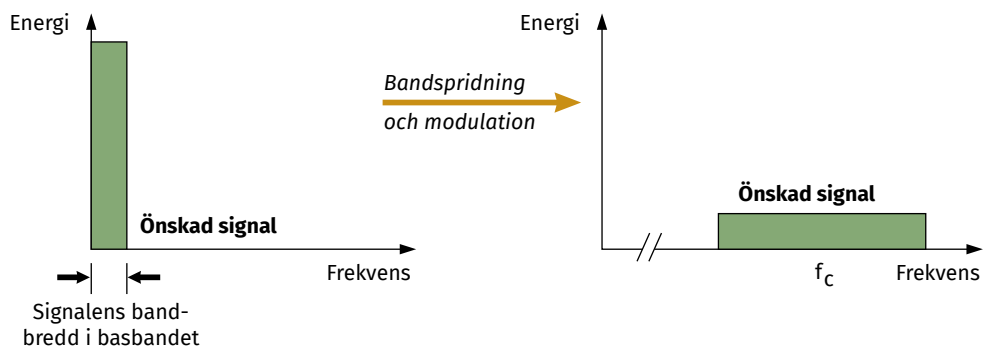
Vid mottagning av direktsekvens leder mottagarens ”avspridning” även till att alla andra signaler, inklusive störning, sprids. Figur 26 och 27

förklarar principen för direktsekvens. I nät med många användare används direktsekvens inte som skydd mot aktiva störare, utan som skydd mot andra användare i samma system. Alla sändare sänder samtidigt och på samma frekvens, men varje sändare har en unik kod för direktsekvensen. Mottagare som känner till en viss sändares unika kod kan skilja den från övriga sändare, vilka upplevs som brus. Se även avsnittet Frekvenser och vågformstekniker i kapitlet Inledning.

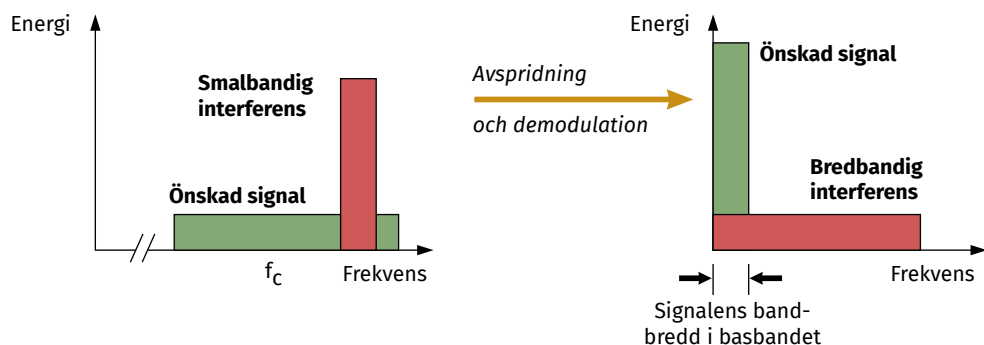
Smygradio

Med smygradio menas att kommunikationen är svår att upptäcka. En metod är att gömma sig i bruset med hjälp av stor bandspridning med direktsekvens, tillsammans med riktantenner och effektkontroll. Riktantennerna strålar endast i den riktning där mottagaren finns och effekten kontrolleras så att den är precis vad som behövs för kommunikationen. En annan metod går ut på att härma redan existerande signaler.

Ett alternativ till direktsekvensspridning är Ultra Wide-Band (UWB), även benämnd impulsradio, eftersom sändningen sker med extremt korta radiopulser. Typiskt är en pulslängd mellan 0,1 och 10 nanosekunder. Tekniken för impulsradio är lämpad för kommunikation på korta håll med låg uteffekt och korta räckvidder vilket gör den tålig mot smalbandiga interferenser och flervägsutbredning. UWB använder en bandbredd större än 500 MHz vid relativt höga frekvenser (i storleksordningen några GHz). Teknikens fördelar är bland annat höga datatakt, små användarterminaler och små antenner. UWB medger även kommunikation i tunnlar och slutna utrymmen. En möjlig militär tillämpning är detektion av föremål som finns inuti och bakom väggar. UWB



Figur 26. Figuren visar hur bandspridning och modulation påverkar en radiosignal. Till vänster visas signalen innan den bandsprids och moduleras, till höger signalen efter bandspridning och modulation. Resultatet blir att signalens effektinnehåll sprids ut över en större bandbredd centrerad kring bärvågsfrekvensen f_c .



Figur 27. Till vänster den önskade signalen (grönt fält) och en smalbandig interfererande signal (röd stapel) före avspridningen, till höger signalerna efter avspridningen. Avspridningen resulterar i att radiosignalens effekt koncentreras och den interfererande signalens effekt sprids ut i frekvens.

använder samma frekvensspektrum som existerande teknik. Det är möjligt eftersom signaleffekten sprids ut över ett stort frekvensområde. Eftersom UWB sänder över ett stort frekvensspektrum med låg uteffekt kommer andra samexisterande radiosystem att uppfatta UWB-signalen som brus.

I vissa frekvensområden dämpas radiosignaler extra mycket med avståndet. Det gör smygkommunikation möjlig. Anledningen är att signalen är i resonans med molekyler i luften. Det gör att energin i radiosignalen mycket snabbt

absorberas, till exempel lämpar sig radiokommunikation på 60 GHz väl för smygradio, eftersom radioenergin absorberas av syremolekyler i luften. Kommunikation som använder 60 GHz har kort räckvidd (några hundra meter vid fri sikt), vilket försvårar upptäckt och avlyssning av kommunikationen. För att kunna avlyssna sändningen tvingas en signalspanare befinna sig närmare sändaren, vilket ökar risken för upptäckt. Även någon som stör avsiktligt använder oftast samma frekvens och samma korta räckvidd och måste därför vara närmare sändaren.

Störning av satellitburna navigeringssystem

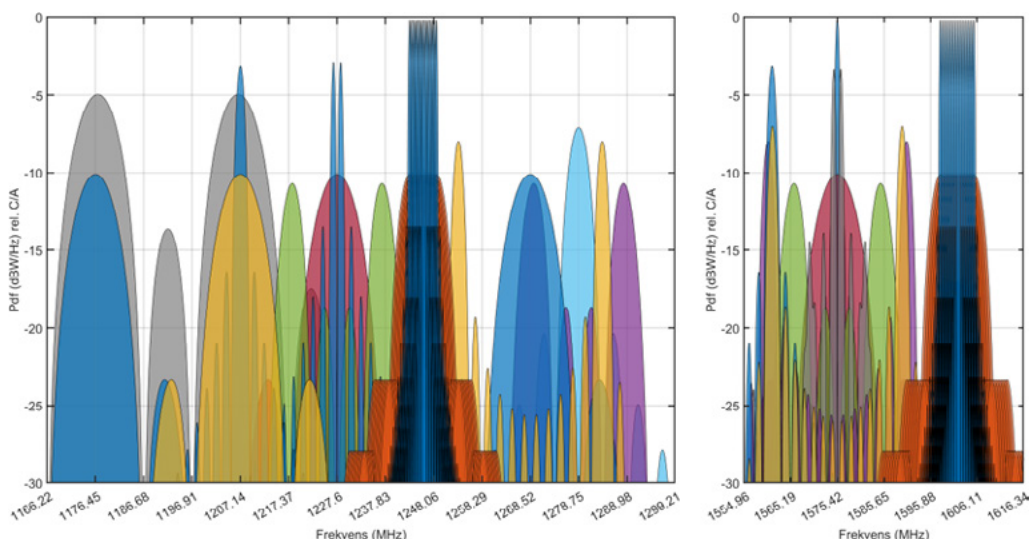
Navigeringsystem

Global Navigation Satellite System (GNSS) är ett samlingsnamn för alla navigeringssystem som bygger på satelliter med global täckning. I dag finns fyra oberoende satellitkonstellationer; amerikanska GPS, ryska Glonass, europeiska Galileo och kinesiska BeiDou. Varje GNSS har 24–32 satelliter i omloppsbanor runt jorden. GNSS-mottagare kan beräkna sin position, hastighet och tid (Position, Velocity and Time, PVT) genom att ta emot signaler från minst fyra satelliter från samma konstellation. Alla GNSS sänder både öppna och krypterade signaler på minst två frekvenser i två olika frekvensband, ett lägre mellan 1165 och 1300 MHz och ett högre mellan 1550 och 1620 MHz, se figur 28.

De öppna signalerna är avsedda för civilt bruk och används, förutom till positionering och navigering, också till tidssynkronisering av bl.a. elproduktion, mobilkommunikation och

datornätverk. Dagens civila samhälle har ett stort behov av tidssynkronisering för olika funktioner och GNSS erbjuder hög noggrannhet till en relativt liten kostnad. Krypterade signaler är främst avsedda för egen militär användning. I Europa kan även vissa myndigheter som polis, tull och kustbevakning få tillgång till krypterad Galileo (Public Regulated Service, PRS). Allierade till ägarna av respektive GNSS ges ofta tillgång till de krypterade signalerna. Sverige är ackrediterad användare av både militär GPS och Galileo PRS.

Moderna civila mottagare tar samtidigt emot flera signaler från flera satellitkonstellationer (Multi Constellation, MC) på flera frekvenser (Multi Frequency, MF). MCMF-mottagare ger både högre tillgänglighet och bättre PVT-lösning. Trenden är att även militära mottagare tar emot fler signaler på fler frekvenser. I Europa pågår utveckling av mottagare som samtidigt tar emot militär GPS och Galileo PRS.



Figur 28. Spektrum för alla GNSS-signaler som sänds 2025 där öppna signaler visas i blå eller grå färg. Alla övriga signaler är krypterade.

Störning

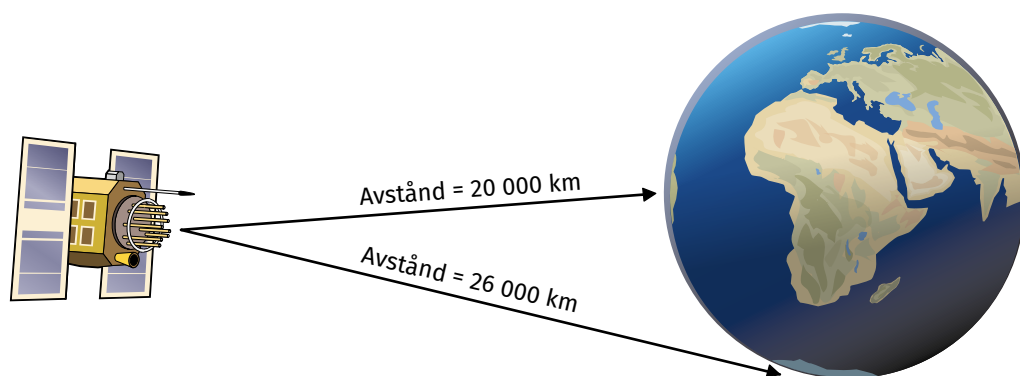
Satellitensignaler sänds på fasta frekvenser och använder teknik för direktspridning. De har teoretiskt ett ganska bra störskydd och tål störning som är betydligt starkare än nyttosignalen. Men signalerna som når jordytan är mycket svaga eftersom satelliterna befinner sig mycket långt bort, cirka 20 000 kilometer över jordytan, se figur 29. Styrkan på signalen som mottas på jordytan är 16–27 dB svagare än det naturliga bakgrundsbruset och merparten av vinsten med direktsekvenstekniken behövs för att över huvud taget kunna detektera signalen. Därför är det inte speciellt svårt för en störare att få ett effekttövertag jämfört med satellitsignalerna även på relativt stora avstånd. Det svåra är att om störaren inte vet exakt vilka signaler som en GNSS-mottagare använder, måste samtliga signaler störas samtidigt på en total bandbredd av cirka 200 MHz.

Störsändare finns från små, enkla sändare som endast stör på en frekvens med 10–100 mW upp till stora, bredbandiga med ut effekter på flera kW. De mindre används oftast lokalt med litet behov av räckvidd. Stora sändare används för större

områden eller när det är långa avstånd till målen. Det kan handla om att påverka motståndarens förmåga till precisionsbekämpning, men även om att störa ledningsfunktioner som ofta har ett GNSS-beroende. Störningar på GNSS-banden är vanliga och störsändare används långt utanför krigsskådeplatser. Användning riktad mot civil verksamhet förekommer i Sverige och vårt närområde. Det kan ses som ett aktivt exempel på hybridkrigföring.

Vilseledning genom att sända falska satellitsignaler (spoofing) är i dag känd och relativt lätt-tillgänglig teknik. En modern mjukvarudefinierad radio (Software Defined Radio, SDR) kan skapa alla öppna GNSS-signaler med godtyckligt informationsinnehåll. Mjukvara för att generera GNSS-signaler med en SDR finns på nätet. Om en falsk signalering är lyckad räknar mottagare fram den PVT-lösning som störaren bestämt. Om det inte finns något stöd från andra sensorer går det endast att skydda sig mot falsksignalering genom att förlita sig på krypterade signaler. Det är bara möjligt för vissa användargrupper.

Att sända satellitsignalen igen eller repetera den (meaconing) ändrar inte informatio-



Figur 29. Signalerna från satelliterna är 16–27 dB svagare än det naturliga bakgrundsbruset när de når jordytan.

nen och påverkar inte heller krypteringen. Det är möjligt, men generellt ganska svårt, att lyckas med en återutsändning. När det sker räknar en GNSS-mottagare fram positionen för återutsändarens mottagarantenn i stället för positionen för sin egen antenn. Det är mycket svårt att skydda sig mot återutsändning om signalen når mottagaren, utan stöd från andra sensorer.

Störskydd

Gruppantenn teknik för att undertrycka signaler är ett bra skydd mot både störning och vilseledning (falsksignalering och återutsändning) som inte kommer från satelliterna. Skyddssystemet kallas ibland CRPA (controlled radiation pattern antenna). Antennen anpassas så att den tar emot mindre signal från det håll där störningen kommer. Antennen består av flera antennelement och signalen når dem vid olika tidpunkter, vilket gör att signalerna hamnar i olika fas jämfört med varandra. Genom att justera amplitud och fas för varje antennelement kan signalerna förstärkas eller undertryckas i olika riktningar med positiv eller negativ interferens (lobformning). Antennendiagrammet kan alltså styras via lobformning så att antennförstärkningen är hög eller låg i en önskad riktning.

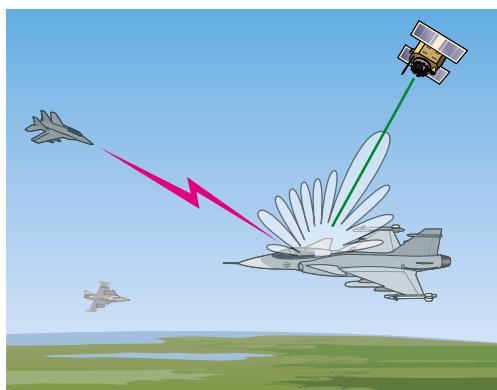
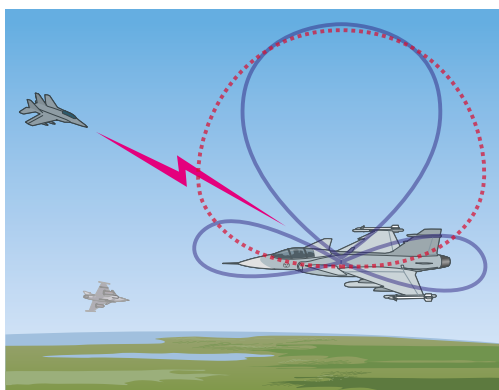
Teoretiskt kan ett skyddssystem med n stycken antennelement undertrycka $n-1$ störriktningar.

Det beskrivs i figur 30. Om det finns satelliter i samma riktning som störsändare dämpas även satelliternas signaler, men förhoppningsvis finns tillräckligt många andra satelliter kvar så att man kan räkna ut position, hastighet och tid. Vinsten med ett gruppantennsystem kan vara mycket stor. Exemplet i figur 31 visar en sändare som kan störa ut en civil mottagare på 90 kilometers avstånd. Samma sändare stör ut en militär mottagare på 30 kilometers avstånd och med ett skyddssystem blir maximalt avstånd för störningen endast 300 meter.

Skyddssystem mot störningar för militär användning har funnits sedan 90-talet och är dyra. Det är inte ovanligt att ett militärt störskyddssystem för GNSS kostar 50 gånger mer än mottagaren som det ska skydda. SDR-teknik håller på att ändra på det. Störskyddssystem baserade på SDR-teknik behöver inte vara mycket dyrare än mottagaren. SDR-tekniken gör att avancerade störskyddssystem är möjliga på många fler och mindre plattformar, inklusive civila. Det innebär också att det blir svårare att skydda sig med telekrig mot precisionsvapen, då även dessa utrustas med SDR-baserade störskyddssystem.

Multisensorsystem för navigering

Trenden är att störning mot GNSS blir vanligare. Radiosignaler på GNSS-frekvenser dämpas

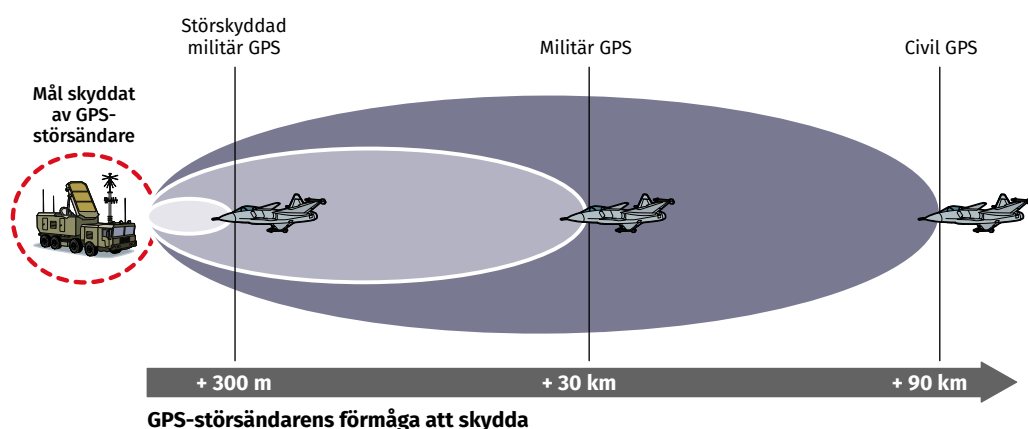


Figur 30. Ett gruppantennsystem dämpar störningar genom att göra antennen extremt okänslig i riktning mot störaren. De mer avancerade störskyddssystemen kan samtidigt förstärka signalen mot satelliterna.

mycket snabbt av terräng och vegetation. Det är stor chans att en mottagare på marken, i alla fall tidvis, är skyddad mot störsändaren och kan bestämma sin PVT-lösning. Det är svårare för flygburna mottagare som ofta har fri sikt till eventuella störare under längre tid.

Ett integrerat navigeringssystem kan överbrygga perioderna då GNSS inte är tillgängligt. Det görs genom att kombinera GNSS-mottagare

med en eller flera andra sensorer, som tröghets-sensor, hastighetssensor, höjdmätare och stabil klocka. I stort sett alla sensorer som kan hjälpa till med att ge en uppfattning om en plattform rörelse eller position kan bidra till en robustare navigeringslösning. Det svåra är att uppskatta tillförlitlighet och fel i respektive sensor så att brusiga eller felaktiga data inte påverkar PVT-lösningen. ■



Figur 31. Jämförelse mellan civil GPS och militär GPS samt militär GPS som är skyddad av ett system mot samma störsändare.

Telekrig mot radarsystem

Radarsystem

RADAR (Radio Detection And Ranging) är namnet på en utrustning och metod för att upptäcka, lokalisera och beskriva objekt genom att belysa dem med elektromagnetiska vågor. En radarsignal sänds ut och riktas mot ett mål med hjälp av en antenn. Signalen fortplantas med ljusets hastighet genom atmosfären, reflekteras i målet och fångas upp av en mottagare. Det gör att i första hand avstånd, riktning och hastighet kan bestämmas. Schematiskt kan ett radarsystem indelas i ett antal block med olika funktioner enligt figur 32.

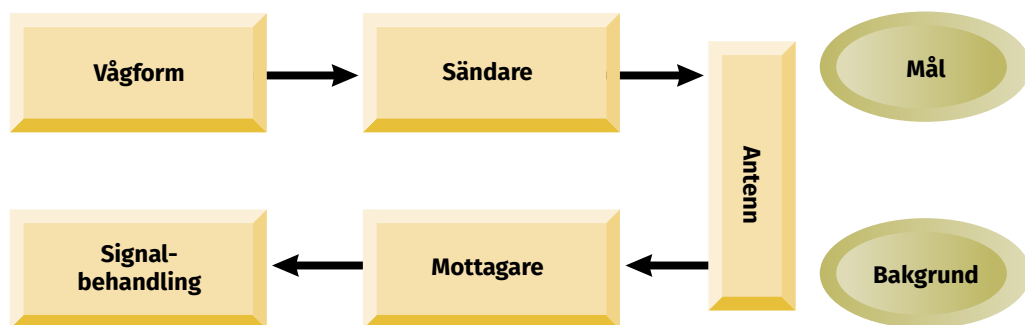
Avståndet till målet ges av signalens löptid från sändaren till målet och tillbaka till mottagaren. Riktningen till målet ges av höjd- och sidvinklar hos antennloben. Förmågan att särskilja mål i vinkel beror på antennens lobbredd. I figur 33 visas ett typiskt strålningsdiagram för ett radarsystem. Diagrammet gäller för såväl sändning som mottagning. Ett måls närmandehastighet ges av frekvensskiftet (dopplerskiftet)

i den mottagna signalen, eller en avståndsförändring över tiden.

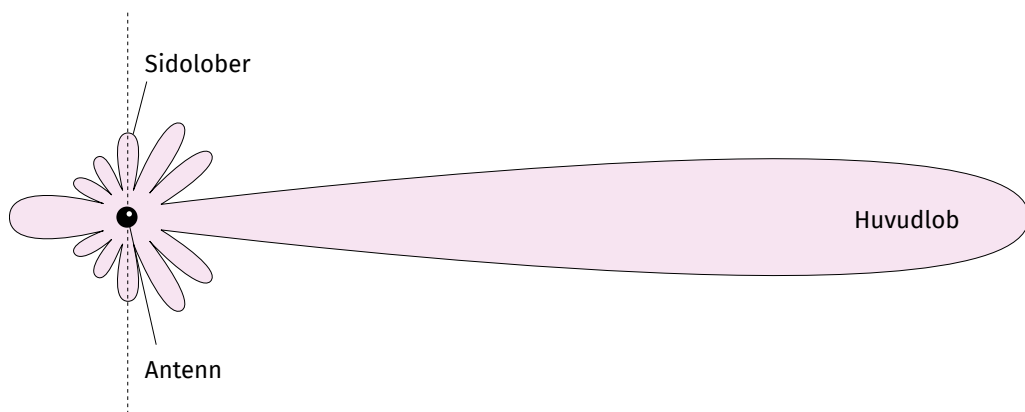
Radarsystem använder olika frekvenser beroende på vilka egenskaper som önskas hos systemet. Låga frekvenser, ända ner till enstaka MHz, kan användas för att se förbi horisonten, eftersom signalerna kan följa jordytans krökning eller reflekteras i jonosfären. Extremt höga frekvenser kan till exempel användas för att skapa högupplösta bilder på korta avstånd. De flesta militära radarsystem använder dock frekvenser i området 1–40 GHz.

Vågform

En radarsignal består av en bärvåg (typiskt GHz) som moduleras på något sätt. Modulationen kan gälla bärvågens amplitud, fas, polarisation eller frekvens. Det är vanligt att förändra amplituden med pulssade signaler, vilket har gett upphov till begreppet pulsradar. Under pulstiden sänds bärvågen ut med hög effekt. De flesta



Figur 32. Blockschema för generellt radarsystem.



Figur 33. Schematiskt strålningsdiagram. Huvudloben har typiskt 30 dB (1000 ggr) högre antennvinst än sidoloberna.

militära radarstationer för spaning och eldledning utnyttjar pulssade signaler. Radar som kombinerar pulsradar och dopplereffekt (pulsdopplerradar) eller den enklare varianten MTI-radar (Moving Target Indication) är en mer utvecklad pulsradar, som använder pulsföljder för att sortera ut rörliga mål.

Det råder ett motsatsförhållande vid avstånds- och hastighetsmätning. Hög pulsrepetitionsfrekvens (PRF) behövs för stort entydigt hastighetsintervall, men leder till kort entydigt avstånd. Låg PRF behövs för stort entydigt avstånd, men leder till låg högsta entydiga radiella hastighet.

Om man använder en medelhög PRF blir både avstånd och radiell hastighet mångtydiga. Men om man varierar PRF flyttar sig felen medan det riktiga värdet är samma varje gång – då kan felaktigheter uteslutas. Fördelen gentemot låg PRF är att man kan sända under en större andel av tiden och på så sätt använda högre genomsnittlig effekt.

Korta pulser krävs för att få hög upplösning i avstånd. En kort puls måste ha högre effekt för att innehålla lika mycket energi som en lång och därmed ge radarn samma räckvidd. Genom att förändra utsända pulser i olika faser och frekvenser och sedan signalbehandla retursignalen kan man uppnå både hög avståndsupplösning och lång räckvidd. Förfarandet kallas pulskompression.

Sändare

Sändarens funktion är att generera och förstärka den elektromagnetiska signalen som ska belysa målet. Traditionellt har sändare baserade på magnetroner eller vandringsvågrör (TWT-rör, Travelling wave tube) använts. Den tekniken gör det möjligt att skapa korta pulser med hög toppeffekt. Nu sker ett skifte mot halvledarförstärkare, t.ex. baserade på galliumnitrid (GaN), som hittills har visat sig mest effektiva och tåliga. Det är svårt att åstadkomma lika hög toppeffekt med GaN-förstärkare som med TWT, men tack vare pulskompressionsteknik som använder långa pulser kan man nå hög medeleffekt. Samtidigt kan förstärkarna göras så små att de kan integreras i stort antal och distribueras i en gruppantenn.

Antenn

Radarantennen ska koncentrera och göra den utsända signalen tillräckligt stark i en smal lob. Det handlar om att styra antennloben i önskad riktning, undertrycka signaler från oönskade riktningar och att ge tillräcklig antennarea för att ta emot signalenergin från målet.

Med digitala gruppantenner kombineras de olika delarna till önskad amplitud och fas för rätt fokus och för att ta bort oönskade riktningar. Det finns också antenner som kombinerar digital och analog teknik, till exempel genom digital styrning i elevation, men analog summering i sida.

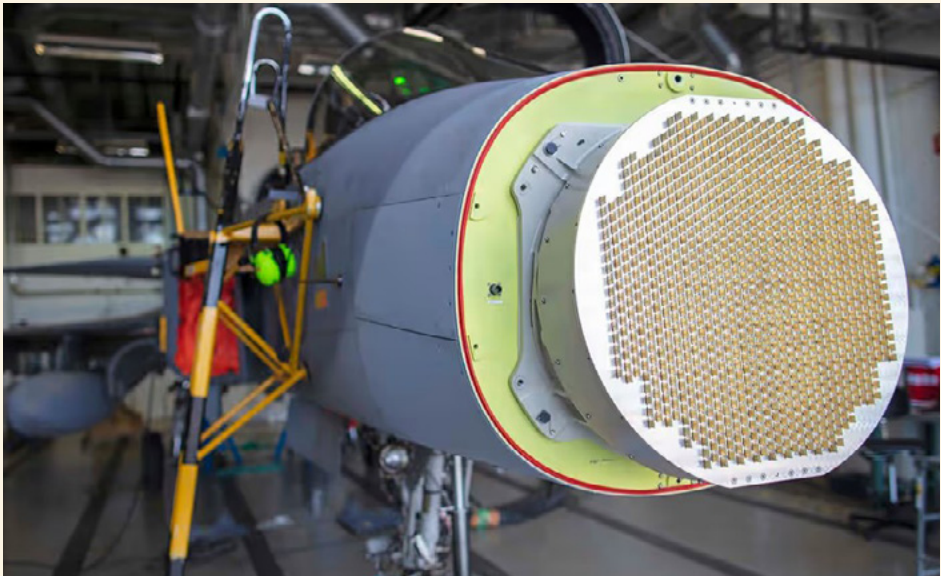
AESA-antennor

En aktiv elektriskt styrd antenn (AESA) är en gruppantenn där varje antennelement har sin egen modul för sändning och mottagning (TRM, Transmit/Receive Module) för effektförstärkning vid sändningen och låg brusförstärkning i mottagningen.

I en fullt digital AESA har varje TRM även sin egen frekvenskonvertering och DA/AD-omvandling. Alternativet är att delantennor skapas där fasskiftskretsar används för lobstyrning inom delantennerna. Då behövs endast en uppsättning frekvenskonverterare och DA/AD-omvandlare per delantenn men en del av flexibiliteten går förlorad.

Fördelar med digitalt styrda antennor:

- Loben går att styra elektroniskt inom ett stort vinkelområde, utan mekanisk tröghet.
- Det går att bilda flera mottagarlober samtidigt, till exempel för hög känslighet och noggrannhet inom en bred belysningslob.
- Det går att sända i flera lober och frekvenser samtidigt.
- Adaptiv lobformning i mottagning kan undertrycka störare och andra interferenser.
- Ankomstriktningen går att uppskatta för enskilda pulser (monopulsfunktion).
- Om det uppstår fel i enstaka antennkanaler så kan många funktioner ändå fungera hjälpligt.



Figur F5. Raven ES-05 AESA nosradar till Gripen E. Foto: Copyright SAAB AB.

Mottagare

Mottagarens funktion är främst att förstärka de signaler som fångats upp av antennen (målsignaler och icke önskvärda signaler) inom det aktuella frekvensintervallet och att genom filtrering generera största möjliga signal/brusförhållande på mottagarutgången.

Signalbehandling

Signalbehandlingen ska bland annat beräkna primära mätdata från den mottagna radarsignalen. Beräkningen görs vanligen genom att sammanställa flera utsända och mottagna radarsignaler inom den så kallade integrationstiden. Signalbehandlingen har även till uppgift att ta bort störningar och oönskade ekon (klotter) för att minska brus och göra det lättare att upptäcka målet. I moderna radarstationer sker signalbehandlingen digitalt och med digitala gruppantennor blir även lobformningen en del av signalbehandlingen.

Spaningsradar

Radarstationer på marken för luftövervakning är normalt stora, effektstarka och har lång räckvidd (mer än 300 kilometer). Den bärande frekvensen ligger vanligtvis i intervallet 1–5 GHz. Antennsystemen är stora för att få smala lobor och kunna urskilja mål i vinkel. Låg PRF och pulskompression har traditionellt använts för entydighet och hög avståndsupplösning. I moderna system med GaN-förstärkare kan pulslängden vara större och även pulsrepetitionsfrekvensen kan vara högre tack vare medelhöga PRF-modor, vilket kan leda till utökad räckvidd. Ett exempel är Giraffe 4A, se figur 34.

Det finns ett antal landbaserade och sjöburna spaningsradarsystem med 3D-förmåga (mäter målet i tre koordinater). Dessa arbetar på frekvenser mellan 3 och 10 GHz.

För spaningsradarsystem som är flygburna strävar man efter lång räckvidd (100-tals kilometer). Det kräver hög medeleffekt och låg frekvens för att begränsa atmosfärsdämpningen. Storleken på antennen begränsas av att den ska monteras på flygplan, men man önskar en relativt smal antennlob, vilket ställer krav på tillräckligt hög

frekvens. Användning av 2–4 GHz är en bra kompromiss mellan dessa olika krav. Genom att använda pulsad dopplerradar kan lågt flygande mål skiljas från oönskade ekon (markklotter).

Radarn i AWACS (Airborne Warning And Control System) är ett exempel på ett spaningsystem. AWACS har förmåga att upptäcka och följa flygande mål och har personal ombord för att leda stridsflygplan. ASC-890 är ett svenskt radarsystem för mindre plattformar som ska ersättas av Global Eye S106. Dessa system utgör först och främst spaningsplattformar som automatiskt skickar bearbetade data om ett upptäckt objekt (mätdata) till ett ledningssystem som finns på marken, men kan även användas för luftstridsledning.

Syntetisk aperturradar

Syntetisk aperturradar (SAR) uppfanns redan 1951, men har fått sin renässans med den digi-



Figur 34. Svensk luftspaningsradar Giraffe 4A. Systemet är en pulsad radar på 3 GHz som har en räckvidd på flera hundra kilometer. Pulsrepetitionsfrekvens och pulslängd är varierbara. Copyright Saab AB. Foto Stefan Kalm.

tala tekniken. I stället för att ha en stor antenn bygger principen på att låta en liten antenn röra sig och samla in reflekterade signaler, som sedan används för att i en dator bygga upp en stor syntetisk antennapertur. Fördelarna är många, men framför allt går det att generera radarbilder med hög upplösning (upp till 10 centimeter) oavsett avstånd. Principen bygger på antagandet att det är en stationär scen som avbildas. Rörliga objekt på marken blir ofokuserade i den slutliga SAR-bilden. Jämför med en vanlig optisk kamera som har en öppen slutare. Alla objekt som rör sig när slutaren är öppen kommer att bli suddiga eller rent av försvinna helt om de rör sig mycket snabbt.

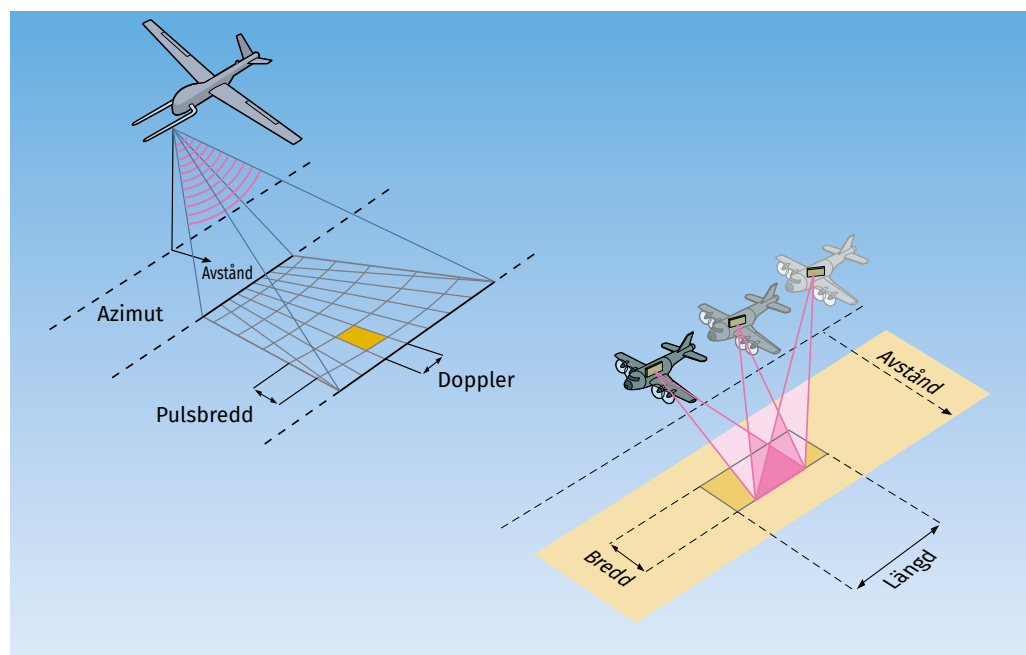
SAR används bland annat för att spana på en motståndares område, till exempel för att få bilder av flyg- eller marinbaser, där enskilda flygplan eller fartyg kan observeras. Långvägiga SAR-system kan till och med se genom olika slag

av maskeringar och tät skog. Fordon eller grupperingsplatser kan därför lätt upptäckas med hjälp av SAR.

Ett SAR-system kan användas i ett flertal moder beroende på uppgift: SAR strip ("strip-map"), SAR spot ("spotlight") och GMTI (Ground Moving Target Indication). De två förstnämnda kan endast upptäcka och lokalisera mål som står stilla under integrationstiden.

Skillnaden mellan moderna är att i stripmod pekar antennen i samma riktning, medan den i spotmod justeras kontinuerligt för att hela tiden peka mot ett visst målområde. Det senare gör att integrationstiden ökar och att bildupplösningen i flygriktningen blir finare. Priset man får betala för den högre upplösningen är att det avbildade områdets storlek samtidigt minskar, se även figur 35.

GMTI-moden med vilken upptäckt och lokalisering av rörliga mål kan göras bygger på att



Figur 35. Avbildningsgeometri för SAR. Till vänster stripmod, till höger spotmod.

diskriminera de rörliga målen från de fasta med hjälp av dopplerfrekvensen hos den mottagna signalen i en viss riktning.

Eldledningsradar

En eldledningsradar har till uppgift att mäta in ett mål med sådan precision att dess vapensystem kan göra verkan i målet. Mätningen måste hela tiden uppdateras (tiotal Hz) eftersom målen i regel kan manövrera snabbt. Radarsystem för eldledning är utrustade med flera olika skydd mot störningar eftersom det förutsätts att motståndaren kan sätta in motmedel. Radarn har smal antennlob för att kunna mäta in målet noggrant i vinkel, vilket ger antennen en hög förstärkning. Radarn har ett begränsat synfält och behöver oftast invisas av ett annat sensorsystem. Eldledningsradar förknippas oftast med luftvärnssystem som, förutom höjd- och sidovinkel, även mäter målets avstånd och hastighet. Då målet kommer in på låg höjd måste radarn undertrycka klottret, vilket den gör med MTI (Moving Target Indication). Eldledningsradar med pulsdoppler har snarlika egenskaper som nosradarn i flygplan. Nosradarn i de flesta jaktflygplan är förutom en spaningsensor även konstruerad för att låsa på och följa mål.

Radarmålsökare

Radarmålsökare finns ofta i jakt- och luftvärnsrobotar med lång räckvidd och är de absolut vanligaste sensorerna i sjömålsrobotar. Deras uppgift är, liksom för eldledningsradarn, att mäta in positionen så att roboten kan styra mot målet. Det är viktigt att riktningen till målet kan mätas under dåliga väderförhållanden. Styrningen mot

ett mål underlättas om avstånd och närmandehastighet kan mätas, men det är inget absolut krav.

För att få en så bra vinkelmätning som möjligt används så kallad monopolsteknik. Det utgör i sig ett bra skydd mot störningar eftersom både höjd- och sidovinkel mäts för varje puls. Det är möjligt tack vare att antennen består av flera delar med tillhörande mottagarkanaler, vilka sedan jämförs. För mål till sjöss används två mottagare. När radarn upptäcker och börjar följa ett mål skapas en följelucka som i sidled är given av systemets lobbredd. I längdled sätts ett avståndsintervall med målet i centrum. Mål utanför följeluckan ignoreras.

Radarsändaren kan finnas ombord på roboten (aktiv målsökare) eller på en annan plattform (semiaktiv målsökare). De senare är vanliga i luftmålsfallet, där en stark sändare kan vara placerad på marken eller i ett stridsflygplan. I de fall då roboten behöver manövrera självständigt på långa avstånd (längre än 100 kilometer) måste sändaren vara placerad i roboten. För radarstyrda jaktrobotar kan flygplanet som avfyrar roboten göra en undanmanöver och behöver inte ligga kvar och belysa målet. Det förekommer även radarmålsökare för markmål. Det är dock relativt svårt för en radar att skilja typiska mål på marken från falska mål, som stenar, träd eller hus. Det går dock att använda en hög avståndsupplösning tillsammans med dopplerinformation. Ett sätt att motverka störsändare, som befinner sig i målet, är att övergå till passiv följning och styra mot storkällan ("home on jam"). Radarmålsökare som styr mot andra radarsändare finns som "signalsökande" robotar.

Radarmålarea

Radarmålarea (reflektivitet) avser en fiktiv yta (skild från verklig yta) och är ett mått på hur stor del av det infallande fältet som reflekteras tillbaka till radarn från ett objekt. Radarmålarean beror på objektets form, material, våglängd, polarisation och betraktarens vinkel. Radarmålarea har dimensionen kvadratmeter.

Elektromagnetisk stödverksamhet

Elektromagnetisk stödverksamhet (ESM), radar-signalspaning, har de primära uppgifterna att:

- upptäcka signaler från emitterande radar-system
- bestämma riktning till – och helst position för – emitterande radarsystem
- identifiera emitterande radarsystem och eventuell tillhörande plattform
- samla in information för att stödja analyser efter genomförda uppdrag och bidra med underlag för att uppdatera telekrigsbibliotek.

ESM-system (Electronic Support Measures) kan till exempel användas för att varna för en annalkande robot med radarmålsökare, men kan även bidra till lägesbilden och har då ofta en viktig roll vid egna vapeninsatser.

Det är viktigt att reagera snabbt för att snarast kunna vidta motåtgärder när till exempel en hotande robot närmar sig. Det är därför önskvärt

att hela det aktuella frekvens- och vinkelområdet täcks utan avsökning. När systemen bidrar till lägesbild och vapeninsats kan till exempel längre räckvidd och noggrannare riktning vara viktigare. Det ger även operatören mer tid för samverkan med system på andra plattformar.

Dagens system kan i många fall kombinera både bra defensiva och offensiva egenskaper, se figur 36. Det beror framför allt på att digitaliseringen av signalerna sker närmare antennerna.

Upptäckt

Flera grundläggande villkor måste vara uppfyllda samtidigt för att en radarsignal ska kunna upptäckas, se den vänstra delen av figur 37. Systemet måste till exempel momentant bevaka den frekvens som radarn utnyttjar för att faktiskt kunna fånga signalen (intercept). Om en riktantenn används i signalspaningen, och signalen är svag, måste troligen även antennens riktlob peka mot radarsystemet. Om signalen fångas upp eller



Figur 36. Korvett HMS Karlstad. Högst upp på fartyget sitter antennen för signalspaning innanför en konisk radom. Systemet kan varna för radarbaserade hot och skapa en lägesbild genom att upptäcka, mäta in och identifiera radarsignaler samt de sändande radarsystemen och plattformarna. Foto: Jimmie Adamsson/Försvarsmakten.

inte beror både på signalspaningssystemet och hur radarsystemet uppträder.

När villkoren för intercept är uppfyllda kan signalen från en viss radar detekteras. Det innebär att en vald tröskelnivå överskrids och händelsen ger data som går vidare i systemet. Det är ganska enkelt att räkna ut sannolikheten för upptäckt utifrån varje mottagen puls och problematiken är i princip densamma som hos en radar. Det som påverkar sannolikheten är effekten hos den mottagna signalen och bruset hos mottagaren samt hur amplituden fördelas. Sannolikheten för upptäckt avgörs av den tröskelnivå som har valts. En sänkning ökar sannolikheten för att en mottagen puls ska detekteras, men samtidigt ökar risken för att tröskeln överskrids enbart av brus. Tröskelnivån är därför en kompromiss som ger tillräckligt god sannolikhet för korrekta detektioner, utan att risken för falska är oacceptabelt hög.

Radarsignalspaningssystem presenterar och rapporterar i princip aldrig enstaka pulser. För att en operatör eller ett automatiskt system ska reagera krävs normalt att flera pulser detekteras, men även att de bedöms höra samman och inte kommer från olika radaremittrar. Möjligheterna att upptäcka en viss radarsignal påverkas därför av hur systemet för signalspaning är uppbyggt, men även signalmiljön kan inverka genom att

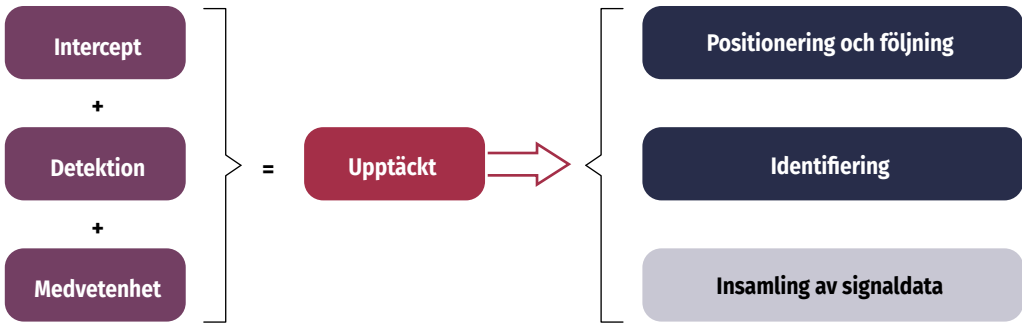
den interna signalsorteringen (se faktaruta) försvåras.

Möjligheterna att upptäcka en radarsignal beror på egenskaperna både hos signalspaningssystemet och radarsystemet. Därför är det inte enkelt att beskriva vilken räckvidd som nås eftersom den dessutom påverkas av signalmiljön och vågutbredningen. Om inte den egna målarean är mycket stor vinner dock i de flesta fall en plattform utrustad med ett signalspaningssystem upptäcktsduellen mot en radar eftersom signalspaning utnyttjar envägsutbredning. I många situationer är även räckvidden mot radarns sidolöber taktiskt användbar.

Kombinationen lång räckvidd och stor momentan vinkeltäckning medför att system för radarsignalspaning ofta har stor momentan yt- eller volymtäckning. Därför kan de med fördel stödja andra sensorer som behöver mycket tid för att avsöka stora ytor.

Riktningsbestämning

De flesta signalspaningssystem kan mäta vilken riktning radarsignaler kommer från, i en eller ibland i två dimensioner. För radarvarningsfunktion är information om hotriktningen ofta tillräckligt för att initiera en undanmanöver och insats av motmedel. Hos många system är också riktningsbestämning ett av flera alternativ som



Figur 37. Ur användarens perspektiv är nyttan med radarsignalspaningssystem att sändare (emitttrar) kan positioneras, följas och identifieras. Först behöver de utsända signalerna upptäckas. Det förutsätter att villkoren för intercept, detektion och medvetenhet är uppfyllda. Ofta samlar systemen även in information om signalerna, som kan användas för analyser efteråt, till exempel framtagning av ett telekrigsbibliotek.

Signalsortering

De olika radarsignalerna som når signalspaningssystemets antenn och passerar mottagaren ger en gemensam ström av inmättningsdata. Den behöver sorteras i realtid för att den efterföljande databehandlingen ska ge användbar information om respektive signal, radarsystem och deras plattformar. Varje detekterad och inmätt puls i dataströmmen representeras av ett dataord, en så kallad signaldeskriptor, som med några hundra databitar beskriver de parametrar som mottagaren mäter in. Parametrar som alltid brukar ingå är ankomsttid, bärfrekvens, pulslängd, amplitud och ankomstriktning. Det är även vanligt att det finns databitar som beskriver eventuell modulering inom pulsen (intrapulsmodulation).

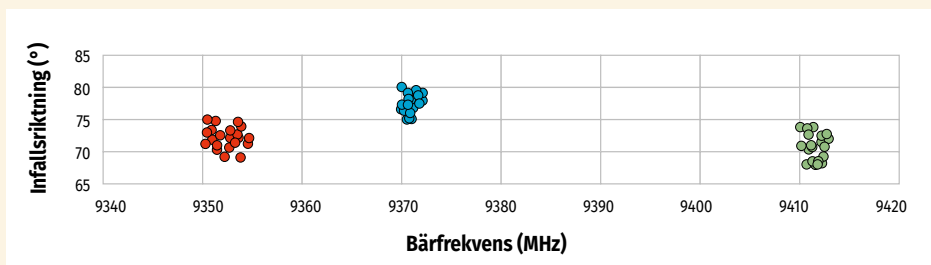
Radarsystem använder vanligen riktlober. De inmätta signalerna består oftast av skurar med signaldeskriptorer som motsvarar de tidsavsnitt när en riktlob har pekat mot signalspaningssystemet. Strömmen av blandade signaldeskriptorer behöver grupperas per radar för att bearbetas vidare av signalspaningssystemet. Signalsorteringen är en förutsättning för att man ska vara medveten om signalnärvaron, vilket är ett krav för att signaler ska kunna upptäckas.

Det finns en stor mängd forskningsartiklar som beskriver och utvärderar olika metoder för signalsortering. Mycket av utvecklingen är dock inte allmänt tillgänglig, utan hamnar under företagssekretess. Även i samband med upphandling av system är det vanligt att tillverkare är ovilliga att beskriva hur de löst problemen med signalsortering, vilket försvårar utvärderingar.

Några faktorer som påverkar signalsorteringen är:

- kvaliteten på signaldeskriptorerna
- antalet inkommande signaler och deras komplexitet
- förekomst av signaler med överlappande parameterområden.

Hos taktiska system behöver signalsorteringen arbeta i nära realtid, vilket kan vara utmanande. Ofta är kravet att kunna hantera signalmiljöer där mottagaren kan producera upp till en miljon signaldeskriptorer per sekund. Förutom den bearbetning som sker i nära realtid har de flesta systemen möjlighet att spela in signaldeskriptorer för att göra analyser efteråt. Inspelningarna kan omfatta alla signaldeskriptorer eller ett urval, till exempel ett visst vinkel- eller frekvensområde. Ett annat alternativ kan vara att spela in signaldeskriptorer som kommer från emittorer som inte har kunnat identifieras.



Figur F6. Exempel på signalsortering som använder frekvens och riktning och som skulle kunna skilja signaler från tre radarsystem åt. Figuren visar endast ett utsnitt av utfallet.

visar ett radarsystems position. Detta är information som ofta har stort taktiskt värde, se vidare avsnittet positionering.

Moderna radarsystem har ofta kapacitet att variera sina vågformsparametrar från puls till puls. I täta komplexa signalmiljöer är det därför önskvärt att rikttningsbestämning av varje mottagen puls sker för att systemets signalsortering ska kunna fungera utan sammanblandningar.

Metoder som mäter ankomstriktningen för varje mottagen puls brukar benämnas monopulsmetoder. De jämför signalerna som kommer från ett antal parallella mottagarkanaler, vars ingångar är anslutna till lämpligt utformade och inriktade antenner. Amplitudmonopuls och fasmonopuls (interferometri) är exempel på två monopulsmetoder för att bestämma riktningen. Ibland kombineras dessutom metoderna och då

ger mätningen av skillnaderna i amplitud entydigheten och mätningen av skillnaderna i fas noggrannheten.

Lobmaxpejling med sidolobsblockering är en annan metod som använder en riktantenn som söker runtom eller i en valbar sektor. Detta görs tillsammans med en antenn som har runtomtäckning, en så kallad omniantenn. Denna metod kan bara göra korrekta rikttningsmätningar när riktloben pekar mot radarsystemet. Lobmaxpejling är därför ingen monopulsmetod. Figur 38 illustrerar ett interferometrisystem för rikttningsbestämning.

Positionering

Det är önskvärt att signalspaningssystemen snabbt mäter in radarsystemens positioner med hög noggrannhet och att radarpositionerna kan



Figur 38. För rikttningsbestämning med interferometri används ofta antenner med 3–5 antennelement som pekar i samma riktning och sitter på rad, se den högra delfiguren. Typiskt för så kallade linjära interferometerarrayer är att avståndet mellan antennelementen inte är identiskt. Den användbara sektorn är ca $\pm 60^\circ$ relativt riktningen tvärs flygplanskroppen. Bilden visar en installation på ett AWACS-flygplan. (Foto: Jason Wells/Shutterstock.)

följas om de ändras. Dessutom bör positioneringen kunna ske inom ett stort område, utan att sensorerna flyttas, det vill säga att de täcker en stor yta eller volym. Idealt sker positioneringen i tre dimensioner, men ofta är två dimensioner tillräckligt, till exempel om identifieringen visar att signalen kommer från en radar på marken eller ytan.

Det finns ett antal olika metoder för att mäta in en radars position. Ett generellt problem är att signalspaningssystem endast i undantagsfall kan mäta avståndet till radarn från en stationär position. Positioneringen sker därför normalt genom att använda mätningar från två eller flera separerade inmätningar. Det sker antingen genom att en sensor rör sig eller att flera sensorer samverkar. I det senare fallet kan positioneringen ofta ske både snabbt och med god noggrannhet, vilket är en av de stora vinsterna vid sensorsamverkan.

Inom Nato pågår införandet av CESMO (Cooperative Electronic Support Measure Operations) som är en standard för samverkan rörande inmätningssdata från olika typer av signalspaningssystem.

När sensorer samverkar är det viktigt att alla mätningar som används avser signal från samma radar, vilket ibland benämns relativ identifiering. Genom att radarsignalspaning har en unik förmåga att identifiera sändare (emitttrar) med hjälp av egenskaperna i vågformen finns i de flesta fall goda möjligheter till en robust relativ identifiering.

Triangulering är en klassisk och välkänd positioneringsmetod som baseras på att riktningen till radarn mäts från olika inmätningsspositioner. När förutsättningarna är lämpliga finns det dock andra metoder som kan ge mycket bättre noggrannhet. I gynnsamma fall kan de stödja insatser med GNSS-styrda vapen. Exempel är TDOA respektive DDOA/FDOA som båda beskrivs i kapitlet Telekrig mot radiokommunikationssystem.

Båda metoderna använder och är beroende av karaktistiken hos de mottagna radarsignalerna. TDOA kan därför ge noggrann positionering av radarsystem med hög upplösning i

avstånd, medan DDOA/FDOA kan vara en noggrann metod mot radar som mäter målets hastighet med hjälp av doppler. Den senare förutsätter rörelse, helst med hög hastighet, och fungerar därför bäst på signalspaningssystem som är flygburna eller satellitbaserade.

Både TDOA och DDOA/FDOA kan besväras av mångtydigheter på samma sätt som radar-sensorer kan vara mångtydiga vid avstånds- respektive hastighetsmätning. I signalspaningsfallet påverkas mångtydigheten såväl av vågformen som av den aktuella inmätningssgeometrin.

Vid TDOA krävs att flera separerade sensorer samverkar och att de samtidigt blir belysta av samma radarpulser. Eftersom de flesta radarsystem använder riktlober uppfylls kravet enkelt genom att sensorerna placeras nära varandra. Noggrannheten vid positioneringen blir bättre om avstånden ökas mellan sensorerna och därför behöver den inbördes valda geometrin vara en kompromiss. Vid signalspaning mot kommunikation är förutsättningarna annorlunda eftersom radiosystemen ofta är rundstrålande. DDOA/FDOA sker däremot antingen med enskilda signalspaningssystem eller genom att flera system samverkar.

Det är fördelaktigt att kunna kombinera flera av metoderna eftersom deras egenskaper skiljer sig åt. Då uppnås bättre noggrannhet och/eller ökad robusthet mot flera olika typer av radarsignaler.

Följning av aktiva radarsystem

För att signalspaningssystemen på bästa sätt ska bidra till lägesbilden behöver nya detektioner och inmätningar leda till att radarsystemet börjar följas. Den aktuella informationen ska sedan uppdateras så ofta det går. En operatör får ofta resultatet av följningen presenterat i form av en lista över aktiva radarsystem, där informationen om respektive radar visas på en egen rad.

Antalet kolumner i en aktiv emitterlista brukar vara omfattande. Den innehåller ofta beskrivningar av inmätta signalparametrar och infallsriktningen, men även resultat från identifieringen och den bedömda hotnivån. I båda fallen baseras resultaten på information från

Klassificering

Inom radarsignalspaning används begreppet klassificering vanligtvis för en funktion som fastställer hur respektive signalparameter varierar över tiden.

Parametrar som klassificeras är bland annat:

- bärfrekvens
- pulslängd
- intrapulsmodulation
- pulsrepetitionsintervall
- antennavsökning.

Vilka klasser som används skiljer mellan parametrarna och beror ofta på den systemlösning som tillverkaren valt. Den sammanlagda klassindelning som ett system har för de olika parametrarna benämns signalmodell.

För flera av signalparametrarna har sannolikt alla signalmodeller en klass som motsvarar att parametervärdet inte ändras alls. För bärfrekvens och pulslängd kan andra klasser till exempel motsvara att värdet skiftas från puls till puls, eller att det sker efter ett antal pulser. På svenska används i det senare fallet begreppet sekvensstagg men ofta även den engelska motsvarigheten dwell and switch.

Signaler som använder sekvensstagg kommer ofta från radarsystem som mäter målens radiella hastighet med hjälp av radarekonas

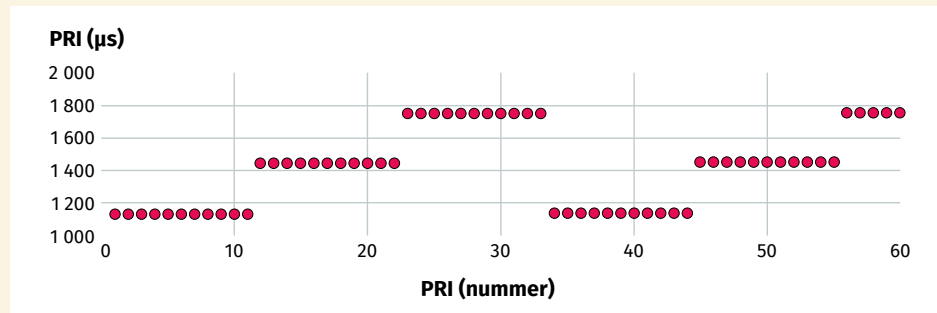
dopplerskift. Vanligtvis sänder dessa en skur med likadana (och koherenta) pulser där repetitionsintervallet är konstant. Därefter växlar åtminstone pulsernas repetitionsintervall för att lösa upp mångtydigheter i avstånd och/eller hastighet samt för att undvika blinda avstånd.

Pulsrepetitionsintervall är en nyansrik parameter och den kan därför delas in i relativt många olika klasser som beskriver olika beteenden. Detsamma gäller intrapulsmodulation, där fasmodulation och frekvensmodulation är vanliga klasser.

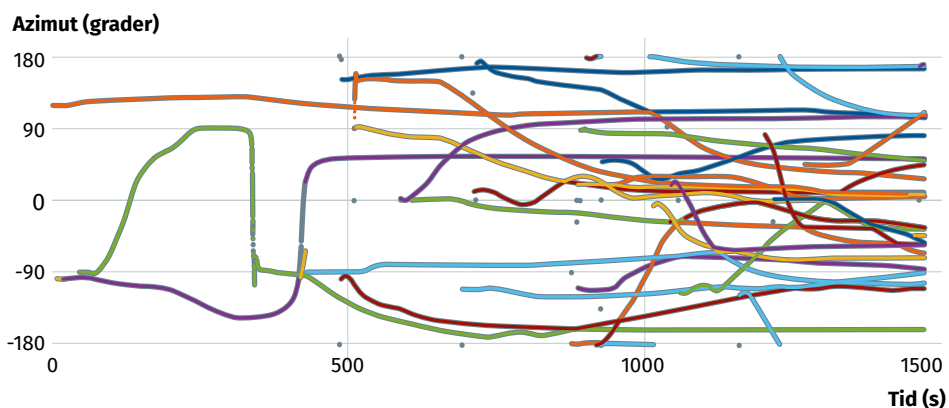
Det största antalet möjliga klasser finns sannolikt inom antennavsökning, där det förekommer många olika avsökningsmönster.

En klassificering av en signal från en viss radar är en sammanställning av klassen för respektive signalparameter. Indata till klassningen är emitterbeskrivningar. Resultatet kan visas i listan med aktiva radaremitttrar. Normalt används det även av signalspanings-systemets funktion för identifiering.

Klassificering skiljer sig från identifiering, bland annat genom att det inte krävs någon tidigare information i ett emitterbibliotek. Det innebär att en signal som inte är känd sedan tidigare ändå kan klassificeras.



Figur F7. Principfigur som ger exempel på en signal där sekvensen med pulsrepetitionsintervall är av typen sekvensstagg.



Figur 39. Illustration som visar hur ett radarsignalspaningssystem följer ett antal aktiva radarsystem. Endast riktningen till respektive radar visas, men följningen utnyttjar även signalparametrarna.

en databas med teknisk information om olika sändare (emitterbiblioteket). Listan kan också visa när följningen började och tiden sedan den senaste uppdateringen. Tiden mellan uppdateringarna vid följningen beror delvis på när intercept inträffar. Det påverkas såväl av radarsystemets avsökningar som eventuella avsökningar utförda av signalspaningssystemet.

Indata till följningen är vanligtvis så kallade emitterbeskrivningar. De mottagna pulserna grupperas av systemets signalsortering och det sker en efterföljande beräkning av parametrar för respektive pulsgrupp. Beskrivningarna innehåller ofta min-, max- och medelvärden för de parametrar som utgör pulsgruppens signaldescriptorer. Det tillkommer även nya parametrar, bland annat tidsskillnaden mellan pulsernas ankomsttider. Det är en viktig parameter som benämns pulsrepetitionsintervall, PRI.

För varje ny emitterbeskrivning behöver systemet avgöra om den ska användas för att uppdatera följningen av något av radarsystemen i den aktiva emitterlistan eller om en ny följning ska påbörjas. Systemets följalgoritmer kan på olika sätt använda både signalparametrar och riktningssinformation, se exempel i figur 39.

Det finns två fundamentala fel som följefunktionen kan göra. Det ena är att uppdatering av en aktiv radar är felaktig, vilket blandar samman information från två aktiva radarsys-

tem. Det andra felet är att en ny följning påbörjas trots att den aktuella radarn var ett av de radarsystem som redan följdes. En konsekvens är att en och samma radar ger två parallella följningar.

Risken för felaktiga sammanslagningar eller splittringar beror mycket på antalet aktiva radarsystem, hur lika de är och hur de varierar sina signalparametrar. I det avseendet är det särskilt utmanande att följa en radar som växlar mellan olika moder. En möjlig lösning kan vara att använda information från emitterbiblioteket som visar att moderna används av samma radartyp.

I bemannade signalspaningssystem får operatören med hjälp av sin erfarenhet ofta manuellt försöka korrigera fel som den automatiska följningen gör.

Identifiering

En viktig uppgift för radarsignalspaningssystem är att identifiera de signaler som upptäcks. Då blir det möjligt att presentera och rapportera vilken typ av radar som har upptäckts, men även att binda plattform och eventuellt vapensystem till denna radar. Eftersom en radar använder olika vågformer beroende på mätuppgift är det även möjligt att avgöra vilken arbetsmod som används. Den informationen är betydelsefull, till exempel för att definiera hotnivån eller välja lämpliga störmetoder.

Viktiga parametrar för identifieringen är bland annat signalens bärfrekvens och pulsrepetitionsintervall. Ytterligare information är till exempel pulslängd, intrapulsmodulation och parametrar som beskriver antennavsökningen. Resultatet från de inmätta parametrarna jämförs med innehållet i emitterbiblioteket och i gynnsamma fall kan entydig identifiering göras. I många fall presenterar systemen flera alternativ och anger sannolikheten för varje alternativ.

Olika radarsystem har ofta likartade signalparametrar, vilket försvårar identifieringen. Vid framtagningen av emitterbibliotek är det därför väsentligt att undersöka vilka identifieringskonflikter som kan uppstå och om möjligt undvika dessa. En viktig del i arbetet är att välja emitterar utifrån vad som bedöms kunna förekomma i aktuellt område. Förberedande underättelser i form av strategisk signalspaning är därför nödvändig, men emitterbibliotek behöver även uppdateras under pågående operationer.

En viktig aspekt av identifiering är att signalspaningssystem inte enbart kan inriktas mot att hantera signaler från motståndarens radarsystem. Många mottagna signaler kommer från egna system eller system som används av neutrala eller civila aktörer. Dessa signaler bidrar till lägesbilden, men kan i vissa fall liknas vid klotter.

Om en inmätt signal inte kan matchas mot någon specifik radartyp eller radarmod i emit-

terbiblioteket återstår kategorisering som en möjlighet. Kategorisering kan sägas vara en grövre identifiering som endast avgör radarklass, till exempel att signalen kommer från en fartygsbaserad spaningsradar.

När radarsignalspaning beskrivs i litteratur och artiklar används ofta begreppen klassificering och identifiering tillsammans, utan att tydligt ange vad som skiljer dem åt. I en separat faktaruta beskrivs den tolkning av begreppet klassificering som är vanligast inom området radarsignalspaning.

Säker identifiering är mycket betydelsefull för att undvika vapeninsatser mot den egna sidan eller civila. Bristande identifiering gör ofta en vapeninsats omöjlig. En av de verkligt attraktiva egenskaperna hos system för radarsignalspaning är förmågan till identifiering. Tack vare den förmågan är den överlägsen det som kan åstadkommas med en radar och identifieringar kan ofta ske inom hela räckviddsområdet. Signalspaningssystemets förmåga att avslöja arbetsmoden hos aktuell emitter är också unik genom att den avslöjar status och intentioner.

Framtida radarsystem kommer troligen i ökad omfattning att ha stor vågformsflexibilitet. Det försvårar inte bara signalsorteringen, utan är allmänt en stor utmaning när funktioner för identifiering i kommande system för radarsignalspaning ska utvecklas.

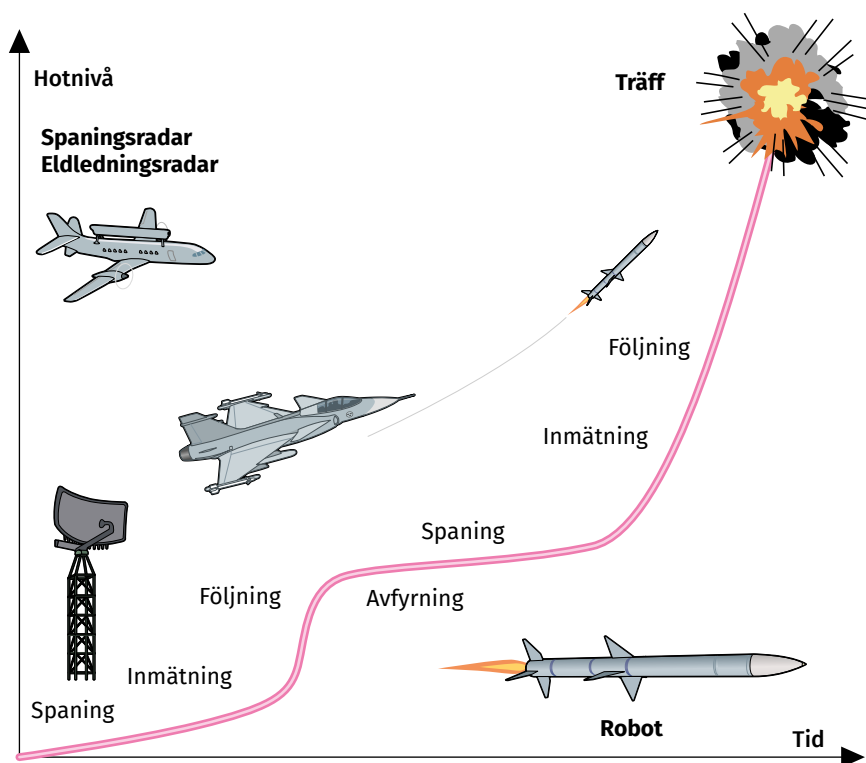
Elektromagnetisk attack

En radarsensor har ofta en mer eller mindre stark koppling till någon form av vapensystem. Det kan till exempel vara en spaningsradar med lång räckvidd som ger invisning till en eldledningsradar. Det leder i sin tur till en vapeninsats med målsökande robot. Det innebär ett akut hot som kräver en mycket snabb insats för att avvärjas.

För att påverka en motståndares radarsystem används bland annat störning i form av elektromagnetisk attack. Syftet är att minska prestandan hos radarsensorerna så mycket att de inte har till-

räckligt med data för att aktivera vapensystemet. Kortfattat kan det beskrivas som att störningen får radarsensorn att inte se saker som finns, alternativt att se saker som inte finns. Radarsensorer har dock vanligtvis metoder för att motverka störning.

Generellt sett är det en stor fördel att bryta händelsekedjan i början genom att störa den långräckviddiga spaningsradarn. Då kan den inte invisa till nästa steg i händelsekedjan och man undviker det något mer akuta problemet med en målsökande robot, se figur 40.



Figur 40. Hotnivån (rosa kurvan) i en telekrigsduell ökar från långräckviddig spaning till inmätning, robotavfyrning, målsökning och träff.

Störningen kan vara maskerande (till exempel täckpuls av brus), vilseledande (till exempel avståndsavhakning) eller mättande (till exempel många falska mål) beroende på typ av sensorfunktion. Beroende på taktisk situation kan störningarna beskrivas som bakgrundsstörning, medstörning, egenskyddsstörning, förgrundsstörning och närstörning, se figur 41–44.

Bakgrundsstörning

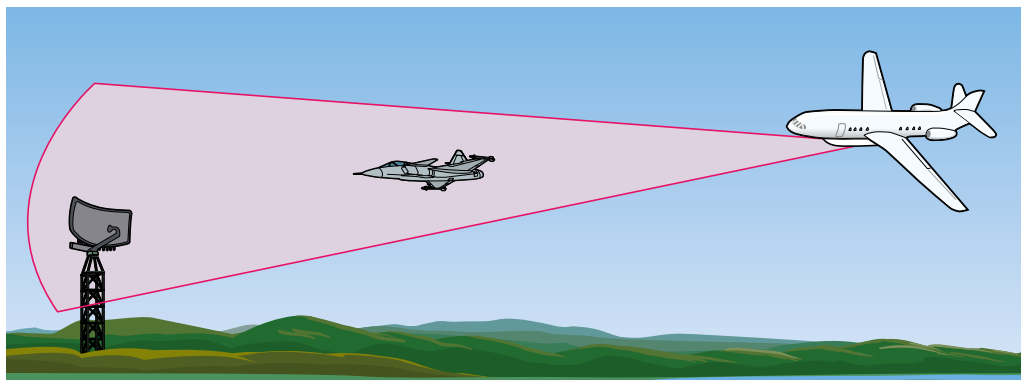
Vid bakgrundsstörning befinner sig störaren långt bortom den man vill skydda och i linje med hotet. Det kan innebära långa avstånd, vilket i sig kräver hög effekt. På grund av avståndet hinner inte störaren mäta frekvensen i tid. Hotradarn, som använder frekvenshopp, kan snabbt byta frekvens innan den upptäcks. Då når störsignalen hotets radar med fel frekvens och sor-

teras bort. Det gör att störaren kan tvingas att använda en bandbredd som täcker hotradarens hela systembandbredd (hoppfrekvensbandbredden). Om störningen även ska ske i radarns sidolobber behöver störningens effekt ökas ytterligare. Bakgrundsstörning är vanligast för att maskera flygplan, då det är lättast att skydda plattformar med liten radarmålarea. Fartyg, som har en mycket stor radarmålarea, är svåra att maskera på stort avstånd.

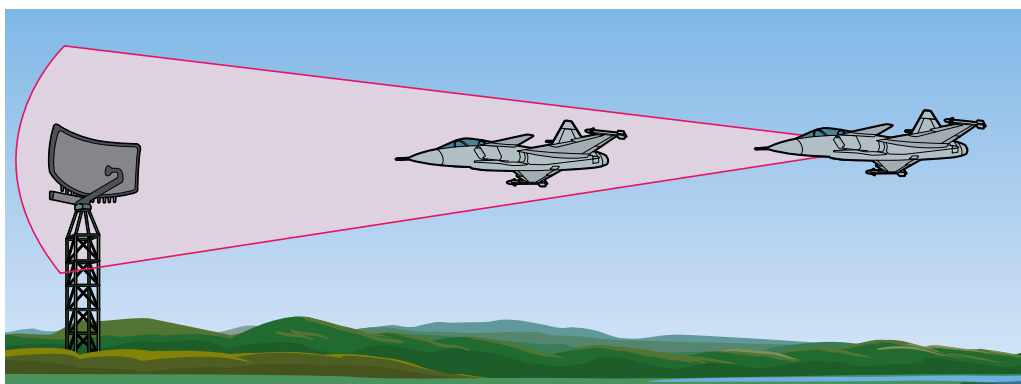
Medstörning

Vid medstörning befinner sig störplattformen i närheten och antingen framför eller bakom den skyddade plattformen. I det fallet krävs inte så hög uteffekt som vid bakgrundsstörning.

För att skydda ett anfallsföretag kan ett av flygplanen förses med en mer kvalificerad stör-sändare i form av en störkapsel. Denna kapsel



Figur 41. Bakgrundsstörning.



Figur 42. Medstörning (eskortstörning).

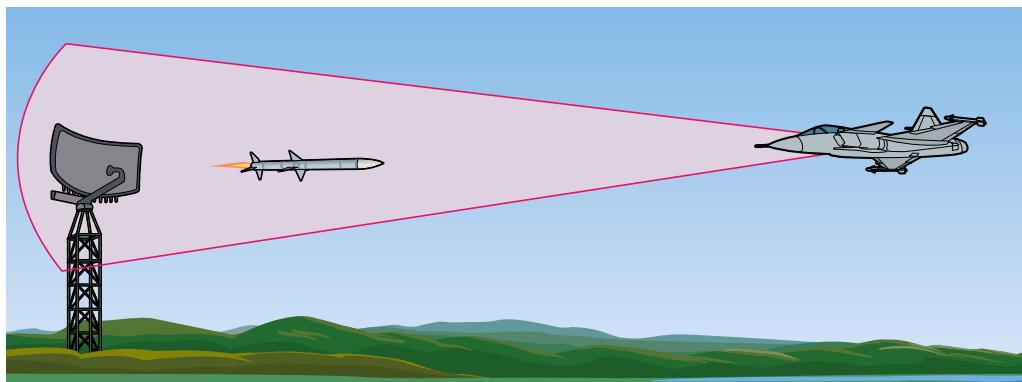
har en betydligt större förmåga än de störsändare som varje flygplan har.

Egenskyddsstörning

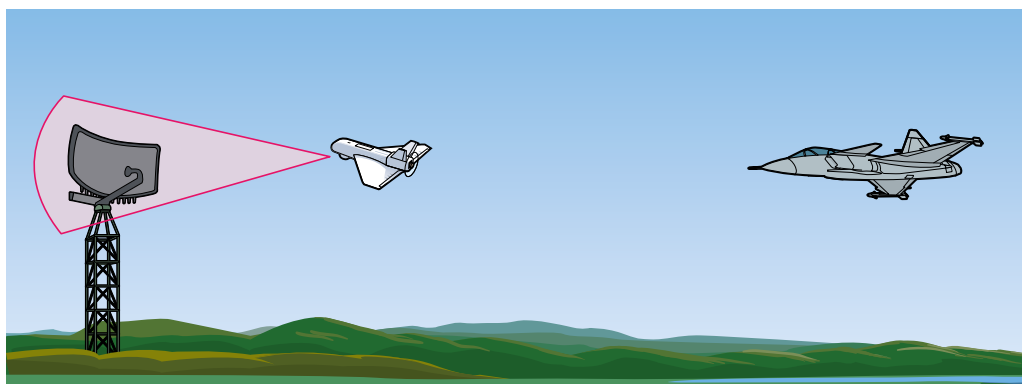
Egenskyddsstörning är det vanligast förekommande fallet av störning, när det gäller att skydda en enskild plattform (flygplan eller fartyg). Här är störutrustningen placerad på plattformen som ska skyddas. Egenskyddsstörning vänder sig främst mot målsökande robotar och andra högt prioriterade hot, till exempel eldledningsradar. En egenskyddsstörare har måttliga krav på uteffekt, då den oftast arbetar med huvudlobsstörning.

Förgrundsstörning

Med förgrundsstörare menas att störsändaren är placerad nära radarn (mycket närmare än skyddsobjektet). Denna typ av störsändare kan vara utplacerad i förväg eller skickas fram med UAV (Unmanned Aerial Vehicle). Då störaren hinner mäta in radarfrekvensen, innan skyddsobjektet nås av radarsignalen, går det att använda smalbandigt brus på den rätta frekvensen, vilket minskar behovet av uteffekt. För maskering är den här störformen i särklass mest effektiv. Ju närmare radarn störaren är, desto bättre kan skyddsobjekten maskeras. Både olika former av brus och generering av stora mängder falska mål



Figur 43. Egenskyddsstörning.



Figur 44. Förgrundsstörning.

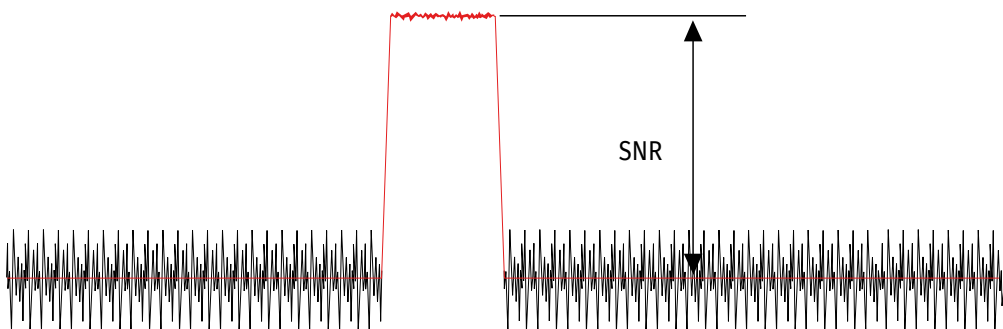
förekommer. Generellt gäller att god störverkan kan uppnås med liten uteffekt.

Ett specialfall av förgrundsstörning kallas för närstörning beroende på att störaren är väldigt nära radarsensorn, från knappt en kilometer till max en mil. Den kan ha utplacerats i förväg eller med UAV. På så nära håll kan skyddsobjekt maskeras effektivt med endast några få watt i uteffekt.

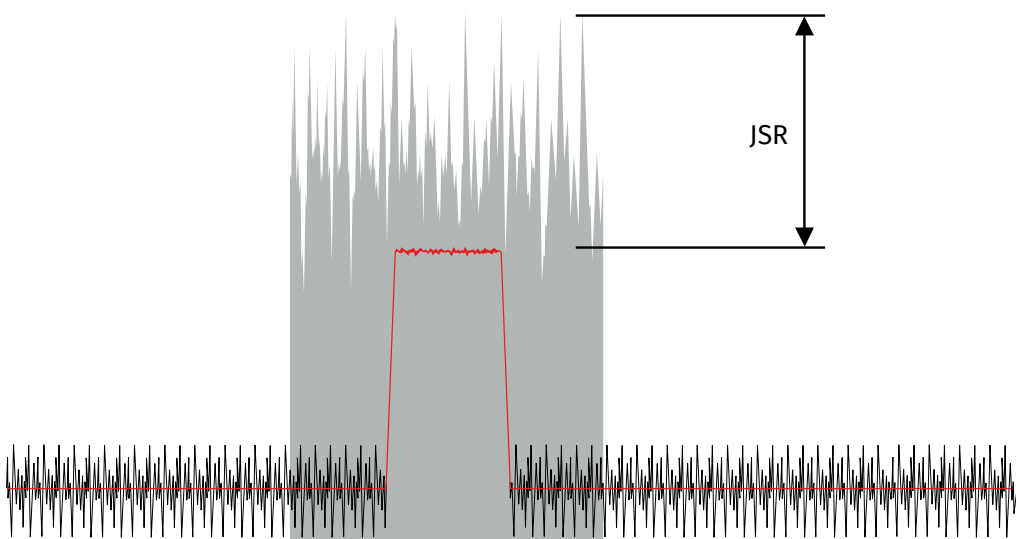
Maskerande störning

Den vanligaste och oftast enklaste maskerande störformen är brus. Bruset höjer radarmottagarens egenbrus, vilket är dimensionerande för dess räckvidd, då förhållandet mellan signal

och brus, SNR (Signal to Noise Ratio), är avgörande för möjligheterna att detektera mål, se figur 45. Det ställs olika krav på brusets bandbredd beroende på hur radarn arbetar. Effekterna av brusstörning går att beräkna. Till exempel kan radarns räckvidd under störda förhållanden enkelt beräknas, om störövertikten JSR (Jamming to Signal Ratio) är känd, se figur 46. Bredbandigt brus kräver mer effekt än smalbandigt för att få samma effekt. Radarns signalbehandlingsvinst gör den i allmänhet mindre känslig för brusstörning. Den enklaste formen av brus består av en bredbandig brusgenerator med möjlighet att styra uteffekten och som inte kräver mottagarfunktion.



Figur 45. Exempel på signal/brusförhållande.



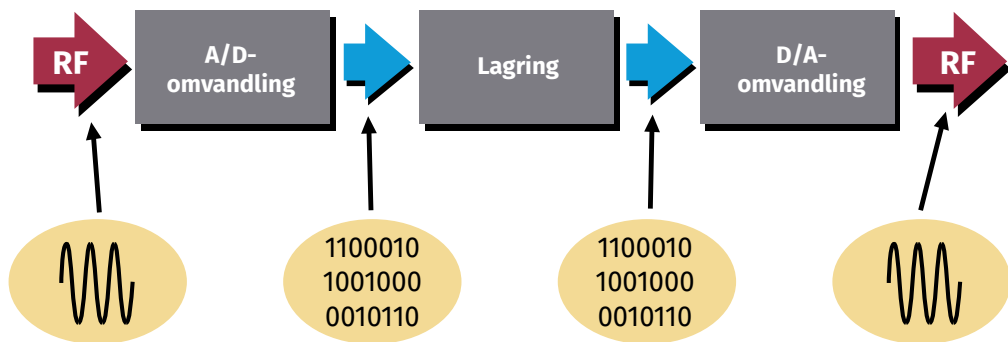
Figur 46. Exempel på störövertakt (JSR).

Mättande störning

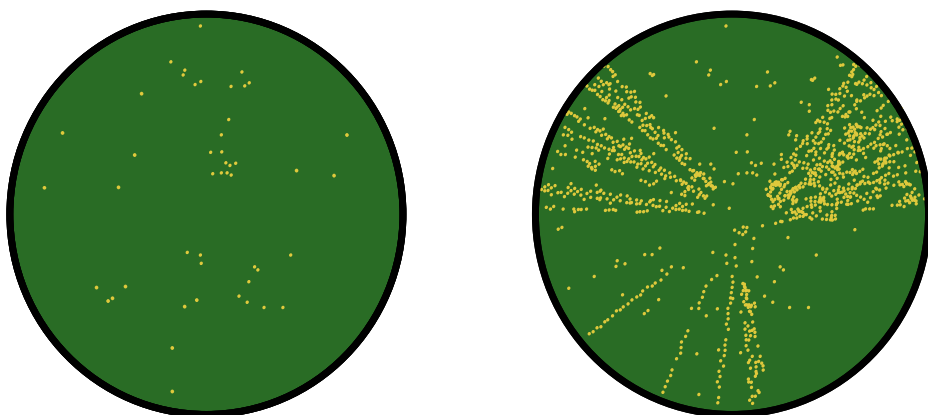
När digitala RF-minnen (DRFM) introducerades blev det möjligt att skapa repetitiva störningar som kan massproducera falska mål, se figur 47. En synkron repeterstörning skapas med ett DRFM och brukar klassas som mättande störning. Störningen kan ses som ett mellanting mellan maskerande och vilseledande störning. Den maskerande effekten fås genom att en stor mängd falskmål genereras, vilket gör riktiga mål

svåra att upptäcka. Radarn är mycket känslig för de falska målen då de är kopior av den riktiga signalen, vilket gör att störsändaren inte behöver sända med särskilt hög effekt. Det viktiga är att störsystemets mottagare kan detektera radarn. I princip kan falskmål alltid skapas så länge störsändarens mottagare kan detektera radarpulserna. Exempel visas i figur 48.

En repeterstörsändare måste ha en mottagare i systemet, vilket innebär att risken för tele-



Figur 47. En nyckelkomponent när det gäller att skapa falska mål är digitala radiofrekventa minnen (DRFM). RF-signalen digitaliseras och lagras i minnen och kan avläsas hur många gånger som helst och efter godtyckligt lång tid. En finess är att störningen anpassas till bandbredden, det vill säga störpulserna ser precis ut som riktiga ekon. Falskmålen drar nytta av radarns signalbehandlingsvinst på samma sätt som de riktiga målen.



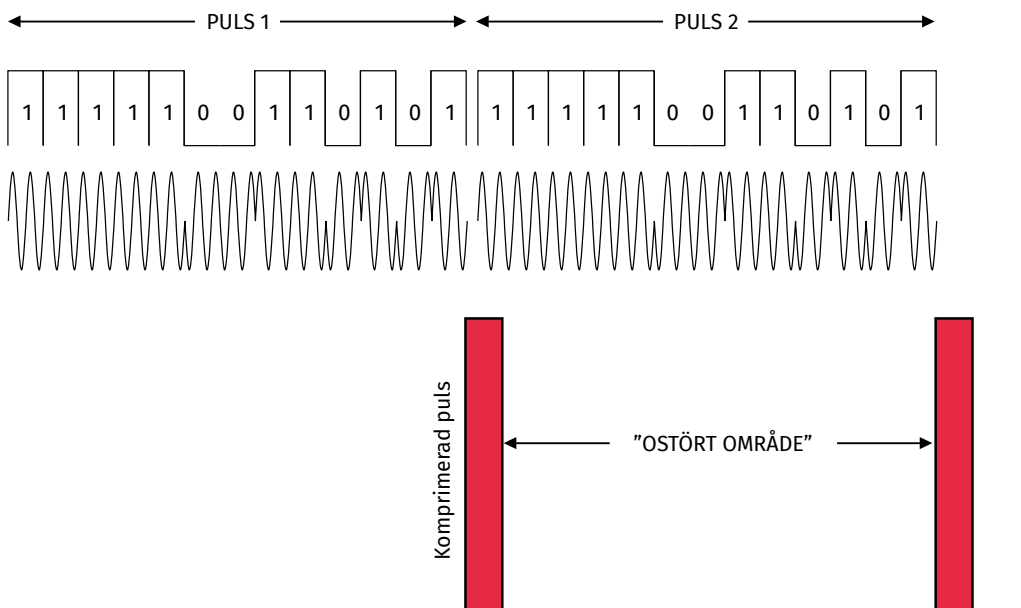
Figur 48. PPI (Plan Position Indicator) till radar för ett ostört fall samt ett som är utsatt för mättande störning.

konflikt ökar. Det gäller att placera sändar- och mottagarantennerna på lämpligt sätt för att få en maximal isolering mellan dem.

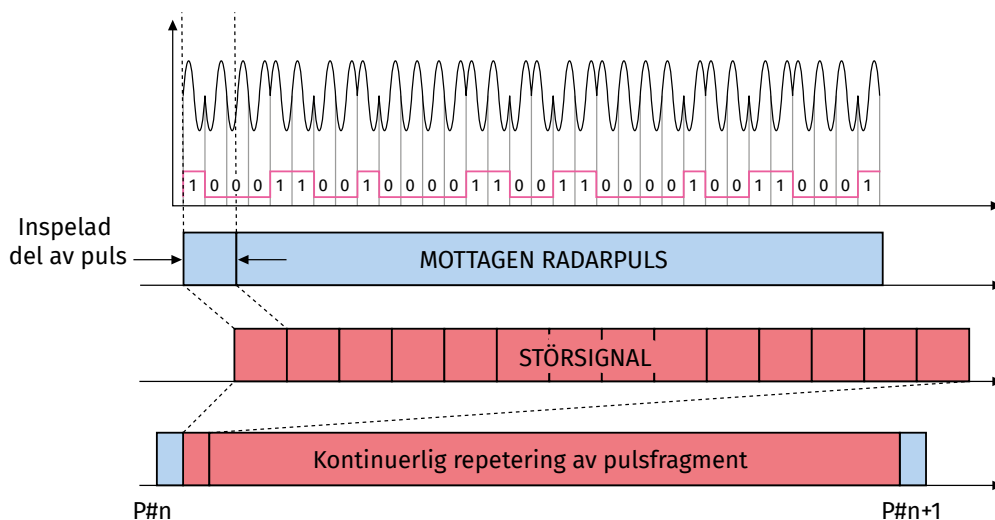
Störning av spaningsradar

En spaningsradar av 3D-typ är främst avsedd för spaning med lång räckvidd mot luftmål. För att uppnå den långa räckvidden behöver radarns pulslängd vara ganska lång, vilket står i kontrast mot avståndsupplösning. Pulskom-

pression med binärfaskodning är en metod för att ändå få god upplösning i avstånd med långa pulser. Avståndsupplösningen blir då lika stor som bitlängden i binärkoden. Den här längden kallas ofta för sub-pulslängd och motsvarar då en avståndsfälla hos radarn. Om ett störsystem repeterar en inspelad radarpuls ”kant-i-kant”, som ses överst i figur 49 som PULS1 och PULS2, kommer det ändå att finnas ostörda partier i avstånd på grund av pulskompressionen.



Figur 49. Störsändaren repeterar radarpulsen kontinuerligt (PULS 1 och PULS 2 som visar binärfas med tillhörande RF-signal). Pulskompressionen gör att det blir ostörda områden i avstånd.



Figur 50. Figuren visar radarpulsens RF-innehåll med tillhörande binär faskod. Den visar att störaren endast repeterar en del av den mottagna radarpulsen kontinuerligt för att få energi i radarns samtliga avståndsfällor. I figuren motsvarar "störsignalen" en sammansättning av de korta repetitionerna till samma längd som radarns pulslängd. Den sätts sedan samman till en kontinuerlig signal, som fyller samtliga avståndsfällor mellan två pulser från radarn. Det vill säga hela pulsintervallet.

Det falska målet komprimeras till en avståndsfälla.

För att motverka dessa ostörda områden kan störaren göra en maskering av avståndsfällor (range-bin-masking). Då kommer endast en del av radarpulsen att spelas in. Den repeteras kontinuerligt för att ge effekt i radarns samtliga avståndsfällor och på så sätt undvika ostörda områden.

Genom att använda en del av den mottagna radarsignalen kommer störningen att vara på rätt frekvens automatiskt, se figur 50. Mot spaningsradarsystem används maskerande eller mättande störning i syfte att förhindra eller försvåra upptäckt (detektering).

Maskerande störsändning som repeteras

Ett DRFM tar emot, lagrar och repeterar radarsignalen kontinuerligt som en pulsskur tills nästa radarpuls anländer. Det innebär att radarn tar emot en kontinuerlig rad av falska mål, vilket

gör det svårt för en operatör att urskilja de verkliga målen.

Brusstörning med DRFM

Ett effektivt sätt att skapa ett brus, som är anpassat efter frekvens, är att använda den mottagna radarpulsen i ett DRFM. Sedan moduleras den signalen med smalbandigt brus, vilket resulterar i ett brus som ligger på radarns egen sändfrekvens.

Störning av SAR

SAR-principen innebär att radarn sänder koherenta (med känt fasläge) pulser under lång tid, från 100 millisekunder (ms) till många sekunder. Under denna belysningstid, som kallas integrationsintervall, tas de reflekterade pulserna emot och integreras koherent. Genom att använda maskerande störsändning kan ett större eller mindre område maskeras från insyn, se figur 51. Om flera störsändare placeras runtomkring kan området skyddas i alla riktningar.



Figur 51. Till vänster visas en SAR-bild (ostörd) från ett fältförsök över norra Visingsö. Till höger motsvarande bild, där SAR-radarn har blivit utsatt för störsändning. Den utsända störeffekten är cirka 10 W.

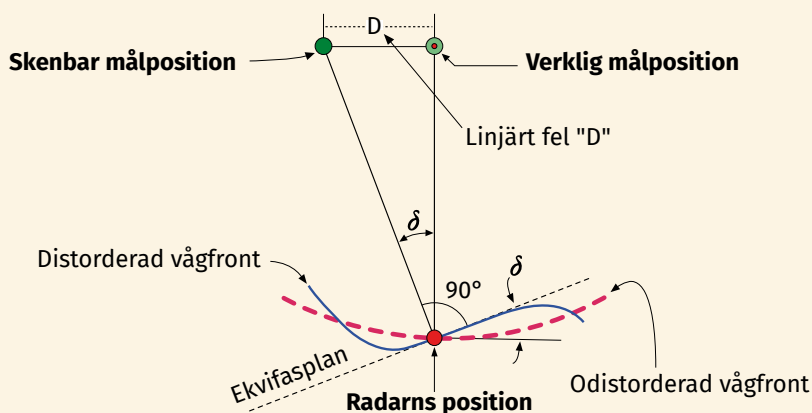
Avståndsavhakning

Avståndsavhakning (RGPO – Range Gate Pull Off) är en repeterstörning som görs med hjälp av ett DRFM-system. En kopia av radarpulsen med högre amplitud än ekot från det egna skrovet fördröjs och sänds ut med ett successivt växande avstånd i förhållande till den mottagna radarpulsen. Om störningens inställningar är rätt valda kommer målsökaren att börja följa den falska signalen i stället för det riktiga målet, eller med andra ord kommer målsökarens följelucka att följa avhakningspulsen. När följeluckan dragits av målet finns det inget skroveko kvar som konkurrerar med falskekot. Då kan störformer som kräver starka störsignaler (stora störövertikter) sättas in, till exempel korspolarisationsstörning eller "cross-eye". Ett annat alternativ är avståndsavhakning i kombination med remsor så att avhakningspulsen leder följeluckan till remsorna. Se exempel i figur 54.

Vinkelavhakning

En av teknikerna för vilseledning i vinkel är fasfrontstörning (cross-eye), som används för att skydda egna plattformar. Den riktar sig mot den fundamentala mätprincipen i en monopulsradar, som till exempel finns i "hotsystem" som målsökare och eldledningsradar.

Principen bygger på repeterstörning från två punktkällor (antennor). Den radarsignal som tas emot i ena antennen skickas tillbaka i den andra antennen och vice versa. Systemet sänder i de båda antennerna med nästan samma amplitud, men den ena signalen är fasvriden 180 grader i förhållande till den andra. Detta ger upphov till en vridning av fasfronten vid målsökaren, det vill säga att en distorderad (förvrängd) vågfront skapas. Monopulsradarn försöker då ställa in sig mot den vridna fasfronten och får då ett vinkelfel gentemot det verkliga målet. Amplitudskillnaden på de två återsända signalerna påverkar hur mycket – och åt vilket håll – vinkelfelet genereras. Störsignalerna från de två antennerna kommer till viss del att ta ut varandra, eftersom de måste vara nästan lika starka och ligga i motfas. Det resulterar i att störsignalen kommer att vara relativt svag. Cross-eye-störningen bör därför föregås av ett avhakningsförlopp så att följeluckan inte innefattar det verkliga målet.



Figur F8. Principen med "cross-eye", där monopulsradarn kommer att försöka rikta in sig vinkelrätt mot den förvrängda vågfronten. Det gör att den riktar in sig mot en skenbar målposition istället för det verkliga målet.

Störning av målsökare

Om störningen av en spaningsradar, som har mätt in målet, misslyckas kommer robotar att avfyras. När detta väl har skett är det inte mycket att göra innan robotens målsökare startar sändningen i en första spaningsfas. Dagens målsökare är till största delen av monopolstyp, vilket innebär att målsökaren mäter infallsriktningen från varje mottagen puls. Även om målsökaren blir störd kan den avgöra riktningen till storkällan och styra mot den. Detta kallas ”Home On Jam”. I ett sådant läge kan det vara säkrare att använda en störsändare som inte är placerad direkt på plattformen som ska skyddas, så kallad ”off board jammer”.

När målsökaren aktiverats börjar en spaningsfas, det vill säga att den gör ett eller några svep med antennen för att hitta angivna mål i området. I det här läget är det mycket viktigt att snabbt komma igång med störning för att hindra upptäckt och läsning på målet. Vilseledande störningar i spaningsfasen kan vara falska mål i sidolob i kombination med täckpuls eller kontinuerligt brus i huvudlob.

Om störning i spaningsfasen misslyckas startar målsökaren följning på målet, det vill säga målsökaren går in i följefas. Då gäller det att få bort följeluckan från målet med någon form av avhakande störning, gärna i kombination med undanmanöver och användning av remsor. Störningen sker genom avhakning i avstånd, hastighet eller vinkel. Mot sjömålsrobotar är det avstånds- och vinkelavhakning som används. Mot robotar med dopplermålsökare mot luftmål används hastighetsavhakning (VGPO – Velocity Gate Pull Off).

Aktivt skenmål

Ett annat sätt att försöka vilseleda i vinkel är att använda så kallade aktiva skenmål. Teknikutvecklingen har gjort det möjligt att ta fram DRFM-system i miniatyr som kan skjutas ut eller släppas från plattformen. En sådan störsändare är tänkt att dra till sig hotet genom repeterstörning och på så sätt stärka det egna skyddet mot eventuella robothot.

Störning med UAV

En UAV kan vara ganska liten och svårupptäckt för en radarsensor som inte är anpassad för att hitta små mål. Det gör den användbar som bärare av störsystem som kan komma nära radarsensorn. Det kommer sannolikt att bli allt vanligare med störningar med hjälp av UAV på många olika sätt.

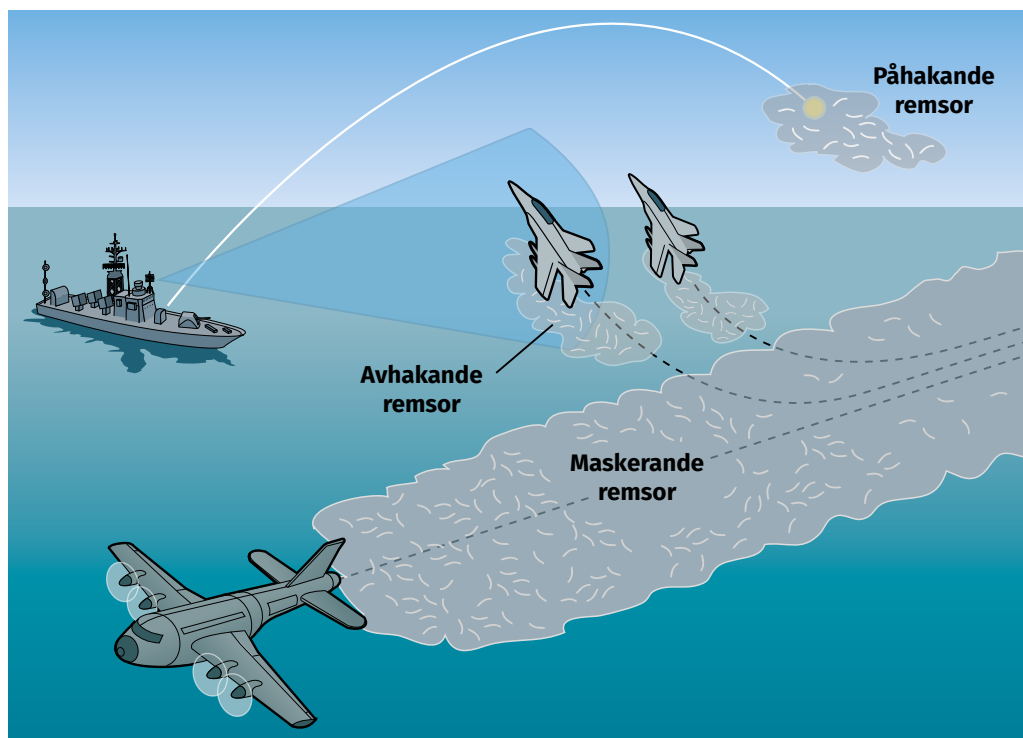
Remсор

Remсор (chaff) är ett av de äldsta motmedlen mot radar. Remсор är tunna trådar som reflekterar radarsignalen och som skjuts eller fälls i mängd för att generera falskmål i syfte att förvilla. Redan 1943 använde de allierade för första gången remsor för att skydda bombflygplan vid räder över Tyskland. Remсор har använts sedan dess för att dölja uppdrag (maskerande effekt), skapa skenmål (påhakande effekt) eller för att få en radar att tappa följning (avhakande effekt), se figur 52.

De första radarremсорna bestod av stanniolfolie uppstagad med papper, medan moderna remsor består av metallbelagda nylon- eller glasfibertrådar. En enskild modern remsa är cirka 20–30 μm tunn och har en ytbeläggning så att de tätt packade remsorna lätt kan separeras, då de skjuts ut eller fälls.

En remsa fungerar som en dipolantenn som reflekterar en del av den mottagna energin från en radar. Reflektionen är störst för de våglängder som matchar längden på remsan. Vanligtvis används så kallade halv vågsresonanta remsor, vilket innebär att remsan klipps till halva den våglängd som den avser att störa. För att störa en 10 GHz radar ($\lambda=3\text{ cm}$), klipps remsan till en längd på 1,5 cm. Se figur 53. Här visas radar-målarean som funktion av frekvensen för en sådan remsa, vilket ger resonanser vid 10, 20, 30 osv GHz.

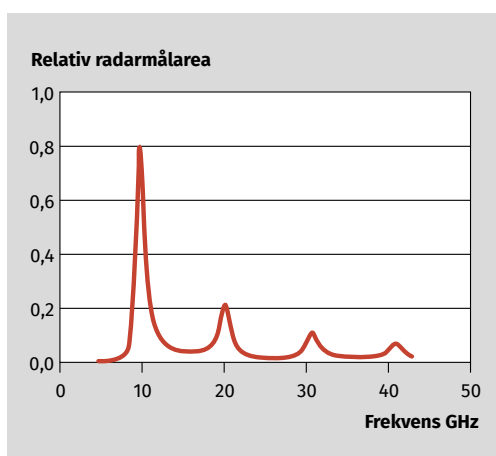
Genom att packa remsor av olika längder får man ett mer kontinuerligt spektrum. Packningen anpassas redan vid tillverkningen efter den troligaste hotbilden. Det förekommer även remsfällarsystem som klipper remsorna efter den våglängd som belyser skyddsobjektet.



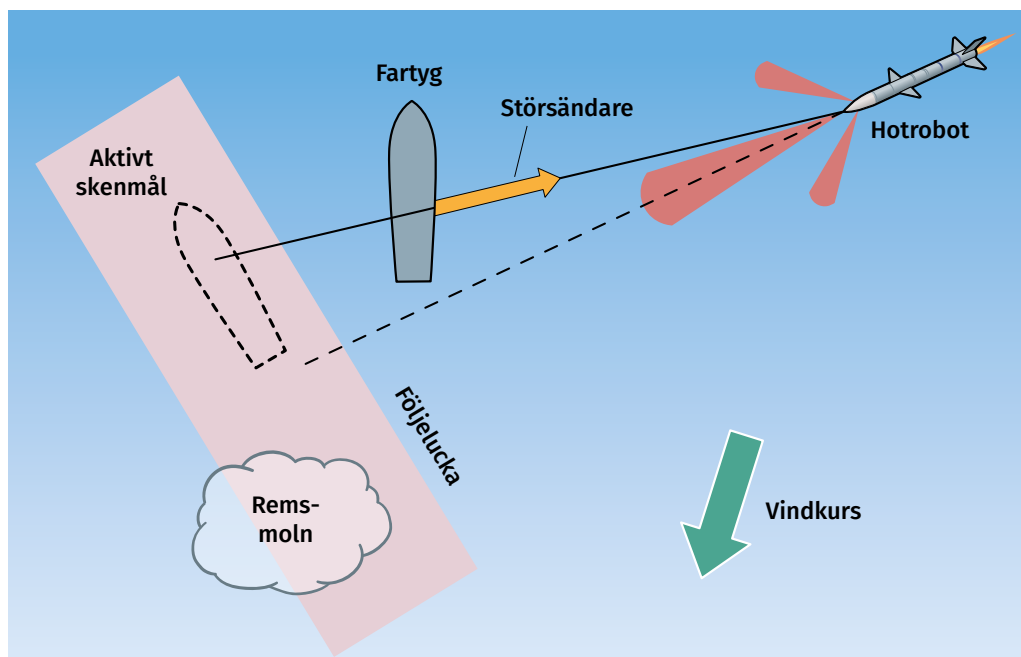
Figur 52. Exempel på användning av remsor.

Spridningen är mycket viktig för att remsorna ska få avsedd effekt. Inom flyget utnyttjas ofta turbulensen bakom flygplanet för att öka spridningen. Remsorna fälls från en plats på flygkroppen som har kraftig turbulens, till exempel en vingspets. Annars går det att montera anordningar på fällningsmekanismen som genererar turbulens. Inom marinen utnyttjas granater för att skjuta remsorna till lämplig plats, där de sprids med en sprängladdning. Fällda remsor har i regel en fallhastighet på cirka 1 meter/sekund. Därför kan de ha effekt långt efter att de har spridits eller fällts från hög höjd.

Fördelarna med remsor är att de är ett relativt billigt motmedel som vilseleder i vinkel och i många fall får en radarstation att använda mindre gynnsamma filtreringsfunktioner. Om remsmå-



Figur 53. Radarmålarean som funktion av frekvens, för remsor med längden 1,5 cm.



Figur 54. Ett avhakningsscenario med både remсор och störsändare. Remsmolnet placeras bakom fartyget sett från hotet. Fartyget kan börja gira för att minska sin målarea för radarn. En aktiv störsändare utnyttjas för att dumpa hotets följelucka på remсорna. Om effekten från remсор och störsändare överväger har störningen lyckats. Störsändaren slås av och hotets följelucka dumpas på remсорna.

let gör att en radar måste använda sin MTI-funktion försämrats möjligheterna att följa mål som rör sig i cirklar runt radarn.

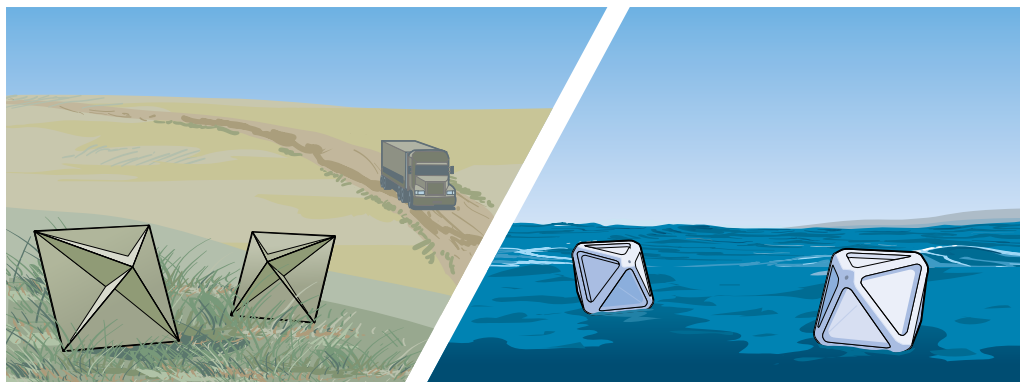
Nackdelar med remсор är att de snabbt stannar upp och går att identifiera. Det görs genom att analysera hur remсорna modulerat den reflekterade signalen. Andra nackdelar är att remсорna påverkar miljön negativt samt att de behöver tid för att utvecklas (uppblooming) för att generera en så effektiv radarmålarea som möjligt.

För att komma till rätta med en del av nackdelarna används remсор ofta i kombination med aktiv repeterstörsändning. Målsökaren eller följradarn lockas att låsa över på remsmolnet (dumpning) genom att repeterstörsändaren genererar avstånds- eller dopplervhakning. Figur 54 visar

ett marint scenario med avhakning, där både störsändare och remсор används.

Oftast kan endast en begränsad mängd remсор tas med under ett uppdrag (speciellt för flygplan). Därför måste man bedöma hur remсорna ska fällas mot en följradar så att ett minimum av remсор används så effektivt som möjligt för att vilseleda radarn. Remсор är det vanligaste passiva motmedlet mot radar, men det finns andra, till exempel hörnreflektorer. Genom att hänga upp eller placera ut dessa på flottar (Rubber Duck) genereras stora skenmål, se figur 55.

Genom att kombinera remсор med hörnreflektorer i fallet till sjöss får man mer fartygslika signaturer, som försvårar ovan nämnda modulationsanalys.



Figur 55. Exempel på hörnreflektorer.

Elektromagnetisk protektion

Störskydd av olika slag finns i radarsystemets olika delar (se blockschemat för ett generellt radarsystem i figur 32) för att undertrycka signaler från störsändare och om möjligt blockera signaler från falska mål. Störskydden är ofta inprogrammerade i moderna radarsystem.

Störskydden skyddar mottagaren från för starka signaler (överstyrning) och gör det lättare att skilja ut målsignalen från störsignalen. Effekten av skydden ökar om inmätning och följning av mål görs med hög robusthet och noggrannhet.

Rörliga plattformar är ett störskydd mot falska mål om flera inmätningar från olika radarpositioner kan korreleras med varandra. Radarns placering gentemot terrängen och förhållanden för vågutbredning kan användas för att dämpa störsignaler utifrån radarns täckningsområde.

Koherenta vågformer innebär ett störskydd eftersom störsignalerna måste vara matchade till radarsignalerna för att vara effektiva. Variabel PRF (pulsrepetitionsfrekvens) innebär ett störskydd eftersom störsändaren inte effektivt kan skapa falska mål på platser närmare radarn än där den själv sänder sina pulser. Vågformer som hoppar mellan frekvenserna är ett viktigt störskydd, eftersom maskerande brusstörning måste spridas ut över en stor bandbredd, vilket ger en försämrad störning.

På liknande sätt är LPI-radar (Low Probability of Intercept) ett störskydd. Tekniken innebär att koherenta vågformer sprider ut den omedelbara effekten över ett stort frekvensområde, vilket gör det svårt att upptäcka.

En stark sändare skyddar också mot störningar, eftersom den gör signalerna tydligare än störningarna. Låga sändarförluster är också viktigt. Det kan man få om förstärkarna sitter nära antennens strålningselement, vilket ofta är fallet med aktiva elektriskt styrda antenner. Dessa gör det också möjligt att styra sändningsmönster och antennlob.

Hög antennvinst eller smal huvudlob är ett viktigt störskydd när sändarantennen följer ett mål, medan en bredare huvudlob med lägre antennvinst kan användas vid sökning. Om en bred sändarlob används är det önskvärt att det kombineras med flera smala mottagarlobber. Detta är möjligt med elektriskt styrd antenn som snabbt kan ändra strålningsriktning och lobform. Det är även viktigt när man vill få sändningsmönster som inte går att förutsäga.

Mottagarantennens utformning är ett väsentligt störskydd. En stor antenn som är bra på att samla in signalerna (hög antennvinst) och fokuserar dem i en smal riktning (med smal huvudlob) gör signalerna tydligare än störningarna (högt signal/störförhållande). Det gör också att

man kan mäta riktningen noggrant. Om antennen också har låga sidolober minskar störningar från annat håll (högt signal/störförhållande).

Adaptiv sidolobsundertryckning (ASLU) för mottagarantennen används för att undertrycka störning från diskreta riktningar i sidoloberna. Sidolobsblockering är ett vanligt störskydd mot pulsade störningar. Monopulsantennerna eller digitala gruppantennerna med flera mottagarkanalerna kan upplösa vilseledande störning och motverka avhakning av målföljning.

Ett grundläggande störskydd i mottagaren är filtrering av mottagna signaler för att hindra störningar utanför radarns bandbredd att komma in i signalbehandlingen. Mottagaren måste också dämpa och blockera starka störsignaler så att den inte överbelastas och skapar nya störningar inom sig själv (olinjära effekter). Reglering av förstärkning och hög dynamik i mottagaren är också viktigt för att kunna filtrera och undertrycka störsignaler i den vidare signalbehandlingen.

De flesta skydd mot störningar införs i radarns digitala signalbehandling, eftersom signalerna kan manipuleras på ett noggrant sätt med väl definierade metoder. Störskydden i signalbehandlingen kan programmeras, utprovas och

modifieras efter hur hoten från telekrig utvecklas. Dopplerfiltrering är ett störskydd mot remsor och andra skenmål som rör sig med långsam hastighet.

Olika typer av adaptiv filtrering är viktiga störskydd som används för att undertrycka störning som är koncentrerad till vissa frekvenser eller riktningar. Ett exempel är samtidig rums- och tidsadaptiv filtrering (space-time adaptive processing, STAP). Den kan dämpa både klotter och störning i en digital gruppantenn.

Givetvis har en mängd störskydd utvecklats under åren för att undertrycka remsstörning. Dopplerupplösning är effektivt för att filtrera bort remsor efter snabba flygplan, då remsorna snabbt bromsas upp och då får helt annan dopplerfrekvens än flygplanet. Av samma anledning är MTI (Moving Target Indication) effektiv för att sälla fram rörliga mål från stillastående eller långsamt rörliga mål (remsor). Med hög upplösning, d.v.s. korta avståndsföljeluckor och smala antennloberna, kan delar av ett mål följas och det blir svårt att placera remsmolnet i följeluckan. Den rörelse som uppstår i remsmolnet genererar en modulation i den mottagna signalen som är möjlig att analysera för att sälla bort remsmolnet som en målkandidat. ■

Telekrig mot elektrooptiska system

Elektrooptiska system

I elektrooptiska (EO) sensorer och system samverkar optiska och elektroniska komponenter. Ett annat begrepp som ibland används är optronik och optroniska system (sammanslagning av optik och elektronik). Det handlar således om elektromagnetiska vågor inom det optiska våglängdsbandet som omvandlas till elektriska signaler eller vice versa. Det optiska våglängdsområdet sträcker sig från 0,1 till 14 μm ($1\ \mu\text{m} = 10^{-6}\text{ m}$, en tusendels millimeter), se tabell 3. I frekvens blir motsvarande område 20 till 3 000 THz ($20\cdot 10^{12}$ till $3\ 000\cdot 10^{12}\text{ Hz}$). För att få hanterliga värden används våglängd när man pratar om elektrooptik.

Elektrooptiska system kräver fri sikt inom sitt våglängdsområde för att kunna utnyttjas. Det som maskerar eller skymmer sikten inom ett våglängdsområde, till exempel rök, kan vara transparent inom ett annat. Det finns två huvudtyper av elektrooptiska sensorer, passiva respektive aktiva sensorer. Passiva sensorer sänder inte ut någon egen strålning, utan mäter reflekterad eller utsänd strålning från objekt och bakgrund.

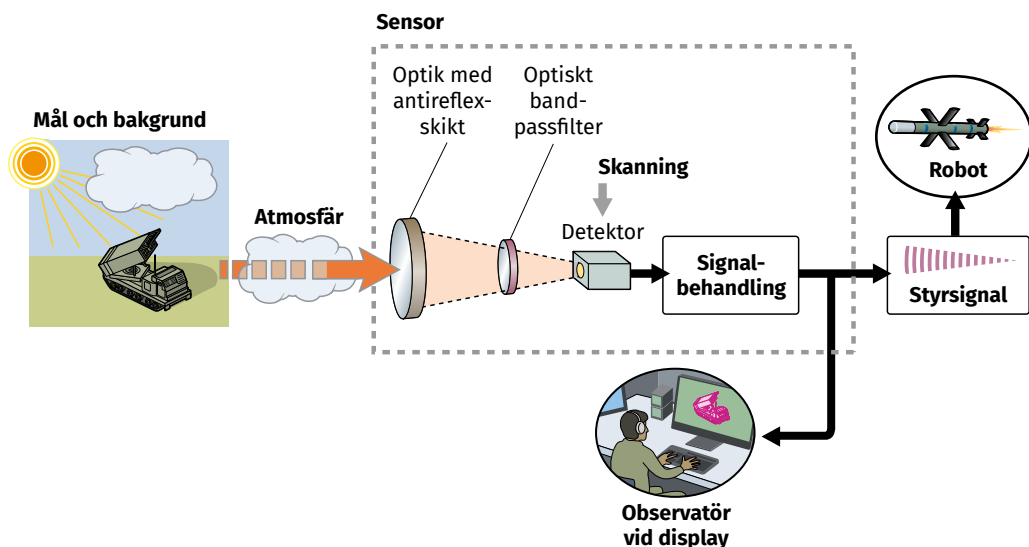
De system som bygger på detektion av reflekterad strålning är vanligtvis system för dagsljus, medan de som bygger på emitterad strålning har dygnet runt-kapacitet. Exempel på passiva system är visuella kameror, IR-kameror, varnarsystem,IRST (infrared search and track) och bildförstärkare. Aktiva EO-sensorer innehåller en aktiv strålningskälla, vanligtvis en laser, och en mottagare (detektor). Exempel på aktiva system är laseravståndsmätare, lidar och optikspanare.

Passiva EO-sensorer

Passiva elektrooptiska sensorer mäter emitterad strålning eller reflektion av naturlig strålning (solljus). En schematisk skiss av ett passivt elektrooptiskt system visas i figur 56. Beroende på typ av mål som ska betraktas används sensorer som är känsliga i olika våglängder. Val av våglängdsintervall för ett system beror på de tänkta målobjektens förväntade signaturer,

Tabell 3. Spektral indelning av det optiska spektrumet. Andra gränser förekommer framför allt för NIR och SWIR, då det inte finns någon standard för begreppen. Begreppet TIR (termisk IR) används ibland för MWIR och LWIR tillsammans.

Spektral- område	För- kort- ning	Våg- längd [μm]
Ultraviolett	UV	0,1–0,4
Visuellt	VIS	0,4–0,7
Nära infrarött	NIR	0,7–1,1
Kortvågigt infrarött	SWIR	1,1–2,5
Mellanvågigt infrarött	MWIR	3–5
Långvågigt infrarött	LWIR	8–14



Figur 56. Ett passivt elektrooptiskt system består av optik, filter, avsökningsmekanik, detektor och signalbehandling. Detta oavsett om systemet ska presentera en bild på en skärm eller generera styr-sig-naler för en robot med passiv målsökare.

bakgrundens variationer (klotter) och atmosfärens transmission. Det finns även elektrooptiska sensorer som är multi- och hyperspektrala och ger spektralupplöst information om målet eller scenen. Hyperspektral information, till exempel i NIR och SWIR, ökar förmågan att upptäcka och klassificera objekt utifrån deras spektrala (materialrelaterade) signatur.

Elektrooptiska system har ofta avbildande matrisdetektorer, men även skannande system förekommer, till exempel för hyperspektral avbildning. Detektorer för längre våglängder (delar av SWIR, MWIR och LWIR) måste ofta kylas för att minska det termiska bruset. För LWIR finns även mikrobolometerdetektorer, som är en relativt vanlig och billig form av detektor och inte kräver kylning.

Spaningssensorer

Elektrooptiska spaningssensorer kan vara placerade på till exempel fordon, flyg, UAV eller satellit. Det är normalt bildalstrande sensorer som används. CMOS- eller CCD-teknik är vanligt i sensorer inom VIS och NIR, men spaning förekommer också i andra spektralområden, till

exempel MWIR och LWIR. Bild- och signalbehandling kan göras direkt av sensorsystemet eller i efterhand för att öka förmågan att upptäcka och identifiera mål i bilderna.

Optisk spaning från satelliter har blivit allt mer betydelsefull och pågår kontinuerligt för inhämtning av information. VIS och NIR är vanligast. Det finns satelliter som ger hög upplösning eller har speciella förmågor, till exempel hyperspektral datainsamling.

Bildförstärkare gör det möjligt att verka i mörker genom att förstärka svagt ljus, bland annat från stjärnor. Den teknik som används i bildförstärkare kan även utnyttjas till mörkersikten, periskop för mörkerkörning, mörkerkikare m.m.

Med elektrooptiska sensorer inom MWIR och LWIR kan spaning ske även i mörker. Dessa sensorer detekterar främst egenstrålning och är inte beroende av någon ljuskälla, till skillnad från bildförstärkare. System som inte kyls ner kan göras små, men har sämre prestanda än kylda IR-sensorer. Den spatiala upplösningen varierar från enstaka µrad till flera mrad beroende på optik och sensorstorlek.

Det elektrooptiska våglängdsområdet

Ultraviolettera (UV) området omfattar 0,1–0,4 μm . Våglängder under 0,2 μm absorberas av atmosfären och har ingen praktisk användning vid optisk vågutbredning. I det så kallade solblinda UV-området, cirka 0,2 till 0,3 μm , gör dämpningen i ozonskiktet att den naturliga bakgrunds-nivån är mycket låg. Målföljare och varnare utnyttjar området för att upptäcka artificiell strålning, till exempel från robotmotorer, utan störande bakgrund. För UV-våglängder från 0,3 till 0,4 μm gör molekylspridningen i atmosfären att belysningen från solen blir mer diffus och skuggorna mindre markanta än i det visuella området.

Visuella (VIS) området omfattar 0,4–0,7 μm . Det mänskliga ögats känslighet är anpassad till solstrålningens spektrala maximum som ligger runt 0,5 μm . Kameror och sensorer används ofta i det visuella området, bland annat för spaning och övervakning.

Nära infrarött (NIR) är området 0,7–1,1 μm . Enkla kiselbaserade detektorer fungerar upp till drygt 1 μm och används bland annat vid övervakning med eller utan aktiv belysning. NIR används också för optikspaning mot visuell optik.

Bildförstärkare, till exempel NVG:er (Night Vision Goggles), utnyttjar NIR-området, ofta tillsammans med det visuella området. Laser används ofta för mål- och scenbelysning i NIR i kombination med bildförstärkare.

Nd:YAG-laser, som är farlig för ögonen, har våglängden 1,06 μm och används för olika ändamål. Oftast används den som belysare för semiaktivt laserstyrda vapen, men den finns även i vissa laseravståndsmätare.

Short wave IR (SWIR) är området 1,1–2,5 μm . Solen ger god belysning i SWIR och sensorer inom detta område kan användas för att upptäcka material som reflekterar annorlunda här jämfört med inom det visuella området. Vid de längre våglängderna runt 2,5 μm syns även termisk strålning från heta objekt. Laser med våglängder runt 1,5 μm används ofta när man vill ha laserutrustning som är säker för ögonen eftersom gränsvärdet för ögonskada är ca 100 gånger högre än i det visuella området, till exempel för laseravståndsmätare.

Medium wave IR (MWIR) omfattar 3–5 μm . Egenstrålning från avgaser och jetflammar syns tydligt inom MWIR-området, men även svalare objekt som personer och fordonsskrov. Solreflexer kan även uppträda inom detta område. MWIR används till exempel för spaning med mörkerförmåga och i robot-skottvarnare.

Long wave IR (LWIR) omfattar 8–14 μm . Naturlig markbakgrund har sin maximala egenstrålning inom LWIR-området. LWIR-sensorer utnyttjas bland annat i sikten och spaningsutrustning för användning i mörker.

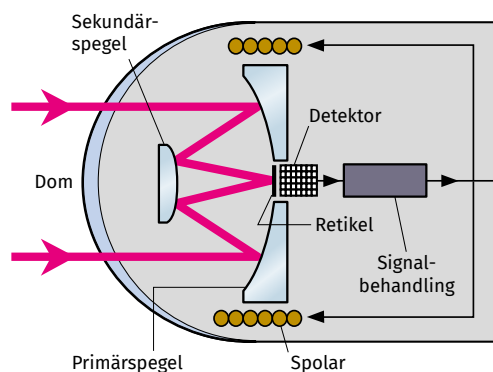
Målsökare

Inom det elektrooptiska området är det främst värmedetekterande och bildalstrande system som utvecklas. System som inte är bildalstrande finns ofta i elektrooptiska jaktrobotar och manburna luftvärnsrobotar, som kan avfyras av en enskild soldat eller liten grupp (MANPADS, MAN Portable Air Defence Systems). Utvecklingen inleddes under 1950-talet och målsökarna utgjordes normalt av retikelsystem.

I första generationens system är principen att låta den infallande strålningen fokuseras på en roterande retikelskiva, som gör det möjligt att bestämma riktningen till ett mål, se figur 57. Retikelskivans mönster och rotationen ger en modulerad signal från vilken målets position kan avgöras. Detta gör att riktningen till en punkt-källa omvandlas till modulation i tiden.

När målet är centrerat inom synfältet blir följningen inte bra med denna typ av system. Om man lutar optiken bort från sin mittlinje (optiska axeln) och låter den rotera kring den linjen får man ett koniskt skannande system (nuterande). Det nuterande systemet har därför ett momentant och ett totalt synfält. Utvecklingen fortsatte sedan med nuterande kors och rosettskannande system. Flera av dagens system är bildalstrande, se figur 58.

Bildalstrande målsökare använder tvådimensionella bilder som antingen skapas av sensorer som sitter i ett rutnär (fokalplansmatris)

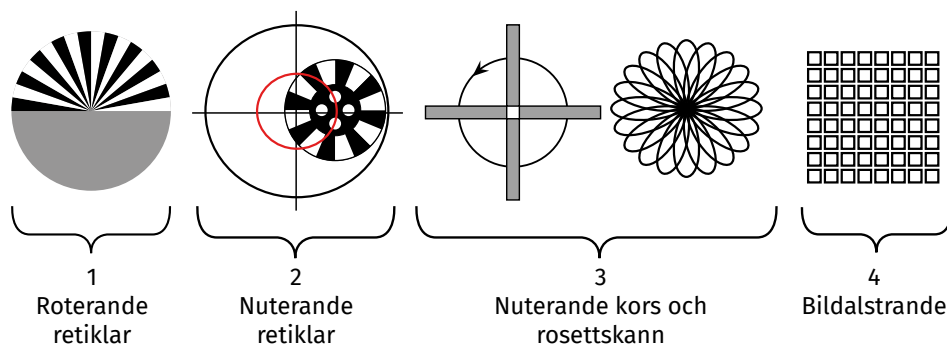


Figur 57. Skiss på ett roterande retikelsystem.

eller av en skannande detektorvektor, som söker av området.

Bilderna förbehandlas bland annat för att minska bruset, förstärka kanterna eller för att upptäcka rörliga objekt (bakgrundssubtraktion). Sedan genomförs segmentering för att hitta intressanta områden och detektera möjliga mål. För att klassificera målen kan till exempel AI användas. Val av mål kan göras av en operatör/skytt eller självständigt av systemet.

Följning kan ske genom en av flera principiella metoder, till exempel korrelation eller centroid. Korrelation bygger på att en referensbild tas (när målet pekas ut) och jämförs med nästa inlästa bild från sensorn. Den del av bilden som matchar bäst mot referensbilden blir följepunkt.



Figur 58. Olika IR-målsökare indelade efter generation.

Uppdatering av referensbilden kan ske kontinuerligt under följningens gång. I en centroidmålföljare försöker man med hjälp av algoritmer hitta och följa ett objekts tyngdpunkt.

Bildalstrande målsökare kräver mer signalbehandling, men ger ett större skydd mot motmedel och störningar. Utvecklingen av algoritmer för såväl målval som målföljning gör stora framsteg, till exempel med stöd av AI.

Aktiva system

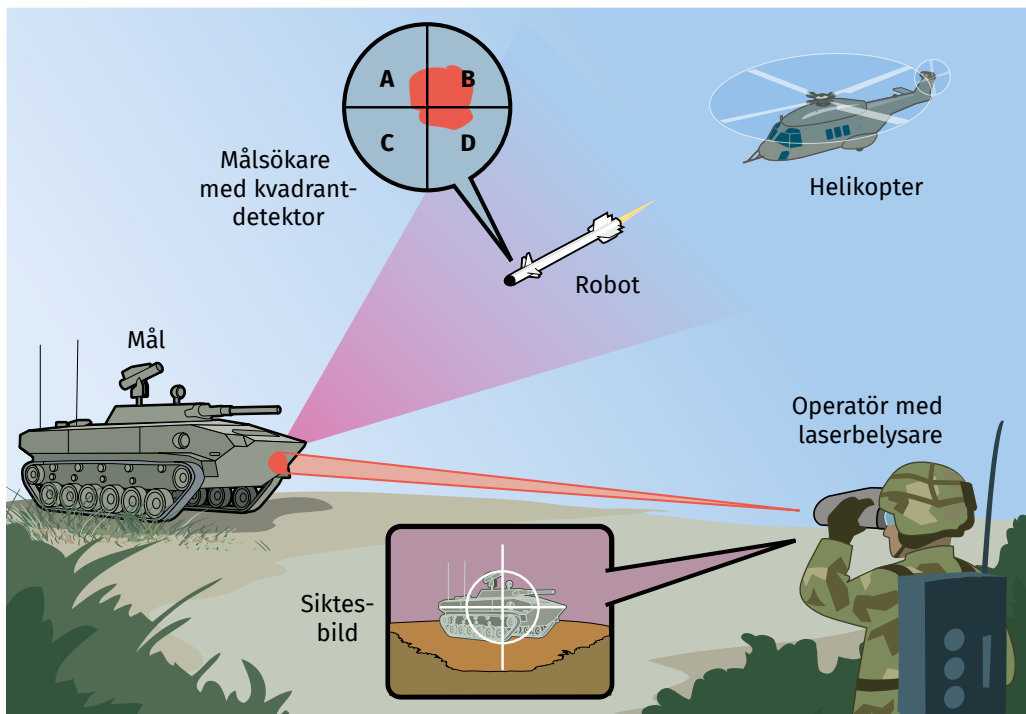
En aktiv EO-sensor är en optisk sensor som mäter reflekterad eller direkt strålning från en egen belysare. Den första militära tillämpningen var avståndsmätning, följt av målinvisning, styrning av robotar med ledstråle samt som sensor i zonerör. Avbildande lidar (Light Detection and Ranging) och optikspaning är andra tillämpningar.

Laserbelysare

Laserbelysare används för att öka precisionen hos robotar, glidbomber och artillerigranater.

Principen för en laserbelysare är enkel. En laser belyser det tilltänkta målet. Sedan styr, till exempel en robot, mot den laserfläck som reflekteras från målet. Målsökaren i roboten består oftast av en kvadrantdetektor. Fyra detektorer registrerar bilden av laserfläcken. Robotens styrning via roder gör att den riktar sig mot fläcken och håller den i centrum.

De lasrar som används är i de flesta fall pulsade Nd:YAG-lasrar. Karakteristiskt för belysarlasrar är hög effekt och mycket smal lob, kring 0,1 mrad (1 mrad motsvarar cirka 1 streck). I belysnings-system på rörliga plattformar, som flygplan och helikoptrar, används lasern tillsammans med IR- eller TV-kameror för att identifiera och följa mål efter att låsning har skett. Lasern riktar hela tiden mot centrum av synfältet för det siktesystem (IR/TV) som används. På så sätt kan laserfläcken hållas på målet även under snabba manövrer. För att öka störskyddet är belysningen kodad. Belysare och vapenbärande plattform behöver inte vara densamma, se figur 59.



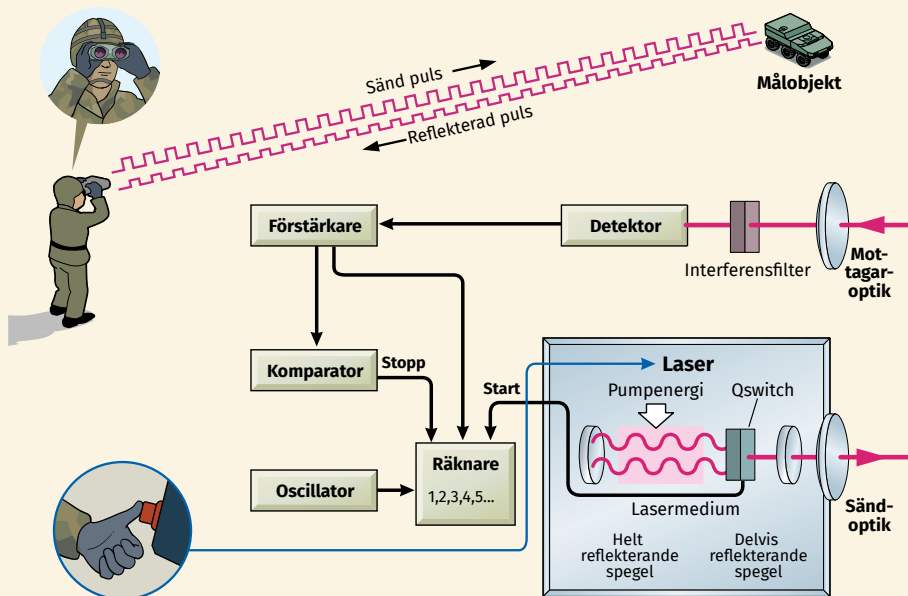
Figur 59. Exempel på laserbelysare.

Laseravståndsmätare

En signal skickas till en laser som sänder en eller flera korta pulser när ett avstånd ska mätas. Samtidigt startas ett räkneverk som räknar pulser från en oscillator. Mottagarens lins fångar upp den reflekterade laserstrålningen och samlar den på en fotodetektor. Där genereras en signalström som med hjälp av en förstärkare förvandlas till en spänning. Den jämförs sedan med en tröskelspänning i en komparator.

Om signalnivån överskrider tröskelspänningen sänds en stoppuls till räknaren. Antalet klockpulser som förflutit är proportionellt mot avståndet enligt $R = Nc/2f$, där R betecknar avståndet, c ljushastigheten (cirka $3 \cdot 10^8$ meter/sekund), N antalet klockpulser och f klockfrekvensen.

Typisk räckvidd för en laseravståndsmätare är 10–20 kilometer vid god sikt. Avståndsmätare med lägre prestanda baseras ofta på diodlasrar som sänder ett stort antal pulser med låg pulsenergi som medelvärdesbildas. Dessa är betydligt svårare att upptäcka med en laser-varnare.



Figur F9. Principen för laseravståndsmätare. I figuren visas ett exempel på en möjlig laser, men det finns andra alternativ.

Laserledstråle

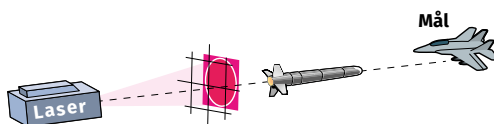
När en robot har skjutits iväg sänds en laserstråle mot en detektor i robotens bakre del, vilket är principen för ledstrålesystem. Laserstrålen är kodad över tvärsnittet så att roboten kan avgöra var i strålen den befinner sig och därmed styra mot centrum av strålen. Roboten styr hela tiden dit laserstrålen pekar. Eftersom detektorn sitter i robotens bakre del och blir direkt belyst av lasern behövs en lägre lasereffekt (cirka 10 000 gånger) jämfört med till exempel laserbelysar-system, vilka förlitar sig på reflekterad strålning. Placeringen av detektorn gör systemet svårstört eftersom den är riktad från målet. Ett exempel på ett sådant system visas i figur 60.

Lidar

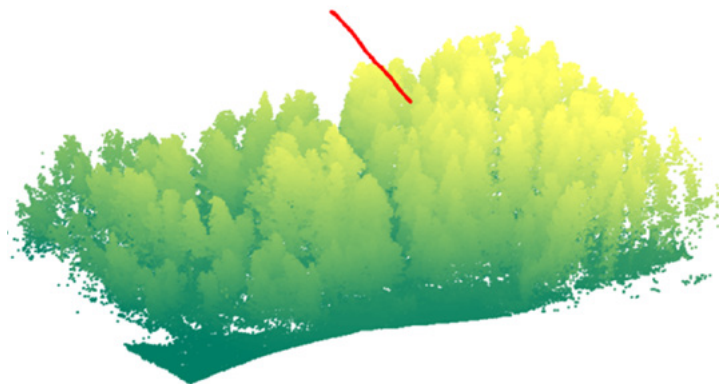
Till skillnad från passiva bildalstrande sensorer kan en lidar, i likhet med en radar på radiofrekvenser, bestämma ett måls avstånd och hastighet. Lidar bygger på samma princip som laseravståndsmätare. Skillnaden är att flera pulser

skickas ut så att systemets synfält oftast skannas eller sveps över en scen, till exempel för att detektera eller lokalisera mål.

En lidar kan ge hög upplösning och kan användas för 3D-avbildning av ett objekt. Figur 61 visar en 3D-modell som ett punktmoln i tre dimensioner, som har samlats in från en lidar integrerad i en UAV. En lidar kan användas som underlag för klassificering eller till och med identifiering, och kan skilja ut mål från terrängen. Lidar kan "se" genom små mellanrum i vegeta-



Figur 60. Principen för ett laserledstrålesystem. Lasern ger en rums-tidsmodulerad stråle som medför att roboten som har en laserdetektor baktill vet sitt läge relativt syftlinjen.



Figur 61. 3D-modell presenterad som ett punktmoln. Punktmolnet är baserat på en lidarmätning från en UAV över ett skogsavsnitt. Den röda vektorn visar farkostens flygrutt.

tion eller kamouflage och lösa upp objekt på olika avstånd. Det kan ge information om delvis skydda objekt. En vanlig våglängd för lidartillämpningar

i luft är 1,5 μm . Den kan även integreras med en passiv bildalstrande sensor, typ FLIR (Forward Looking InfraRed).

Elektromagnetisk stödverksamhet

Optikspanare

Med en optikspanare kan man upptäcka elektrooptiska system. Optikspaning bygger på principen att en laser, som belyser en optisk sensor inom dess våglängdsband, ger upphov till en retroreflex (kattögereflex) om lasern befinner sig inom sensorns synfält. Även med lasern strax utanför synfältet kan reflexen vara betydligt starkare än diffusa reflexer från den omgivande bakgrunden. En optikspanare utnyttjar retroreflexen för invisning och följning.

Optikspanaren består i grunden av en laser som belyser scenen antingen genom skanning med en smal laserstråle eller ”flodbelysning” av ett större område samtidigt. Om det finns ett elektrooptiskt system inom det skannade området kan man få en retroreflex. Den gör det möjligt att bestämma läget med stor noggrannhet. Retroreflexen detekteras antingen med en avbildande sensor, se figur 62, eller med en detektor som mäter in riktningen (ibland även avstånd) till retroreflexen.



Figur 62. NVG-bild av retroreflektion från en fältskikare på två kilometers avstånd.

Varnarsystem inom det elektrooptiska området

Funktionen för ett varnarsystem är att detektera inkommande hot och varna plattformen som ska skyddas. Ett typiskt scenario innehåller följande delar: en plattform som ska skyddas, ett omedelbart hot och en omgivande miljö, som innehåller olika händelser och objekt, och som ska skiljas från själva hotet.

UV-baserad robotskottvarnare

En varnare för fientliga robotskott kan använda det solblinda UV-bandet vid cirka 0,20–0,28 μm . Fördelen med det bandet är att det har väldigt lite störande bakgrundsklotter, vilket gör det enklare att upptäcka inkommande robothot. UV-varnaren detekterar flamman från robotens raketmotor och kan med hjälp av signalbehandling avgöra om det är ett hot för den egna plattformen.

IR-baserad robotskottvarnare

En annan metod för att upptäcka robothot är IR-baserade robotskottvarnare som detekterar robotens strålning inom MWIR. IR-varnare lider generellt av betydligt mer klotter, då bakgrunden emitterar inom detta band. Problemet går att lösa med modern signalbehandling som kan avgöra vad som är klotter respektive inkommande robothot.

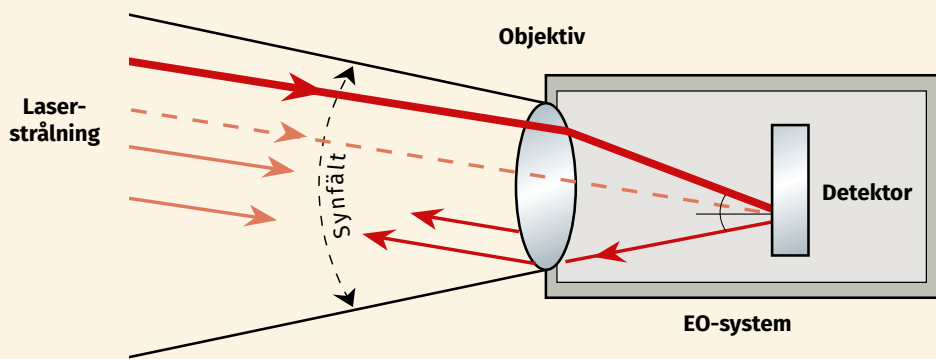
IRST

Infrared Search and Track (IRST) är IR-baserade sensorsystem för autonom detektion och följning av mål och kan förekomma både på flygande, marina och markgående plattformar. Systemen skannar typiskt över en relativt stor sökvoly, som kan smalnas ned vid behov av högre uppdateringsfrekvens. IRST-system verkar vanligtvis

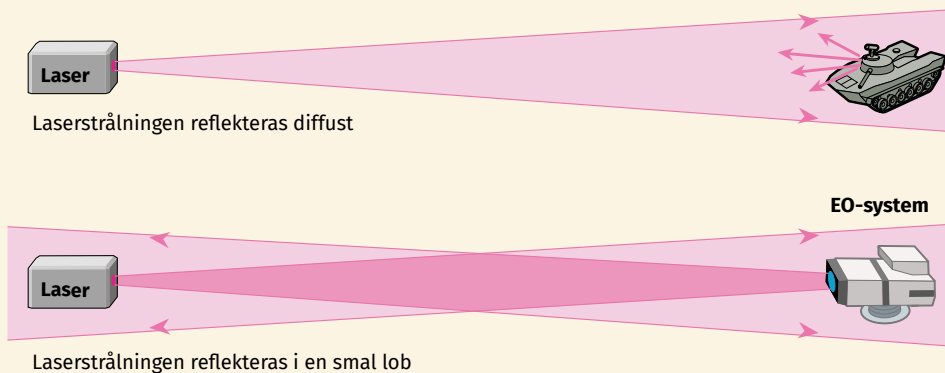
Retroreflektion

När en laser belyser ett objekt reflekteras laserstrålen. Normalt är reflektionen diffus och endast en liten del av den reflekterade strålningen kommer tillbaka till laserkällan. En retroreflex uppstår när man använder elektrooptiska system med detektor eller kikarsikten med streckplattor. Det innebär att en del av den strålning som träffar optiken

fokuseras och reflekteras tillbaka. Vid retroreflektion är signalen typiskt många storleksordningar större än vid diffus reflektion. Retroreflektion kan uppstå i alla typer av optiska sikten (även IR) förutsatt att den belysande våglängden transmitteras och fokuseras i siktet.



Figur F10. Princip för retroreflektion.



Figur F11. Diffus reflektion och retroreflektion.

Laservarnare

Laservarnarens primära uppgift är att detektera pulssade lasrar som används för avståndsmätning, semiaktivt laserstyrda robotar, glidbomber och artillerigranater samt robotar som styrs med laserledstråle. Förutom dessa hot kan man även upptäcka olika typer av system för spaning och lidar, men även pulssad bländande laser och laserbaserade störsystem.

Laservarnare finns hos allt från enskilda soldater till större fartyg. Komplexiteten varierar från en enkel detektor, som bara indikerar i en grov vinkelsektor, till system med många sensorer och noggrann inmätning av hotets riktning och som även möjliggör klassificering.

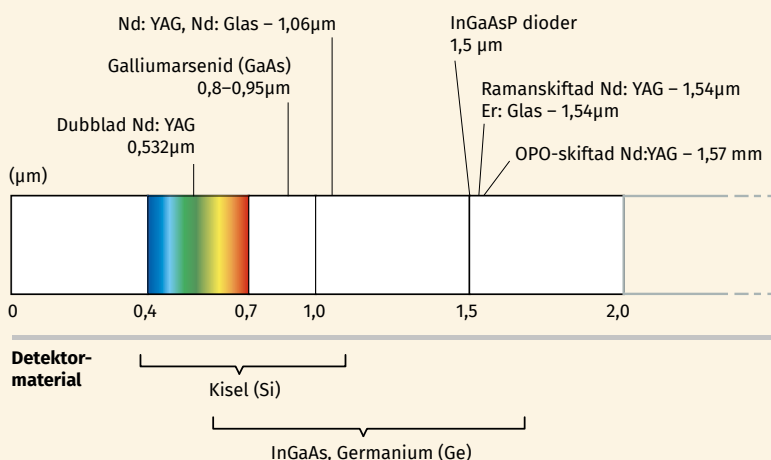
Vinkeltäckningen för en laservarnare varierar beroende på vilken plattform som skyddas (fordon, helikopter eller fartyg). Vanligtvis krävs 360° vinkeltäckning i horisontalplanet. Invisningssektorn varierar från $\pm 45^\circ$ för de enklaste systemen ned till $\pm 1^\circ$ för de mer avancerade.

Laseravståndsmätare och belysare har smala laserlober. I vissa fall är strålens diameter så

liten som 1 meter på 10 km avstånd. Spridning i atmosfären medför dock att en laservarnare kan detektera laserstrålning från avståndsmätare och laserbelysare, även om de rikts tiotals meter vid sidan av laservarnaren.

Laservarnare kan skilja på laseravståndsmätare, laserbelysare och ledstrålelasrar genom att mäta pulsrepetitionsfrekvensen (PRF) hos inkommande laserpulser. Mer avancerade system använder biblioteksfunktioner för identifiering av specifika system, framför allt ledstrålestyrda robotar. Förutom PRF kan även våglängdsinformation utnyttjas för identifiering. Det är komplicerat och ovanligt att noggrant bestämma våglängden hos en hotlaser i en laservarnare. En del varnare utnyttjar optiska filter i ett antal band för att kunna bestämma våglängden.

Det finns en rad potentiella källor till falsklarm, till exempel solreflexer, blyxtljus, mynningsflammar, eldsvådor och elektromagnetisk interferens. Falsklarm undertrycks med hjälp av avancerad signalbehandling. Tekniker som används är bland annat att skilja signaler åt baserat på tid, koherens och våglängd.



Figur F12. Vanliga hotlasrar samt olika detektormaterial som utnyttjas i laservarnare.

i MWIR- eller LWIR-området, men kan också förekomma med känslighet i båda (s.k. dualband-system) för falsklarmsreducering. Ibland verkar systemen även tillsammans med ett optiskt sikte för förbättrad klassificering och identifiering av upptäckta mål.

Laservarnare

En laservarnares uppgift är primärt att detektera ”hotsystem” som använder laser för inmätning

och vapenstyrning, men kan också upptäcka olika typer av aktiva spaningssystem. En laservarnare måste kunna täcka ett stort våglängdsområde, ha stor vinkeltäckning, hög känslighet och samtidigt generera få falsklarm. Laservarnare finns på många olika plattformar, till exempel stridsfordon, helikoptrar, flygplan och fartyg inklusive ubåtar. De kan även användas på mobila installationer, fasta anläggningar eller av enskilda soldater.

Elektromagnetisk attack

Det finns ett antal olika system med både aktiva och passiva tekniker för att störa elektrooptiska system. Lasersystem kan störa eller till och med förstöra sensorer och målsökare. Det finns även facklor som genererar en IR-signatur för att vilseleda hot. Enkla fysiska skenmål eller avskärmande rök eller vattendimma kan också dölja objektet som ska skyddas.

Aktiva metoder

Laserstörare

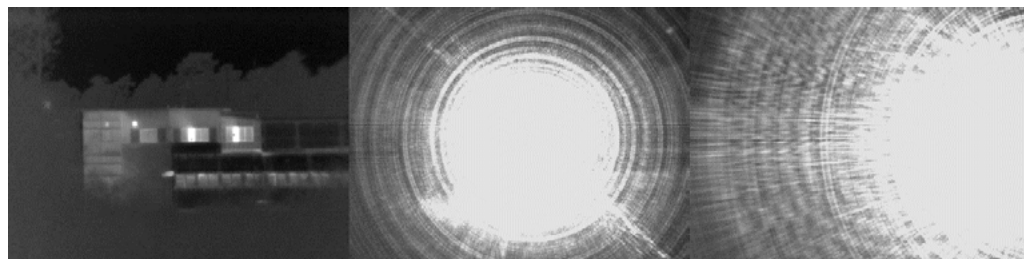
Laser som motmedel mot optiska sensorer i vapen- och eldledningssystem ska störa, blända, vilseleda eller förstöra sensorn för att avvärja eller motverka ett hot. Laser kan till exempel användas för att skydda plattformar genom att störa ut målföljaren hos det hotande systemet. För en lyckad störning krävs att lasern utnytt-

jar en våglängd som ligger i det intervall inom vilket sensorn är känslig, se figur 63.

Invisning och inriktning av en störlaser kan ske på olika sätt, alltifrån manuell inriktning till information från kamera, robotskottvarnare, lasermålföljare, lidar, laservarnare eller radarsystem. En störlaser kan även vara sammonterad med eldrörsvapen eller robotlavett. Den kan då utgöra en tillsatsfunktion när målet är bortom vapnets räckvidd. Laserstörare utnyttjas ibland tillsammans med optikspanare.

Facklor

Facklor är skenmål som huvudsakligen är avsedda att lura elektrooptiska hotsystem, som inte är bildalstrande. Facklor är pyrotekniska anordningar, vilka emitterar sin energi i målsökarens våglängdsområde. De var från början avsedda för att skydda flygplan.



Figur 63. Laserbländning av en IR-kamera inom området 3–5 μm . De tre bilderna visar från vänster till höger det ostörda fallet, laserstörning inom synfältet samt laserstörning 6 grader utanför synfältet.

DIRCM

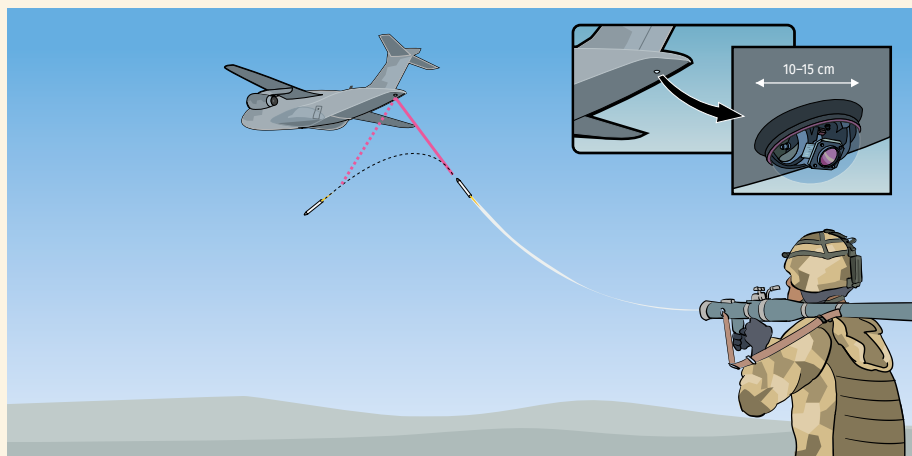
Ett modernt skydd av flygande plattformar mot manburna robotar med IR-målföljare (MANPADS, MAN Portable Air Defence Systems) är DIRCM (Directed InfraRed Counter-Measures). Flera länder tillverkar DIRCM-system. Dessa installeras internationellt på allt fler helikoptrar, transportflygplan och andra större och långsamma flygplan. Än så länge används DIRCM inte på stridsflyg, vilket har både tekniska och taktiska orsaker.

DIRCM är ett reaktivt motverkanssystem som aktiveras när robotskottvarnaren har upptäckt ett inkommande hot. Synfältet för en målföljningskamera och en lasersändare med våglängd inom robotmålsökarens känslighetsband riktas då in mot hotet via ett spegelbaserat pekhuvud. När målföljaren har låst på den hotande roboten tänds lasern och belyser robotmålsökaren. Lasern skickar ut ett pulsmönster (störkod), som efterliknar signalen från ett mål i kanten av synfältet för robotens målsökare. Detta fungerar för robotmålsökare som kodar riktningen till målet med en tidsvarierande signal, vilket innebär IR-målsökare med enfärgsdetektor.

För flerfärgsmålsökare krävs en laserkälla per band, som emitteras via samma pekhuvud. På grund av den smala laserloben kan en hög stör-till-signalkvot relativt plattformssignaturen uppnås med bara några watts lasereffekt. Med rätt störkod för det inkommande hotet överröstas signaturen från plattformen och robotmålsökaren styr efter störkodens pulsmönster och svänger bort från plattformen. Fel störkod förstärker plattformssignaturen och robotmålsökaren styr mot laserkällan. DIRCM-systemet har därför ett bibliotek med störkoder för kända hot, och koderna provas en i taget tills någon fungerar.

Viktiga fördelar med DIRCM-system är snabb och effektiv verkan mot vissa hot. Jämfört med till exempel facklor har man obegränsat antal aktiveringar (inget begränsat magasin) och här finns ingen brandfara, som vid pyroteknik.

Utvecklingen inom DIRCM går mot mindre och lättare system för placering på mindre plattformar samt verifiering av verkan för att snabbare kunna växla mål vid multipla robothot.



Figur F13. Illustration av MANPADS-hotet. Bilden visar hur ett DIRCM-system kan vara installerat på ett transportflygplan och avleda inkommande robothot.

Syftet är att facklorna ska vara mer lockande för en målsökare än det riktiga målet så att roboten jagar facklan i stället. Facklorna måste ha en spektral fördelning anpassad till den hotande sensorn för att det ska lyckas. Facklornas intensitet måste också vara högre än målets. Det behövs också en snabb uppblomningstid (tid från initiering eller fällning tills att facklan har full intensitet) och en tillräckligt lång brinntid. För att en eller flera facklor ska ha effekt måste de vara tillräckligt skilda från målet så att roboten inte kommer nära. Därför bör utskjutningsvinkeln vara anpassad till den riktning som hotet kommer från. Exempel på fällning från flygplan visas i figur 64.

Utvecklingen av facklor och störskydd i målsökarna har gått hand i hand. De enklaste facklorna är heta och strålar bredbandigt. De sänder starkt (strålningsövervikt) i flera våglängdsband och används mot målsökare utan störskydd. Flera andra facklor har utvecklats för att motverka olika typer av störskydd. Det finns spektralt anpassade facklor, där energin i facklan efterliknar ett mål i olika våglängdsband. Aerodynamiskt stabiliserade facklor har viktfördelning och eventuell raketdrift som påverkar hur de faller. Facklor används för skydd av flygplan, helikoptrar och fartyg.

Ett annat motmedel är en stor mängd flarn med material som självantänder när det kommer i kontakt med luftens syre (pyrofort material). Detta skapar ett skenmål med större utbredning än en konventionell fackla.

Kombinerad metod

Ett motmedel mot elektrooptiska system för svenska ytstridsfartyg är Multi Ammunition Softkill System (MASS). För att ge effekt i flera våglängdsområden består varje skenmålsgranat av såväl en fackla som en last med remsor (för verkan inom radarområdet). För att skydda fartygen och ge ett tillräckligt stort skenmål skjuts ett antal skenmålsgranater i avsikt att kunna lura målsökare. Exempel på detta visas i figur 65.



Figur 64. Flygplan Gripen C som fäller facklor.



Figur 65. Fartyg som skjuter ut 16 skenmålsgranater. Notera att skenmålet tidvis täcker fartyget. Foto: Rheinmetal Waffe Munition GmbH.

Vilseledande laser

Vilseledning av laserbelysare kan åstadkommas genom att utnyttja data från en laservarnare för att med egen laser vilseleda laseravståndsmätare och laserbelysarsystem. När en avståndsmätare laserpuls upptäcks kan den egna lasern sända ut en egen puls som ger avståndsmätaren ett extra falskt svar. Ett laserbelysarsystem kan vilseledas genom att skenfläckar skapas som de lasersökande vapnen kan styra mot. För att det ska lyckas krävs en flexibel laser som kan kopiera koden från laserbelysaren. Kopplas lasern till en optisk fiber som läggs ut, se figur 66, kan ett effektövertag skapas för den falska laserfläcken.

Passiva metoder

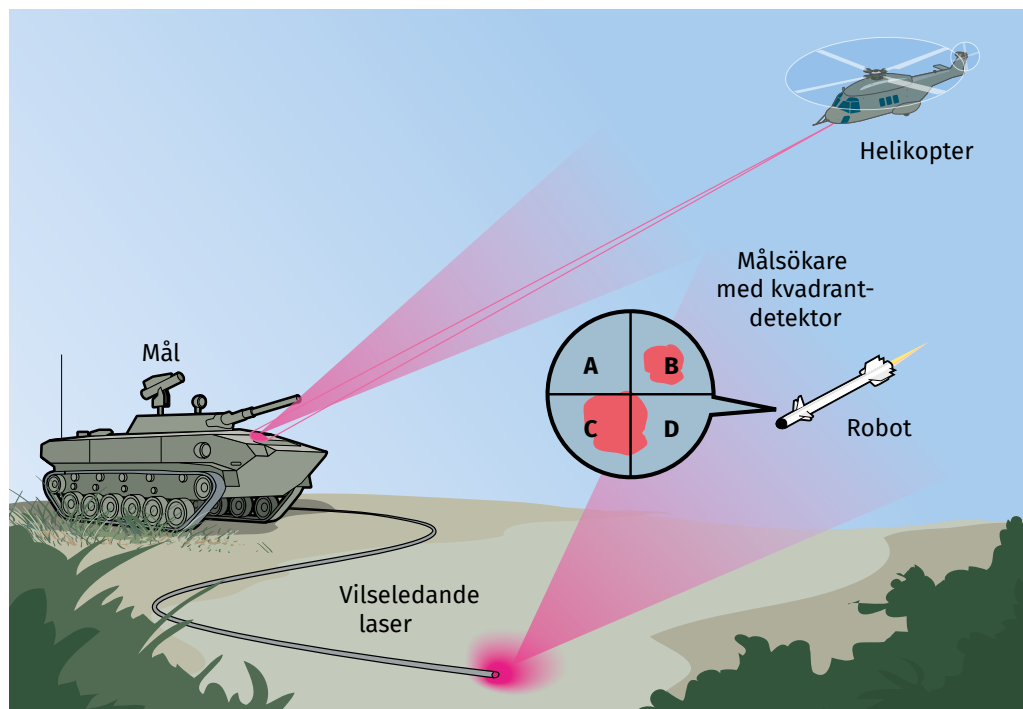
Skenmål i 2D och 3D

Skenmål kan vara två- eller tredimensionella konstruktioner som fysiskt efterliknar skarpa

objekt. Även enkla skenmål kan ha effekt, något som exempelvis visades under kriget i Kosovo. Skenmålen signaturer bör överensstämja med de verkliga objekten vad gäller våglängd och signalstyrka. Utöver en visuell signatur krävs främst en relevant signatur inom IR-området. Det går att åstadkomma genom att använda enklare värmekällor. Denna typ av skenmål är främst tänkta att användas mot spaningsensorer. Prismor som ger retroreflex kan användas som skenmål mot laser. Önskvärt är att skenmålet simulerar aktiv sändning som överensstämmer med vad det verkliga målet skulle ha genererat. Exempel på uppblåsbart skenmål visas i figur 67.

Avskärmning

Avskärmning innebär att siktlinjen mellan målsökare och plattform bryts, till exempel med rök, facklor eller vattendimma, som täcker den



Figur 66. Vilseledning av laserbelysarsystem.

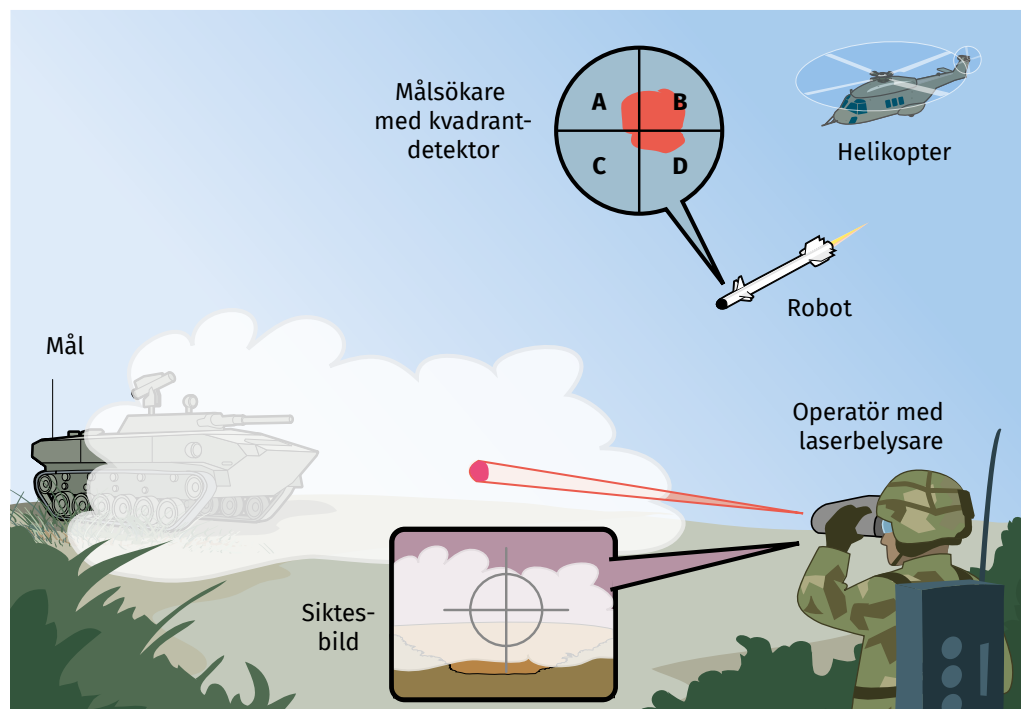
plattform som ska skyddas. Det är viktigt att partikelstorleken hos den avskärmande röken eller vattendimman minst motsvarar våglängden som ska dämpas ut. Om en rök önskas som kan dölja inom 8–12 μm bör storleken hos partiklarna i röken ligga kring 10 μm .

I fallet med stridsfordon sitter normalt två kastare på tornet, en på vardera sidan om eldröret. En insats består av 6–8 rökgranater som kompletteras med undanmanöver. Om hotet är en laserstyrd robot gör röken dels att siktlinjen skymms, vilket ger problem för den operatör som ska följa målet, dels att laserstrålen reflekteras i rökmolnet. Det ger i sin tur upphov till en geometrisk felvisning som kan leda till att roboten missar, se figur 68.

Vattendimma bildas genom att vatten trycks ut ur ett antal munstycken, som är anpassade för att skapa vattendroppar av rätt storlek. Exempel på detta visas i figur 69.



Figur 67. Exempel på uppblåsbart skenmål.



Figur 68. Rök i avskärmande syfte. Här flyttas punkten där laserstrålen reflekteras och sikten blockeras så att bilden inte syns tydligt.



Figur 69. Vattendimma applicerat på ett stridsfordon. Här avskärmas vagnen från hot uppifrån, till exempel slutfasstyrda granater. Det tar cirka tre sekunder innan vagnen är helt täckt av vattendimman (bilden till höger).

Elektromagnetisk protektion

Störskydd

Många passiva målsökare använder störskydd för att skydda sig mot elektrooptiska motmedel. Moderna system kan ha avancerade störskydd, där man diskriminerar mål som inte har vissa specifika egenskaper. Enklare system använder ofta varianter av de metoder som beskrivs i resten av det här stycket.

Målsökaren kan detektera att den är utsatt för störning på flera olika sätt, till exempel genom att:

- upptäcka snabba ökningar i den inkommande strålningsenergin (intensitetsstegring)
- studera energiförhållandet i flera våglängdsområden (multispektral).
- detektera följehastighetsändringar (kinematisk).
- detektera flera mål inom synfältet (spatial).

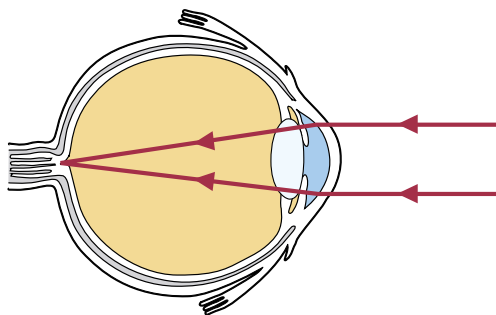
När målsökaren detekterat att den är utsatt för störning aktiveras motåtgärder. Sektordämpning innebär att en del av synfältet, där motmedlen oftast är, dämpas. Blind styrning eller minnesgång betyder att roboten blint (det vill säga på den senaste kursen) fortsätter sin bana en kort tid i förhoppningen att motmedlet (men inte målet) ska vara borta ur synfältet då styrningen

återupptas. ”Push-pull” innebär att målsökaren drivs från det starkare mot det svagare målet. ”Push-ahead” innebär att målsökaren styrs ut i målets senast bestämda färdriktning, när ett motmedel upptäcks, och att man hoppas att motmedlet ska hamna utanför synfältet. Det får till följd att detektorns utsignal påverkas mindre av motmedlet.

Laserskydd

Laserhotet ökar allt mer till följd av det ökande antalet lasrar och tillämpningar som blivit aktuella i militära sammanhang. Det behövs skydd även mot det hot som oavsiktlig laserbelysning innebär; till exempel har flygplansbesättningar utsatts för belysning med relativt enkla lasrar. Behovet av laserskydd blir ännu tydligare när systemen avsiktligt ges tillämpningar som vapen.

Laserbelysning riktad mot ögon kan medföra synnedsättning eller blindhet. Hornhinnan och linsen kan liknas vid ett brännglas som fokuserar laserstrålningen till en punkt på näthinnan, där intensiteten förstärks i storleksordningen 100 000 gånger, se figur 70. Det gör att den skadas betydligt lättare, trots att näthinnan inte är mer skadkänslig än hud. Förstorande optik,



Figur 70. Ögats lins och hornhinna koncentrerar laserstrålningen.

som kikare eller sikte, ökar skaderisken ytterligare eftersom koncentrationen på näthinnan då blir ännu kraftigare. Motsvarande förhållanden gäller även för elektrooptiska sensorer, där ögats lins motsvaras av ett objektiv som fokuserar strålningen på en detektor.

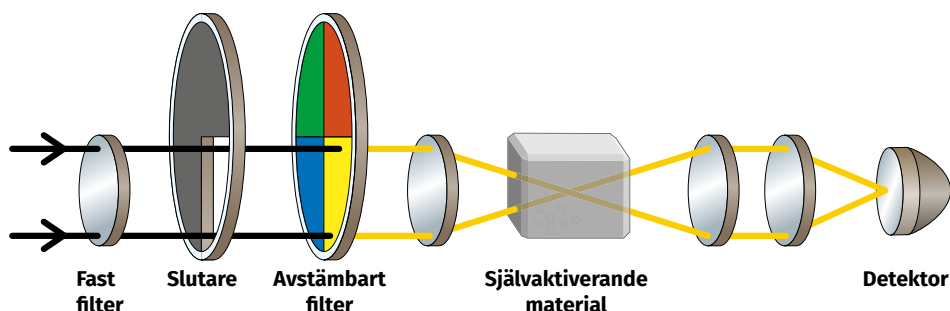
Förstorande optik ökar risken för att bli upptäckt av optikspaning, vilket i sin tur ökar risken för laserangrepp och skada. Taktiska skydd går därför ofta ut på att minska risken för upptäckt, bland annat genom att minimera exponeringen av den optiska utrustningen och i övrigt begränsa

den visuella kontakten med omvärlden. Även vilseledning, till exempel skenmål, kan ses som ett taktiskt skydd.

De tekniska skydden kan i sin tur delas in i tre kategorier: statiska, styrda och självaktiverande. Statiske skydd förändras inte under ett laserangrepp, till exempel fasta spektrala filter och indirekt seende. Fasta filter utgör ett gott skydd under förutsättning att hotets våglängd är känd. De är också användbara för att filtrera bort våglängder utanför det område som utnyttjas av sensorn eller ögat. Därigenom reduceras risken för upptäckt och skada orsakad av strålning som inte kan detekteras. Figur 71 visar exempel på skydd mot laserhot.

Indirekt seende, till exempel via videokamera, bildskärm eller bildförstärkare, kan skydda ögonen även mot okända våglängder. Indirekt seende ger dock sämre upplösning och mindre synfält än direkt seende och oftast försämras färgseendet. Elektrooptiska sensorer är dessutom ofta mer känsliga för bländning än ögat.

Det krävs att ströljuset i sensorns optik minimeras för att ge skydd mot störning av en optisk sensor från laserkällor utanför synfältet. Det kan göras genom bländare och motljusskydd



Figur 71. Figuren illustrerar ett skydd mot laserhot. Ett fast filter blockerar de våglängder som inte ger någon optisk information. En kort och oväntad laserpuls med hög energi dämpas kraftigt av ett självaktiverande skydd i ett mellanfokus. Ett skydd mot efterföljande laserpulser ges om det avstämbara filtret snabbt kan ställa om och blockera laservåglängden. Då blir det möjligt att fortsätta informationsinhämtningen. I vissa fall kan det vara önskvärt att utesluta alla våglängder, vilket går att göra genom att aktivera slutaren.

samt ytbeläggningar som minskar spridning och reflektion av ljus. Det är också viktigt att tänka på skydd mot upptäckt och konstruera en sensor med så liten retroreflex som möjligt (minimal lasermålarea).

Styrda skydd, till exempel slutare och styrbara filter, kan förändra sina optiska egenskaper på kommando från en yttre styrsignal, som en laservarnare. Utvecklingen går mot styrda elektrooptiska komponenter som är snabbare än mekaniska. Höga krav ställs på omslagstid och dämpning. Under tiden slutaren är aktiverad kan man inte se genom systemet. Ett avstämbar filter ska i princip ge samma skydd mot laser som en slutare, men släppa igenom ofarliga våglängder. Då får man ett skydd som gör det möjligt att använda optiken trots kontinuerlig belysning.

Självaktiverande material skyddar automatiskt ögat eller sensorn, utan påverkan från yttre styrsignaler. Med ökande intensitet hos ljuset minskar transmissionen för dessa så kallade optiskt icke linjära material. Effekterna kan vara tillfälliga såväl som permanenta. Optiska begränsare minskar hur mycket strålning som släpps igenom under en tid, däremot stoppar optiska säkringar strålningen helt när den blir för stark.

Det krävs ofta hög energinivå för att de självaktiverande skydden ska fungera. Därför måste de placeras i ett mellanfokus. De är mycket snabba och kan skydda mot skada, men inte mot störning och bländning. Operativt dominerar fortfarande statiska filter som är enkla och robusta. ■

Telekrig mot laser- kommunikationssystem

Laserkommunikation

Ända sedan lasern uppfanns runt 1960 har tankar funnits på att använda den för optisk kommunikation. I mitten på 1970-talet skedde också en explosionsartad utveckling av optiska fibrer nästan helt inriktad mot detta. För trådlös förbindelse är fortfarande laserkommunikation ett kraftfullt alternativ till radio. Optisk trådlös kommunikation i en bredare bemärkelse omfattar lösningar som inte nödvändigtvis använder laser och där ljuset sprids ut mer. Sådana lösningar används främst på kortare avstånd, inomhus eller under vatten.

Med laserkommunikation menas länkar som upprättas med riktade strålar, laserstrålar, genom luften eller i rymden, se figur 72. Komponenterna bygger inte sällan på samma teknik som för fiber-optisk kommunikation. Laservåglängden ligger typiskt kring $1,5\text{ }\mu\text{m}$ där transmissionen genom atmosfären är hög. Det förekommer också system baserade på andra våglängder, till exempel kring $0,8$ och $1,3\text{ }\mu\text{m}$, där transmissionen också är hög.

Framstegen inom rymdområdet har varit omfattande under det senaste årtiondet. Laserkommunikation är nu en etablerad teknik för anslutning mellan satelliter och även från satelliter ner till jorden. Starlinks nätverk av satelliter har till exempel flera tusen så kallade optiska terminaler för dubbelriktad kommunikation med en datahastighet på 100 Gigabit per sekund (Gbps). Det är en fördel att rymden saknar atmosfär, som naturligt begränsar ljusets utbredning. Satelliter är också relativt stabila plattformar som gör det möjligt att rikta laserstrålen mycket exakt. Det gör att väldigt smala laserstrålar kan användas

och optiska signaler kan överföras över mycket långa avstånd.

Teknikutvecklingen i rymden gör att operativa system snart kan introduceras på flygande plattformar i luften. Detta har redan gjorts och visats upp i demonstrationer genom åren. Turbulens, dimma och vibrationer gör det mer utmanande i luften, trots de relativt korta avstånden jämfört med i rymden.

Laserkommunikation för fast bredbandsförbindelse genom luften har funnits kommersiellt tillgänglig sedan början på 2000-talet. Sådana länkar har en räckvidd på uppemot fem kilometer och har aktiv siktlinjjustering. De har även en relativt stor strålningslob. Terminalerna har oftast flera laser- och mottagaraperturer, som är separerade i rummet, för att i likhet med radios MIMO (Multiple Input Multiple Output) motverka den fädnings som uppstår av turbulens i atmosfären. De används oftast mellan infrastruktur som byggnader och master. Liknande utrustning finns även för marint bruk på fartyg.

Terminalerna för fasta förbindelser lämpar sig inte för flygande plattformar. Det beror dels på att fasta förbindelser har flera aperturer, dels på att de kan vara för skrymmande. De lösningar som är under utveckling bygger på sändning och mottagning från en gemensam optisk enhet monterad i ett pek huvud som kan peka, följa och läsa, så kallad PAT (Pointing, Acquisition and Tracking), på en annan terminal. Pekhuvudet, som kan vridas i stora vinklar, kombineras oftast med en inre elektromekanisk spegel som kan finjustera laserstrålens riktning i snabb

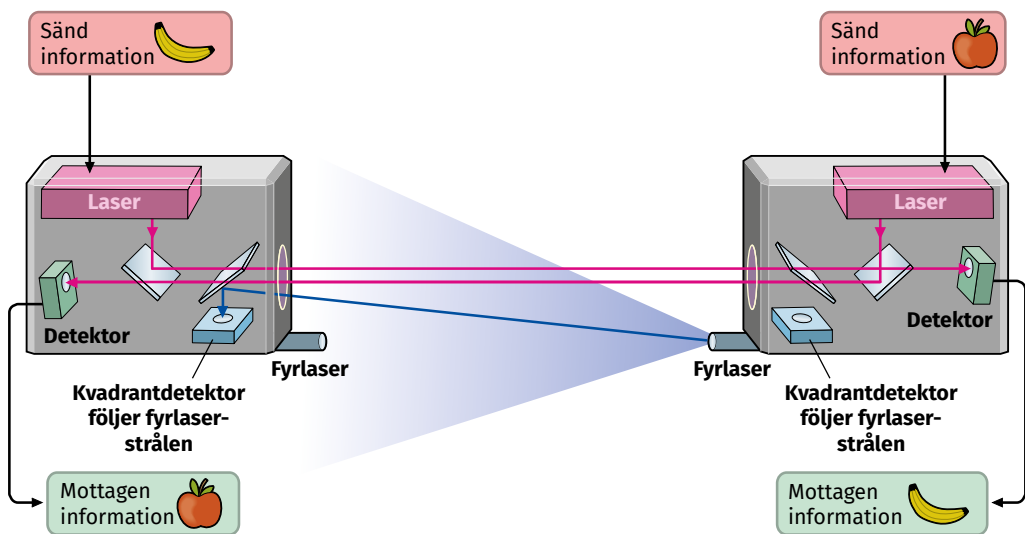
takt. Det gör att systemet kan kompensera för vibrationer och turbulens i luften som annars skulle få strålen att peka fel. Pekfunktionen har avgörande betydelse för länken och är kanske den största tekniska utmaningen. Oftast behövs en smal strålningslob och ett litet synfält för mottagaren i kommunikationskanalen för att få önskvärd räckvidd. Lobvinkeln för laserstrålen är typiskt en milliradian (motsvarar en meter på 1 km avstånd) eller mindre. Mottagarens synfält är av samma storleksordning. Det beror delvis på att den använder en liten och snabb optisk detektor tillsammans med en mottagarapertur på två till tio centimeter. Mottagarens inriktning kräver således samma precision som lasersändaren.

Inriktningen av pek huvudet behöver hela tiden få återkoppling genom vinkelangivelser från en riktningvisande detektor. En sådan kan i princip vara en kamera som följer den andra terminalen, men generellt är den lösningen för

långsam och kräver alltför många beräkningar. I stället används kvadrantdetektorer i mottagaren för att mäta riktningen mot en ljuskälla på den andra terminalen. Det finns flera sätt att implementera den här funktionen.

För att underlätta PAT-funktionen kan terminalerna till exempel utrustas med en andra laser, så kallad fyrlaser, med mindre krav på överförd effekt, men med en lobvinkel som är cirka fem till tio gånger större än kommunikationslaserns strålningslob. Strålningen från fyrlasern läggs vid en våglängd, som kan filtreras bort från kommunikationskanalen, och leds genom samma mottagare, men i det här fallet till kvadrantdetektorn. Kanalerna separeras sedan i mottagaren.

Pek huvuden sveper över ett vinkelområde tills dess att respektive fyrlaser detekteras och länken etableras. Det gäller både för den inledande fasen och om lösningen går förlorad. Inledningen är särskilt utmanande eftersom



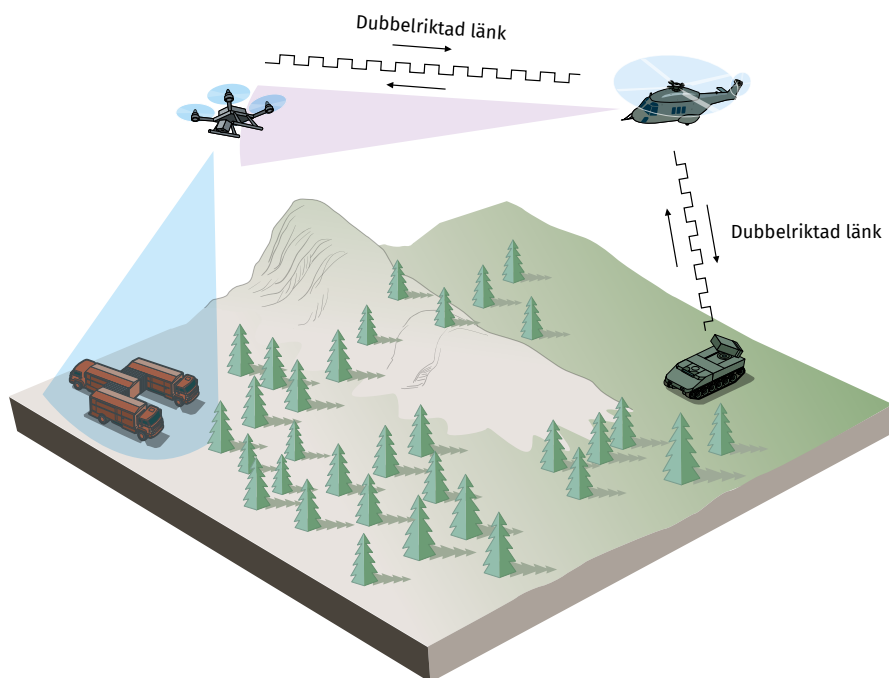
Figur 72. Så här kan en dubbelriktad laserkommunikationslänk se ut. Båda sidorna är utrustade med sändar- och mottagarenhet. Här syns även länkprincip och ingående komponenter.

ingen av terminalerna med säkerhet riktar sin strålningslob mot den motstående terminalen. Olika metoder kan användas för att underlätta den fasen, till exempel adaptiv fyraserlob eller retroreflektorer. En retroreflektor ger ett kraftfullt blänk i retur när laserstrålen träffar, vilket kan användas för följningsfunktionen.

Så fort laserlänken är låst startas överföringen av data. Vanligast är att lasrarnas intensitet moduleras. Mottagarna måste kunna hantera relativt kraftiga variationer i den mottagna optiska effekten, både på grund av inriktningsregleringen och eventuell turbulens. Det går i regel inte att använda standardformat för fiber-optisk kommunikation. En anpassning krävs för att optimera dataöverföringen till den mer varierande kanalen. Det kan till exempel behövas kodning som rättar fel, så kallad omflätning (interleaving), adaptiv sändning och adaptiv tröskelsättning för att upprätthålla en robust dataöverföringslänk.

Med koherent detektion går det även att ändra fas och polarisation. I de mest avancerade systemen kan den utgående laserns vågfront justeras via återkoppling från mottagarsidan. Syftet är att motverka effektvariationer (scintillationer) hos mottagaren. Generellt är länkar med koherent detektion förhållandevis komplicerade och ännu inte utvecklade för att tillämpas på mobila plattformar.

En så kallad retromodulator gör det möjligt att sända information tillbaka mot en belysande terminal genom att använda reflekterad laserstrålning. Det gör att behovet av pek huvud och laser försvinner och man får en väldigt kompakt, enkel och strömsnål terminal. För sändning mot retromodulatorn behöver den kompletteras med en mottagare. Tekniken med retromodulator skulle passa väl för små UAV:er (Unmanned Aerial Vehicle) som inte kan bära mycket last och behöver sända information i hög takt, till exempel som i scenariot i figur 73.



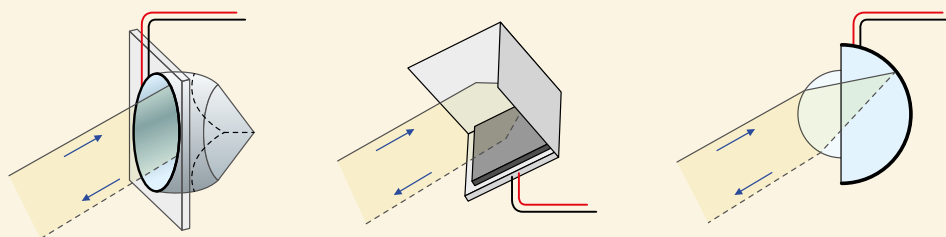
Figur 73. Kommunikation mellan fordon och UAV som använder en flygande plattform som relästation.

Retromodulatorer

Retromodulatorn kombinerar en retro-reflektor med en modulator. Retroreflektorn returnerar strålen tillbaka mot lasersändaren oavsett riktningen in mot den. Modulatorn kodar informationen på strålen som reflekteras tillbaka.

Varje retromodulator har ett visst synfält inom vilket ljus reflekteras tillbaka, vanligen några tiotals grader beroende på typ och upp-

byggnad. Genom att kombinera flera retromodulatorer är det möjligt att täcka ett större synfält. Nackdelen jämfört med traditionell laserkommunikation är kortare räckvidd. Datatakten blir också lägre. Kvantbrunnsmulatorer, som är en teknik under utveckling, ser dock ut att kunna nå en datatakt uppemot 1 Gbps. Tekniken lämpar sig för jämförelsevis små plattformar, till exempel enklare UAV-system, master, bojar och utrustning som bärs av soldater.



Figur F14. Olika principer för en retromodulator; transmissiv modulator, reflektiv modulator och kattögeoptik.

Elektromagnetisk stödverksamhet

Laserstrålarna i en kommunikationslänk är normalt svåra att upptäcka då de breder ut sig i luften. Spridning från små droppar eller partiklar i atmosfären kan dock göra det möjligt att upptäcka strålen från sidan, till exempel vid disigt väder. Den största möjligheten till upptäckt är nära lasersändaren, där intensiteten i laserstrålningen är som högst, eller kring mottagaren, som är belyst av lasern när länken är upprättad.

För en dubbelriktad länk finns både sändare och mottagare i varje terminal. För sändaren är det svårt att undvika viss spridning i en vinkelsektor kring laserstrålen, vilket gör att terminalen kan upptäckas även från sidan. Även laser-

belysningen som träffar mottagaren eller objekt i bakgrunden kan upptäckas. Laserlänkar med den vanligaste våglängden kring $1,5 \mu\text{m}$ syns inte i kameror för det visuella våglängdsbandet. Då behövs särskilda kameror för kortvågs-IR (SWIR) eller motsvarande sensortechnik.

Ett framtida alternativ kan bli att sända vid en längre laservåglängd, till exempel inom våglängdsbandet $9\text{--}12 \mu\text{m}$. Det gör det svårare att upptäcka laserstrålningen på grund av värmestrålningen som finns naturligt i bakgrunden (termisk bakgrund). Dessutom minskar också störningar från atmosfären på grund av turbulens.

Elektromagnetisk attack

Det är svårt att störa en kommunikationskanal med smala sändar- och mottagarlober. En eventuell störlaser måste normalt befinna sig inom ett ytterst begränsat område och inriktningen måste göras noggrant. Dessutom måste den störande lasern sända med samma våglängd som laserlänken för att störningen ska vara effektiv. Länkar som har PAT-funktion blir mer sårbara

eftersom pekfunktionens optiska kanal i regel har ett större synfält. Det gör det lättare att rikta störande laserstrålning mot detektorn. Även här krävs dock att rätt våglängd används. Ytterligare en möjlighet är någon form av hinder mellan laserterminalerna, till exempel kraftig rök. Det kan göra överföringen sämre och göra att länken tillfälligt inte kan nås.

Elektromagnetisk protektion

De flesta kommunikationslänkar via laser förväntas få ett bra inbyggt skydd genom avancerad kodning. I vissa fall kan ändå kryptering av data-trafiken vara nödvändig för att minska risken för signalspaning i underrättelsesyfte (avlyssning).

För att avlyssna en laserkommunikationslänk krävs avancerad utrustning som normalt måste placeras i laserloben och riktas mot sändaren. Det gör att den som försöker avlyssna länken sannolikt röjer sin egen position.

Laserstrålningen som träffar mottagaren kommer oftast att belysa en större yta. För en laserstråle som har en lobvinkel på en mrad (milliradian) ökar till exempel diametern på laserstrålen med en meter per kilometer. Då kommer både farkost och eventuell bakgrund att vara belysta och sprida strålningen i alla riktningar. Rent hypotetiskt skulle en riktigt känslig mot-

tagare kunna riktas in från nära håll intill den spridda strålningen från mottagaren, eller annat objekt i bakgrunden, och på så sätt avlyssna den diffust spridda strålningen. För en kommunikationslänk som arbetar med hög dataakt, till exempel någon Gbps, ger en sådan spridning en alltför låg nivå för att avlyssningen ska fungera.

Det stora synfältet för en terminal baserad på retromodulator blir en nackdel om det finns en risk för avlyssning. Det beror på att moduleringen kan avläsas från en andra belysande laserterminal som befinner sig inom synfältet. Därför behöver en sådan terminal kombineras med en detektor som ger varning för laserbelysning och som också kan användas för att öppna för egna signaler och starta sändningen. En slutare kan också användas för att inte ge en optisk signal, då information inte överförs. ■

Tillämpningar

Även om telekrigföring till stor del handlar om växelverkan mellan tekniska system, eller en duell mellan medel och motmedel, är det viktigaste ändå hur detta sker i en taktisk eller operativ situation. Ett sätt att sätta in tekniken i dess sammanhang är att diskutera telekrig på förbandsnivå. Då blir fokus på vilka resurser förbandet har för att genomföra telekrig och hur dessa växelverkar med resten av Försvarsmaktens resurser.

En viktig tillämpning är telekrig för egen-skydd, både av enskilda plattformar och hela förband. I fallet för egenskydd handlar det främst om varnar- och motverkanssystem (VMS). De är integrerade lösningar både för att upptäcka hot och motverka dessa hot. Motverkan kan handla om störning, vapeninsats eller rena taktiska åtgärder, till exempel undanmanövrer. I detta kapitel läggs fokus på telekrigsåtgärder.

Telekrig på förbandsnivå

Telekrig är en viktig komponent både för att spana mot och påverka en motståndare.

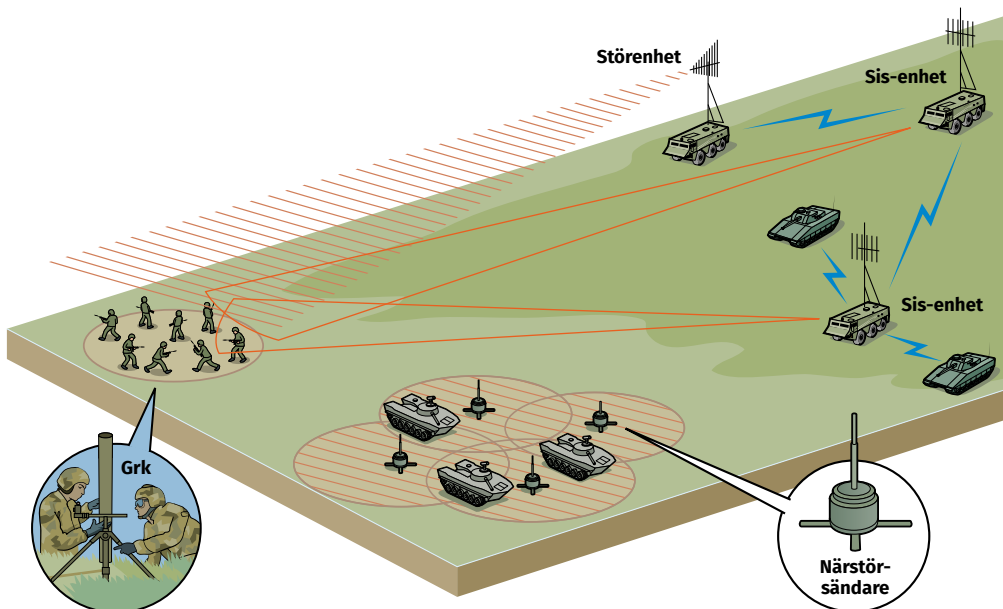
Spaning (ESM) genomförs mot radar- och kommunikationssystem. Radarsignalspaning ger information om sändande radar, vilka system som används och var de befinner sig. Kommunikationssignalspaning (KOS) kan utöver detta ge viss information om hur och vad som kommuniceras – och vem som sänder till vem. Det gör det möjligt att identifiera typ av förband, förbandsstorlek och pågående verksamhet. Den informationen kompletterar lägesbilden både översiktligt och på detaljnivå. Spaningsdata utgör också underlag för underrättelsetjänsten, som kan göra en djupare analys av innehållet i avlyssnade meddelanden eller av strukturen på signalerna.

Störning (EA) kan göras mot motståndarens system inom kommunikation, radar, navigation eller andra typer av system. Syftet är främst att minska motståndarens förmåga till spaning eller ledning, eller öka sitt egenskydd. EA kan försvåra eller förhindra motståndarens kommunikation, vilseleda genom falsk signalering eller sätta ner kapaciteten. Det går också att störa ut

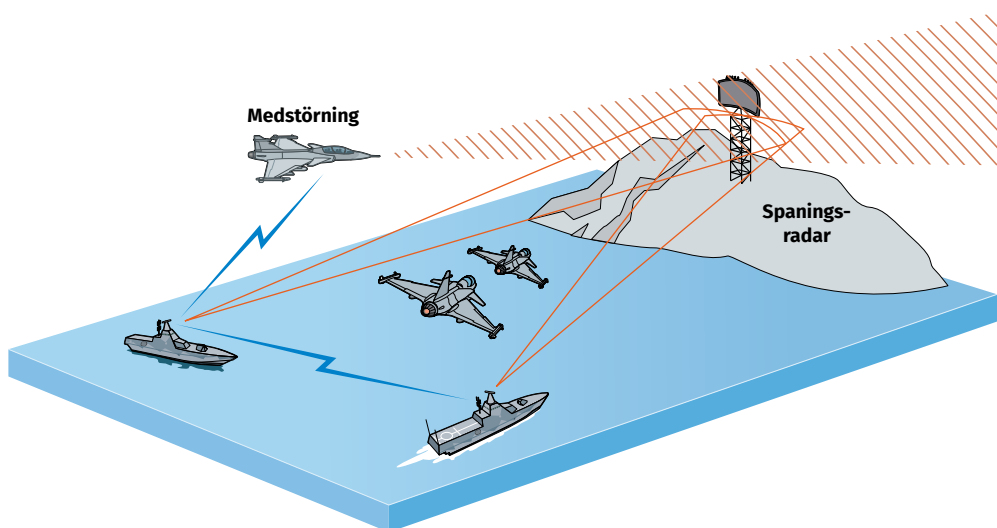
signaler för radarsystem som används för in- vision av robotar och målsökare, eller undertrycka spaningsradarstationers täckning, för att dölja det egna förbandets rörelser och verksamhet.

Att inte röja sig i onödan är en del av elektro- nisk protektion (EPM) och ingår i normalt tak- tiskt uppträdande, som en del av skyddet mot ESM. Ett exempel är en ubåtschefs övervägan- den att gå från dolt undervattensläge till ytläge eller att sticka upp mast eller antenn över vat- tenytan och därmed utsätta sig för den elektro- magnetiska miljön.

Samordningen av olika förbands telekrigsför- måga ger ett mervärde då förbanden var för sig kan ha olika förutsättningar. Markbaserade tele- krigsförbands förmåga att kunna övervaka stora ytor är viktig för uppbyggnad av den gemen- samma lägesbilden även över hav (mot fartyg) och i luft (mot flyg). Sjögående och flygburna telekrigsplattformar kan genom hög antennhöjd och vid bra vågutbredningsförhållanden över- vaka mycket stora täckningsområden varifrån information kan inhämtas och delges, se figur 74 och 75.



Figur 74. Telekrigssystem signalspanar och bidrar då till sammanställningen av lägesbilden. Störning kan genomföras i olika former. Störsändare kan antingen arbeta i automatmod eller fjärrstyras. Störsändare i närområdet kan placeras ut i förväg. Tyngre system är fordonsburna och lättare system kan bäras av soldater.



Figur 75. Två korvetter genomför taktisk signalspanning mot radarstationer. Läget rapporteras vidare så att medstörning kan genomföras i syfte att skapa förutsättningar för offensiva luftattacker.

Egenskydd

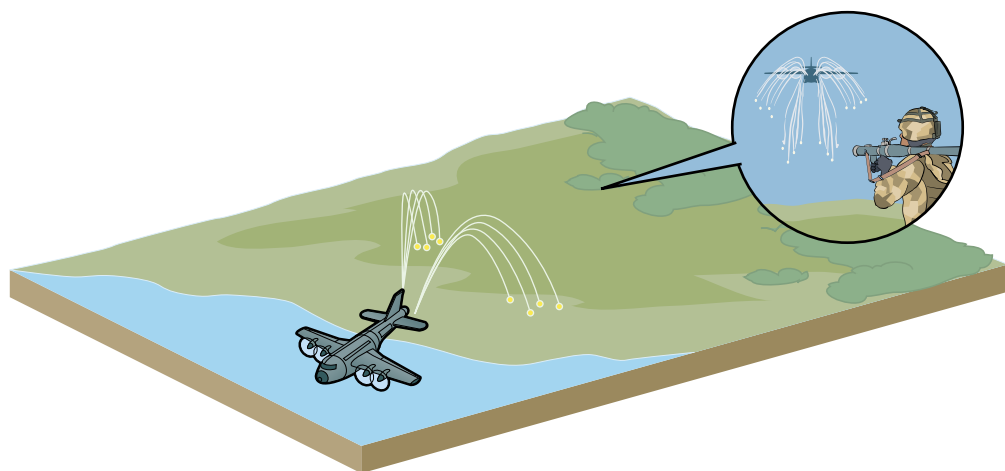
Operativ verksamhet kräver egenskydd i de flesta miljöer, bland annat varnar- och motverkanssystem (VMS) till fartyg, flygplan, helikoptrar och fordon, se figur 76.

Ibland används termen varnar- och motmedelssystem istället för varnar- och motverkanssystem. Skillnaden är att motmedelssystem i huvudsak omfattar telekrigssystem för att motverka hotet. Motverkanssystem avser alla tänkbara sensorer och vapen som kan bidra till denna motverkan. I princip kan man vidga begreppet till sensor- och motverkanssystem, eftersom även andra sensorer och vapen kan bidra till att ett hot upptäcks, klassificeras, undviks eller bekämpas.

Generellt ställs ständigt högre krav på förmåga att hantera allt mer kvalificerade hot mot den egna plattformen. Detta ställer stora krav på telekrigföring och angränsande verksamheter, bland annat signaturanpassning och inhämtning av underrättelser.

Det finns en stark koppling mellan signaturanpassning och motmedel. Om plattformen är väl signaturanpassad krävs mindre mängd motmedel för att dessa ska få övervikt. Det är betydelsefullt att känna till egna signaturer, dels för att veta vilka krav som ska ställas på motmedel, dels för att kunna optimera den uppvisade signalen mot ett hot. Motverkan kan därför också kombineras med taktiska åtgärder, till exempel att telekrigsinsatsen kombineras med undanmanöver eller annat anpassat uppträdande.

Ett varnar- och motverkanssystem bygger på att hotet upptäcks och klassificeras i så pass god tid att åtgärderna hinner påbörjas och få önskad effekt. Plattformar utrustas därför med olika typer av varnare för att kunna utföra sina uppgifter i en kvalificerad hotmiljö. Det kan vara radarvarnare, laservarnare eller robotskottvarnare baserade på UV eller IR. Motverkanssystem inom telekrigsområdet är bland annat anti-sensorlasrar, radarstörare, facklor och remsor.



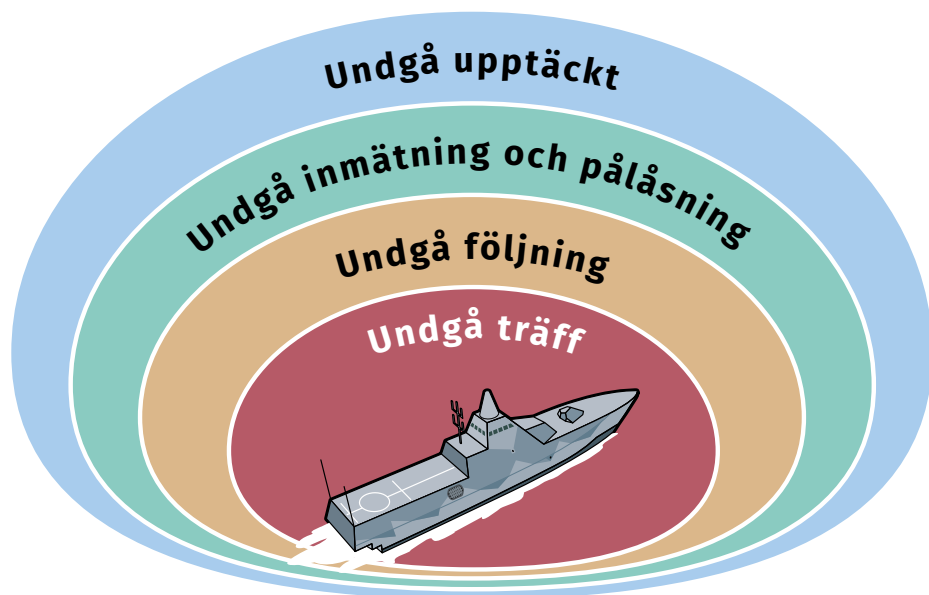
Figur 76. Transportflygplan som detekterat en inkommande robot och släpper facklor.

Vissa situationer kräver preventiva åtgärder innan hotet har klassificerats. Dessutom kan speciella telekrigsresurser ge understöd under en insats, till exempel genom att flygplan, som utrustats för störning, släcker ut motpartens luftvärnsradar.

Skyddet av en plattform kan illustreras med hjälp av en "lökmodell", se figur 77. Här beskrivs schematiskt olika faser där telekrigsinsatser ger olika former av skydd. I alla dessa steg kommer

signalspaning och varnare (ESM) att kunna ge information om spaning och hot. Motmedelssystemen ska bryta de olika länkarna i kedjan från upptäckt till träff.

För att överleva är första steget att undvika upptäckt. Passiva medel kan vara maskerande remsor eller rök. Aktiva medel är bland annat störsändning mot spaningssystem. I båda fallen är en riktigt utformad signaturanpassning (SAT) av stor betydelse. Å andra sidan kan till exempel



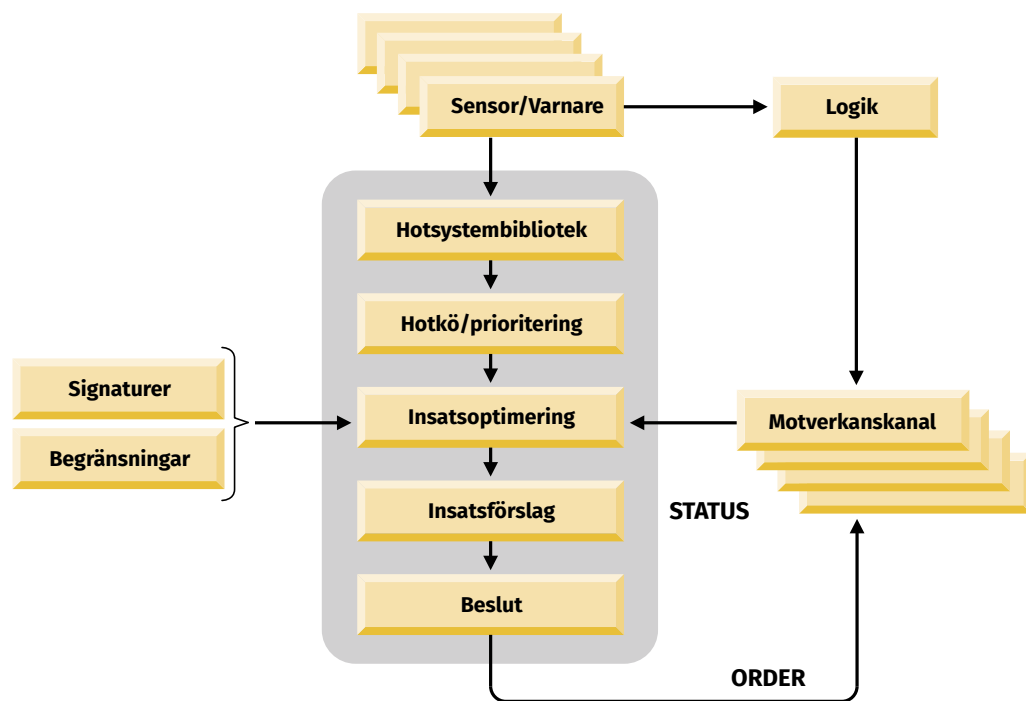
Figur 77. Schematisk bild över ett tänkt skalskydd för fartyg. Den viktigaste uppgiften för varnar- och motverkanssystemet är att förhindra upptäckt, inmätning, pålåsning samt följning av sikten och målsökare för att undvika träff. För att undgå upptäckt utnyttjas i första hand signaturanpassning, eventuellt i kombination med maskerande insatser.

rök också vara röjande och leda in spaning. Den visar att det finns något där som lagt ut röken.

Om plattformen blir upptäckt är nästa steg att undvika inmätning och pålåsning av olika typer av sikten och/eller målsökare. Även här kan olika former av störande eller vilseledande motverkan bidra till att förhindra att följning kan påbörjas. Skulle följning påbörjas kan telekrigsinsatser sättas in för att försöka bryta denna.

I det sista skedet, när det handlar om att undgå att faktiskt bli träffad, är motverkansåtgärder t.ex. att genom avhakning flytta bort målföljningen från plattformen.

Ett varnar- och motverkanssystem (VMS) består principiellt av varnare/sensorer, motverkanssystem samt bibliotek, se figur 78. I många fall är ett VMS integrerat i plattformens ledningssystem. ■



Figur 78. Schematisk illustration av ett generellt VMS. Information från en sensor och/eller varnare skickas för klassificering till ett systembibliotek över hot. Därefter sker prioritering av hotet, följt av insatsoptimering. Förloppet tar en viss tid eftersom optimeringen tar fram ett förslag på olika slags motverkan beroende på aktuellt hot. Insatsförslaget som väljs kan då antingen genomföras automatiskt eller bekräftas av operatör innan det verkställs. Vid upptäckt av radarpulser är det bra att skicka varningen direkt till en logikenhet som reglerar om radarstörning ska påbörjas direkt eller inte.

Närliggande verksamheter

Telekrigföring är ingen isolerad företeelse, utan måste koordineras med andra verksamheter för att undvika att motverka dessa.

Följande exempel på angränsande verksamheter sker parallellt med telekrig och diskuteras närmare i detta kapitel:

- Produktion av telekrigsbibliotek (signalunderrättelsetjänst och dataförsörjning).
- Signaturhantering (EMKON, SAT och telekonflikter).
- EM-vapen (HPM och laservapen).
- Övrig signalkrigföring.

Signalunderrättelsetjänst

Med signalunderrättelsetjänst (SIGINT) avses strategisk och operativ inhämtning av underrättelser genom signalspaning för att fastställa motståndarens eller annan parts läge, verksamhet och tekniska prestanda. Signalunderrättelsetjänst tillhör funktionen underrättelsetjänst.

Inom strategisk signalspaning har arbetssättet mot kommunikation respektive radar ofta skilt sig väsentligt åt. Det beror på att om informationsinnehållet i radiokommunikationen kan utvinnas ger det ett stort mervärde. I radarfallet finns inget sådant informationsinnehåll, utan slutsatserna är beroende av de tekniska parametrar som kan mätas i signalen, till exempel pulsbredd och pulsrepetitionsfrekvens, tillsammans med den förkunskap om olika radar-system som finns. I Sverige har begreppen för de båda arbetssätten varit kommunikationssignalspaning (KOS) respektive teknisk signalspaning (TES). Exempel på svenska plattformar för såväl KOS som TES visas i figur 79 och 80 på nästa sida.

Det finns stora likheter i tekniken mellan taktisk signalspaning (ESM) och SIGINT. De skil-

jer sig dock åt vad gäller syfte och användare. Syftet med operationen avgör om det handlar om ESM eller SIGINT. Allmänt stödjer ESM telekrigföring och taktiska aktiviteter med information. SIGINT stödjer med underrättelser för användare på alla nivåer, från den nationella regeringsnivån ner till taktiska chefer. Syftet spänner från långsiktig planering till att i nära realtid stödja operationer, inklusive telekrigsoperationer.

SIGINT förser också telekrigsfunktionen med nödvändiga tekniska data och underrättelser för att kunna utveckla utrustning och procedurer. Det sker bland annat genom omfattande prov- och försöksverksamhet, där system provas i både simulerad och verklig miljö under längre perioder. Det krävs ett nära samarbete mellan ESM och SIGINT när separata enheter eller utrustningar används.

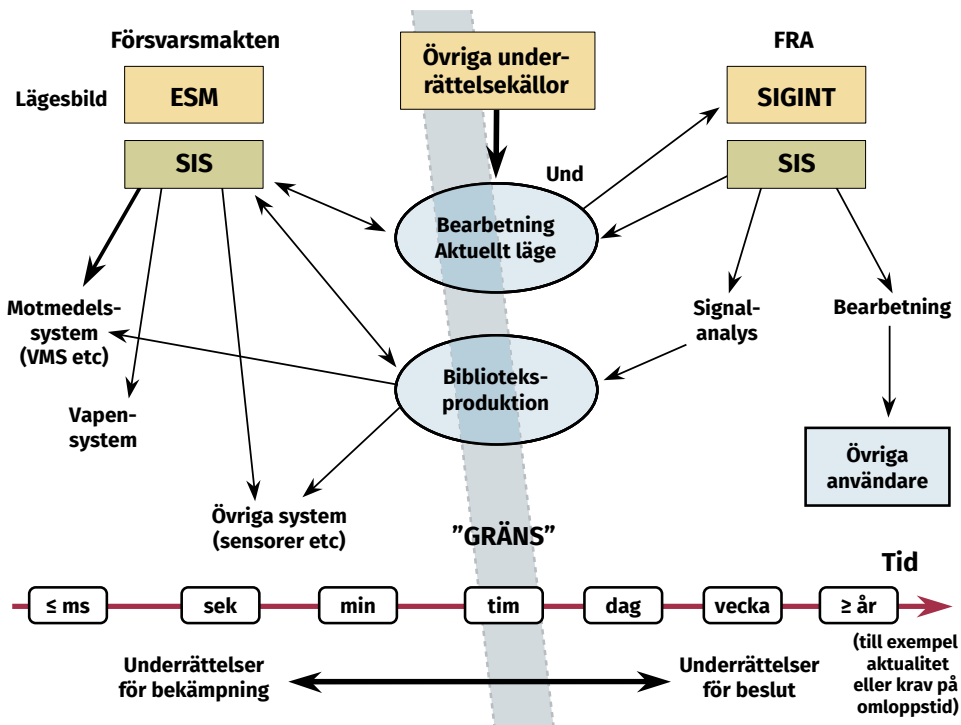
ESM och SIGINT skiljer sig även oftast åt i hur snabbt de arbetar. ESM arbetar från några sekunder upp till timmar, till exempel vid direkt bekämpning. SIGINT arbetar med längre tidsperspektiv, från timmar upp till år, se figur 81.



Figur 79. S102 B Korpen som används för teknisk signalspaning. Foto: Peter Liander /Försvarmakten.



Figur 80. Underrättelseplattform HMS Artemis. Foto: Cecilia Lindberg/Försvarmakten



Figur 81. En illustration av de olika tidsperspektiven för ESM och SIGINT.

Dataförsörjning

Deltagande i internationella insatser ställer också krav på utbyte av information om frekvenser och moder hos egna system och även uppdatering av systemens telekrigsbibliotek för att hantera nya hot. Försvarsmaktens telekrigstödenhet (TKSE) är den enhet inom Försvarsmakten som i dag svarar för anpassning av telekrigssystem och telekrigsfunktioner i andra system. Det innebär bland annat att tillverka "bibliotek" till radarvarnare, störsändare och annan telekrigsutrustning. Verksamheten vid TKSE omfattar alla led i bibliotekstillverkningen, det vill säga dataåtkomst, datalagring, produktion, verifiering, validering, distribution, utbildning, analys/utvärdering och feedback. De främsta leverantörerna av

data är, förutom egna förband, Försvarets radioanstalt (FRA), Totalförsvarets forskningsinstitut (FOI) och Försvarets materielverk (FMV).

Det finns en stark koppling till taktik, strids teknik och soldaten som ska använda telekrigssystemet. Telekrigssystemen producerar kunskap som ger effekt och därmed gör det möjligt för insatsförband att verka på den internationella arenan. Framtiden pekar på ett ökat behov av telekrigsstöd. Det finns behov av dataförsörjning när nya system inom nya våglängdsområden tillkommer.

Försvarsmaktens uppgifter på den internationella arenan ställer också krav på ett snabbt och uthålligt telekrigsstöd.

Telekrigsbibliotek

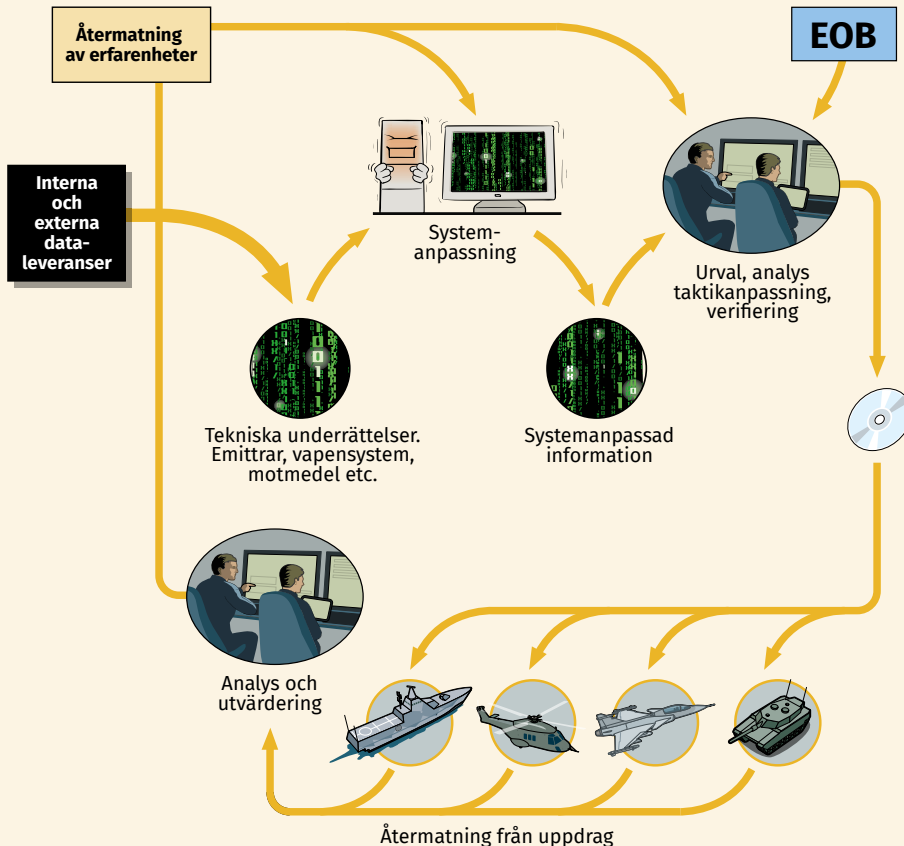
För att moderna varnar- och motverkanssystem ska ha avsedd verkan krävs att de laddas med omvärldsinformation, så kallade telekrigsbibliotek. Dessa bibliotek innehåller bland annat information om emitterar och vapensystem för identifiering och olika motmedel och åtgärder för egenskydd.

För att tillverka telekrigsbibliotek behövs kunskap inom följande områden:

- Information om fysiska vapensystem och emitterar. Detta omfattar fientliga, egna, neutrala och civila system (EOB, Electronic Order of Battle).

- Goda tekniska underrättelser om ovan nämnda vapensystem och emitterar.
- God kännedom om de egna telekrigssystemens funktion och kapacitet.
- Goda taktiska kunskaper.

Telekrigsbiblioteken skräddarsys för plattform och typ av uppdrag. Det är t.ex. stor skillnad mellan ett bibliotek för ett marint system och ett för flygande system. I marina system finns oftast en operatör som tolkar informationen. I ett flygande system har inte piloten tid att tolka informationen i samma utsträckning. Beroende på uppdrag ställs det också olika krav på bibliotekens innehåll.



Figur F15. En schematisk beskrivning av processen för framtagning av telekrigsbibliotek.

Kontroll av hur det elektromagnetiska spektrumet används

Telekrigföring har också en viktig roll i att kontrollera utnyttjandet av det elektromagnetiska spektrumet, EMKON (på engelska EMCON). Det handlar till exempel om att undvika elektromagnetiska konflikter, både mellan egna system och mellan egna och eventuella koalitionspartners system.

Det gäller att se till att olika system inte påverkar varandra på ett ogynnsamt sätt, till exempel genom oavsiktliga störningar. Om sådan påverkan undviks kan systemens samlade effekt utnyttjas effektivare. Det innebär också att vi kan styra vilken information motparten uppfattar, vilket är avgörande för vår förmåga till dolt uppträdande och vilseledning.

Ett kontrollerat utnyttjande av det elektromagnetiska spektrumet blir också allt viktigare, och mer komplicerat. Detta eftersom fler militära och civila system utnyttjar det elektromagnetiska spektrumet.

För att kunna kontrollera den elektromagnetiska emissionen krävs mycket god kunskap om såväl egna som koalitionspartners system samt motsvarande kunskap om civila system inom operationsområdet. För att upprätthålla detta krävs det dessutom att vi har utvecklade metoder för snabbt utbyte av telekrigsdata. För att samordna förbands och systems emissioner över tiden behöver vi också utvecklade metoder för att snabbt styra dessa emissioner.

Signaturanpassning

Syftet med signaturanpassning är att minimera kontrasten mellan ett objekt och bakgrunden. Detta gäller inom hela frekvensspektrumet. Metoden benämns signaturanpassningsteknik (SAT). I naturen är kameleonten känd för att kunna anpassa sig efter sin omgivning och den används därför ofta som symbol för teknikområdet, se figur 82.

Signaturanpassning är inget självändamål, utan är tillsammans med alla andra skyddsåtgärder en del i överlevnadskonceptet, se figur 77 (den så kallade skyddslöken) i kapitlet Tillämpningar. En del av konceptet består av vilseledning, signaturanpassning och skenåtgärder, VSS (CCD – Camouflage, Concealment, Deception). SAT omfattar, förutom konstruktionsåtgärder och ytbeläggningar, även tilläggsmaskering och tillfälliga åtgärder för att minska kontrasten.

Den optiska signaturen beror på den yttersta ytans egenskaper och vinkel i förhållande till ljus och omgivning. Inom optikområdet bestäms

signaturen av ytans förmåga till reflektion och objektets form.

Den termiska signaturen beror dessutom på objektets temperatur. För en bra signaturanpassning i det termiska området måste värmen från interna källor, till exempel motorer, kontrolleras. Det görs genom isolering, skärmning eller ventilation. Man kan också använda lågemissiv ytbeläggning. En termisk sensor ”ser” då en kallare yta. Heta avgaser kan kylas eller skärmas av.

Radarsignaturen beror främst på objektets ledande egenskaper, form samt integrationen av alla yttre komponenter som luckor, vapen, utblickar och sensorer. Inom radarområdet väljer man att reflektera bort strålningen eller att absorbera den i radarabsorberande material (RAM). Särskild omsorg ägnas åt håligheter eftersom de kan ge direkreflexer. De kan täckas med galler, som ligger i samma plan som ytterytan, eller invändigt kläs med radarabsorberande material.

Eftersom formen är så viktig är det uppenbart att robusta och kostnadseffektiva signaturreducerande åtgärder måste beaktas tidigt i utvecklingsarbetet. Formgivning avser de åtgärder som utförs på ett objekts yttre form. Vid formgivning fastställs storlek, areaförhållanden och vinklar mellan objektets olika ytor, kantlängder vid angränsande ytor och krökningsradier hos ytor och kanter. Formgivningen fastställer också objektets silhuett i olika aspektvinklar. Valet av maskeringsbeläggning påverkar indirekt såväl den termiska som radarsignaturen. Till objektsignatur räknas också strålningsbidrag från avgasmoln och spårbildning. Objektets funktion sätter dock gränser för formgivningen. Kända objekt där SAT har utnyttjats för att nå taktiska fördelar är bl.a. det amerikanska smygpassade flygplanet F-117 samt den svenska fartygsklassen Visby, se figur 83.



Figur 82. Kameleonten är bra på signaturanpassning. Foto: Michelle McDonald/iStock



Figur 83. Korvett HMS Karlstad. Foto: Jimmie Adamsson/Försvarmakten

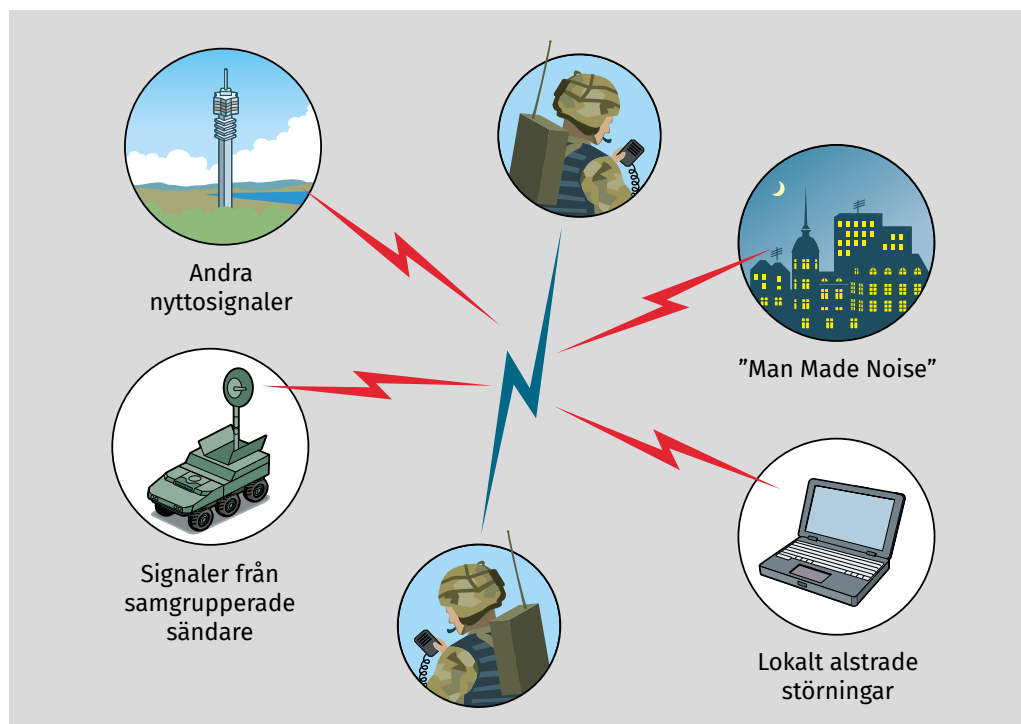
Telekonflikter

Telekonflikter uppstår när oavsiktliga störningssignaler kopplas in i radiomottagare via antennen, se figur 84. Telekonflikter har varit ett känt problem för militära radiosystem under lång tid och en mängd telekonflikter finns rapporterade från olika militära operationer. En utmaning är när system som sänder med hög effekt ska kunna användas i närheten av känsliga mottagarsystem, exempelvis på fartyg där radar- och kommunikationssystem ska samexistera eller på arméplattformer där flera radiosystem ska kunna användas.

Telekonflikter är också något som behöver beaktas i det civila samhället, exempelvis används

skyddsavstånd kring flygplatser för installation av solcellsanläggningar för att de inte ska riskera att störa mottagarsystem på flygplatsen. För att förhindra problem med telekonflikter finns tekniska och metodmässiga åtgärder, som användning av filter eller frekvensplanering.

Genom välfungerande kontroll av utnyttjandet av det elektromagnetiska spektrumet (EMKON) kan risken för telekonflikter minskas. Typiskt uppstår telekonflikter i nyuppkomna situationer, som när enheter från olika vapenslag eller olika nationer genomför gemensamma insatser och system som inte tidigare har använts samtidigt ska samexistera.



Figur 84. Telekonflikter är störningar kopplade via antennsystemet.

HPM-vapen

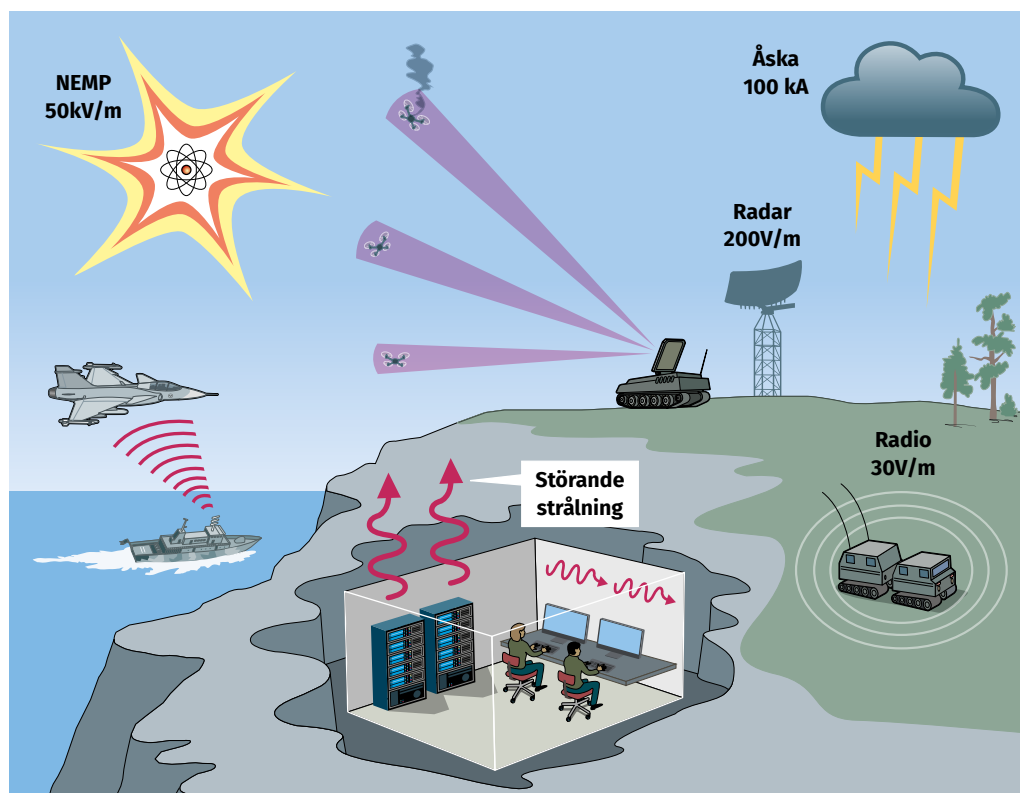
HPM utgör en delmängd av den elektromagnetiska miljön, se figur 85. Huvudsyftet med HPM-vapen (High Power Microwave) är att störa eller förstöra funktionen hos elektronikberoende system. HPM-strålningen kan ta sig in i målet på två sätt. Det sker antingen via bakvägskoppling eller framvägskoppling, se figur 86.

Ett exempel på bakvägskoppling är bekämpning av drönare med roterande vingar. Om tillräckligt med effekt stör elektroniken kan styrningen sluta fungera och då störtar drönaren. Ett exempel på framvägskoppling är bekämpning av kommunikationssystem, där energin går in genom antennen och förstör ingångssteget. Olika elektroniska system är känsliga för olika

typer av pulsformer. Med pulsform menas här kombinationen av utsänd frekvens, pulslängd och pulsrepetitionsfrekvens.

Typiskt för HPM-vapen är att de producerar mycket höga topeffekter. Siffran 100 MW anges ibland som en undre gräns för ett HPM-vapens uteffekt, men ofta går det att få önskat resultat med lägre effekt genom att skräddarsy pulsformen. Konventionella HPM-vapen använder elektronrörsteknik, som kan ge mycket höga pulseffekter, men har små möjligheter att skräddarsy pulsformen. De genererar smalbandig strålning vid den frekvens de konstruerats för.

En annan teknik är att skapa en relativt bredbandig strålning (400–1000 MHz). Det görs



Figur 85. Den elektromagnetiska miljön för militära system, där telekrig, EMP och HPM är en del av denna miljö. Ett åsknedslag kan förorsaka oönskade strömstyrkor och därmed skador genom att kopplas in i materiel och byggnader som saknar åskskydd, och där ge upphov till strömmar och potentialskillnader i elektrisk utrustning.

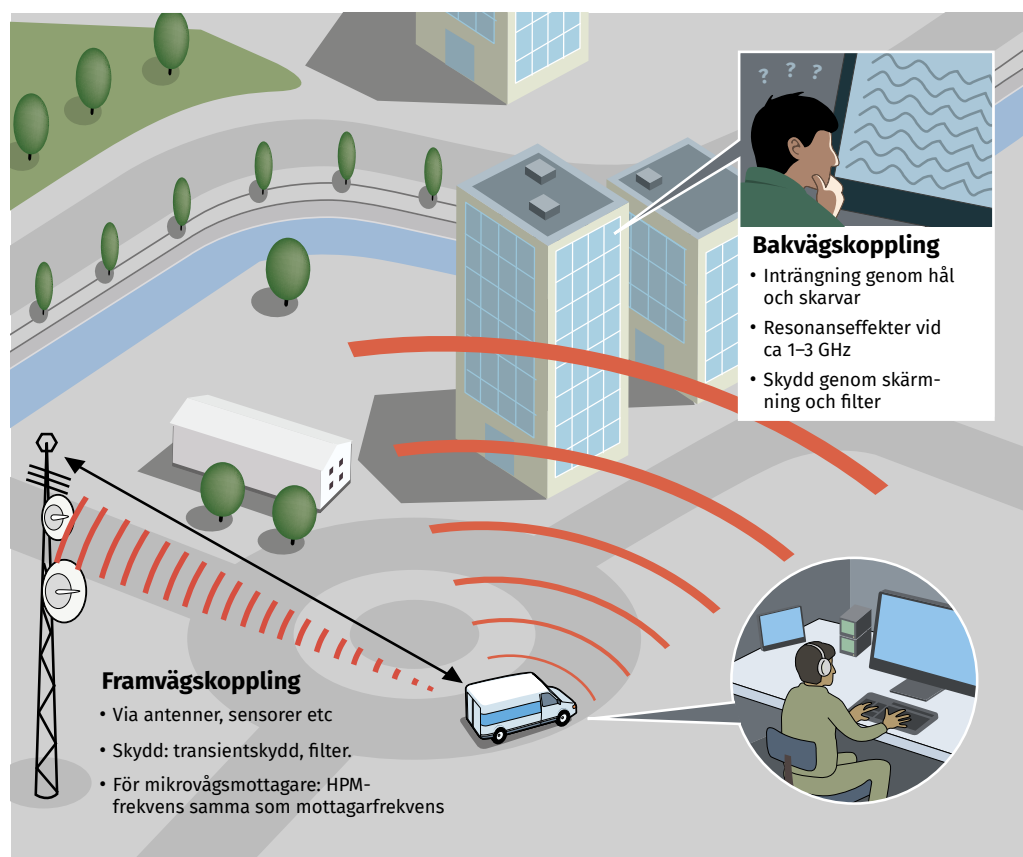
genom att ladda ur högspänningskondensatorer över en induktor som matar en antenn. Det kallas för en dämpad sinusvåg. Den senare tekniken kan ge topeffekter på 10 GW i mycket korta (~ 5 ns) pulser men eftersom strålningen är bredbandig är det en utmaning att konstruera en effektiv antenn och energiinnehållet i varje puls blir lågt i jämförelse med smalbandiga källor.

Den senaste utvecklingen inom HPM-vapen utgår från samma teknik som ingår i moderna radaranläggningar av AESA-typ och kan generera pulsformer inom en mycket stor parameterrymd, men inte med samma uteffekt som elektronrören. Det är möjligt tack vare transistorer för höga topeffekter och utvecklingen kommer troligen att fortsätta med helt nya och mer spänningståligena och robusta material, till

exempel galliumoxid som ännu inte är kommersiellt tillgängligt.

HPM-tekniken har fått ett uppsving på grund av möjligheten att bekämpa mindre drönare genom bakvägskoppling in i styrsystemet. Nu finns flera företag som erbjuder HPM-vapen för drönbekämpning. HPM är ett intressant alternativ speciellt för drönare som är svåra att bekämpa med telekrig, till exempel sådana som styrs via fiber, eller som använder tröghetsnavigering och geografisk information. De tre teknikerna som nämndes ovan för att generera strålning används för drönbekämpning i olika typer av HPM-vapen.

En annan tillämpning är att stoppa fordon. Flera företag har färdiga lösningar för att stoppa både bilar och båtar. I allmänhet finns



Figur 86. HPM har två typer av inträngning i målet, framvägs- respektive bakvägskoppling.

det inga krav på skydd mot HPM, varken militärt eller civilt. Det finns dock vissa undantag för moderna militära system. Flygplan och helikoptrar, även civila, är skyddade mot intensiv radarstrålning och har därmed ett gott grundskydd mot HPM.

Lite tillspetsat kan man säga att skyddsmetoder för bakvägskoppling finns kommersiellt tillgängliga. Förenklat handlar det om traditionell skärmning, medan skydd mot framvägskop-

pling kräver skräddarsydda lösningar, som speciella filter och skyddskretsar.

Det är dock tveksamt om existerande skyddslösningar klarar de höga nivåer som HPM kan generera. I det senare fallet innebär skyddet oftast att funktionen försämras. Särskilt för bakvägskoppling är det svårt att verifiera ett systems tålighet mot HPM. Det beror på HPM-hotets stora parameterrymd och oftast höga komplexitet, ibland med flera inkopplingsvägar.

Laservapen

Laservapen använder sig av ljusets hastighet (kulor av ljus), vilket medför att momentan verkan fås i målet. En laserstråle från ett laservapen har väldigt liten divergens, vilket innebär att kollaterala skador kan undvikas. Vidare fås en låg kostnad per skott då enbart elektrisk kraft krävs. Magasinet är också stort i jämförelse med kinetiska vapen.

Eftersom laserstrålen fokuseras till centimeterstorlek på målet krävs det att systemet har väldigt bra följnoggrannhet. Här används ofta finstyrning av laserstrålen. Ett antal delfunktioner och delsystem behöver beaktas vid utveckling och tillverkning av ett laservapen.

Bekämpningssekvensen för laservapen kan enkelt beskrivas som i figur 87. Först detekteras målet med en sensor som spanar i en stor vinkelsektor, därefter in visas laservapnets siktlinje (teleskopet) och vapnets sensorer för målföljning tar över. Här används optiska sensorer med hög vinkelupplösning så att en klassificering av målet är möjlig och träffpunkt kan väljas. När träffpunkt har valts så hålls laserstrålen på målet tills verkan åstadkommit, vilket kan innebära strukturell skada eller att målet börjar brinna eller exploderar beroende på måltyp och val av träffpunkt. Bekämpning av målet kan bekräftas efter någon eller några sekunder, beroende på typ av mål och laserstrålens effekttäthet.

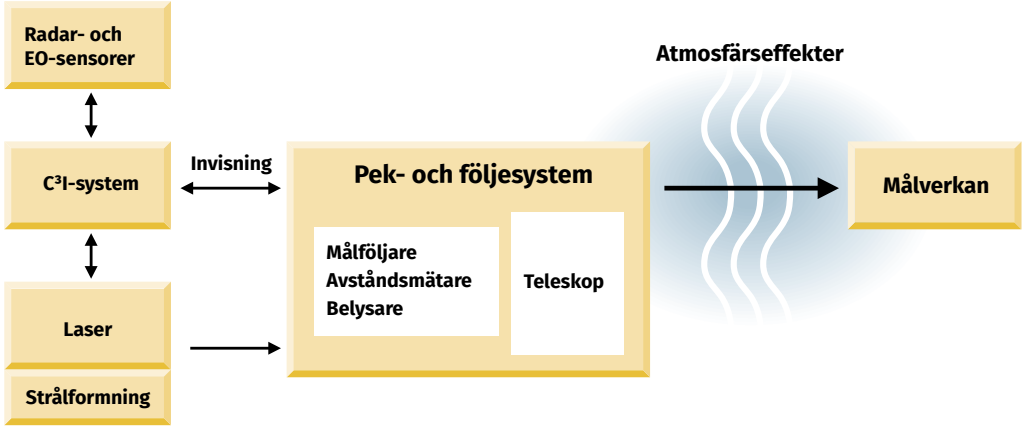
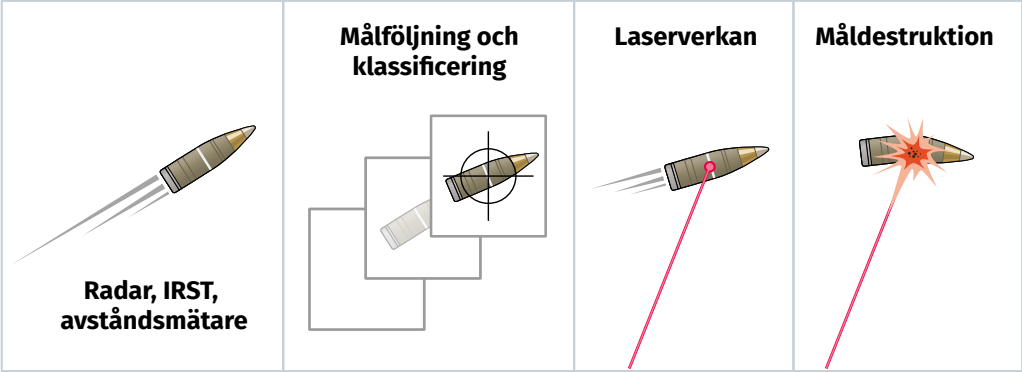
Skada uppstår genom att målet hettas upp på grund av absorption och värmeledning av

laserstrålning. Här kan flera fysikaliska processer uppstå som smältning, förångning, värmeinducerad mekanisk belastning och plasmabildning. Allt detta kan bidra till strukturella skador i målet.

Effektkraven spänner från tiotals kilowatt (kW) till megawatt beroende på vilka mål som är intressanta för bekämpning, se tabell 4. För bekämpning av drönare (Unmanned Aerial Vehicle, UAV) krävs ett tiotal kW beroende på drönarens storlek och på vilket avstånd den befinner sig från laservapnet.

Ett annat hot som prioriterats är olika typer av raketer och granater, vilka kräver en högre medeleffekt för en effektiv och snabb bekämpning. Intressant är också större och "hårdare" mål, till exempel robotar eller flygande plattformar. Men då krävs betydligt högre lasereffekter, som hundratals kilowatt eller mer, beroende på avstånd till målet. Kraven på inriktning och peknoggrannhet hos laserstrålen ökar med avståndet till målet.

Vilka svårigheter och begränsningar har då användandet av ett laservapen? Eftersom laserstrålen utbreder sig i atmosfären kommer den att påverkas av väder och vind. Små partiklar i atmosfären, som regndroppar, dimma eller snö, kommer att orsaka spridningsfenomen hos laserstrålen. Det minskar transmissionen och därmed intensiteten hos den laserstrålning som träffar målet. Effekten beror på vädret och i många fall ökar tiden för bekämpning om vädret försämras.



Figur 87. Bekämpningssekvensen för ett laservapensystem.

Tabell 4. Effektkrav på lasern för bekämpning av olika typer av mål.

ca 10 kW	Tiotal kW	ca 100 kW	100+ kW	ca 1 MW
UAV:er				
	Raketer, granater, robotar			
			Flygplan	
		Sjömålsrobotar, kryssningsrobotar (subsoniska)		Supersoniska samt ballistiska robotar

Ett annat fenomen relaterat till atmosfären är att luftens brytningsindex förändras slumpmässigt beroende på turbulens. Turbulensens styrka varierar med temperatur och lufttryck, och är kraftigast nära markytan varma sommar dagar. Turbulens i atmosfären ger avlänkning av laserstrålen samt att strålprofilen bryts upp och breddas. Sammantaget orsakar störningar på grund av turbulens att intensiteten på målet minskar, men aktiv eller adaptiv optik och finstyrning av laserstrålen kan minska effekten. Vid utbredning av laserstrålen genom atmosfären kan även strålning absorberas, vilket värmer upp luften och orsakar förändringar i brytningsindex. Detta sker vid relativt höga lasereffekter, ca 30–40 kilowatt eller högre. Uppvärmningen av luften får till följd att laserstrålens intensitetsprofil kan förvrängas och intensiteten reduceras. Även här kan adaptiv optik användas för att kompensera för effekten.

Teknikutvecklingen sker inom områdena laserkällor, strålkombinering och finföljning av mål. Dessutom sker även utveckling av teleskop, optimering av kylning och kraftförsörjning samt minskning av vikt och volym.

I dagsläget har elektriskt drivna fiberlasrar med våglängden cirka en mikrometer använts i demonstrationer och även i system som testats av militära förband. Det går att tillverka moduler av fiberlasrar upp till fem kilowatt som har den kvalitet som krävs för vapenanvändning. För att öka effekten kan moduler kombineras spektralt med gitter (jämför med ett prisma som bryter ljus), där varje modul skiljer sig något i våglängd. Tekniken bedöms kunna användas upp till cirka 300 kilowatt lasereffekt.

En annan teknik, där fiberlasrar används, är koherent strålkombinering med en utgående apertur på vapnet som delas av flera fiberlasrar. Fasen hos de ingående laserkällorna kan kontrolleras, vilket kan jämföras med syntetisk aperturradar men inom det optiska våglängdsområdet. Koherent strålkombinering kan öka intensiteten på målet och kompensera för fasstörningar, som till exempel har uppkommit i atmosfären.

Parallellt med teknik för fiberlasrar pågår utveckling av andra elektriskt pumpade

lasertyper. Det ser lovande ut att använda fasttillståndslasrar med ett flytande kylmedium för att få höga lasereffekter. På lång sikt studeras även hur monolitiska matriser av halvledarlasrar ska kunna användas till vapen. En kritisk teknologi för laservapnet är finföljning som inkluderar både följensensor och korrigerande element, exempelvis snabba speglar. Här studeras olika typer av högupplösande kameror i olika våglängder, ibland kombinerat med laserbelysning.

Säkerheten är viktigt både för egen personal och tredje man när man använder ett laservapen, eftersom laserstrålning kan skada ögonen på mycket längre avstånd än man tror. Säkerheten kring ett laservapen bedöms kunna utformas så att den inte skiljer sig markant från vad som gäller för kinetiska vapen. Det utvecklas därför laserkällor som använder våglängder som är mindre skadliga för ögonen (1,5–2 mikrometer).

Skydd och sårbarhet är ett viktigt område relaterat till laservapen. Det behövs en analys av skydd och sårbarhet för kritiska plattformar och installationer eftersom man kan anta att laservapen kommer att bli operativa i framtiden. Kritiska delar behöver identifieras och modifieras för att bättre tåla laserexponering. Nya material och tekniker kan också minska effekten av ett laservapen. Om ett mål teoretiskt reflekterar 100 procent av laserstrålningen kommer ingen energi från vapnet att deponeras i målet.

Var befinner vi oss då i dagsläget? Laservapen studeras på alla militära arenor men drönarhotet är prioriterat. Här kan mindre drönare på kortare avstånd bekämpas med system som i medeltal har en effekt på 5–10 kilowatt. Ett system som ska fungera i en operativ miljö behöver öka medel-effekten till 10-tals kilowatt, se figur 88.

Skydd av marina plattformar är ett område som bland annat prioriterats av USA. Även i Tyskland har laservapen demonstrerats på en marin plattform. Andra tillämpningar inkluderar laservapen på markfordon. USA har installerat system för armén och fasta installationer för luftvärn för att skydda viktig infrastruktur. Laservapen på flygande plattformar studeras men här sker teknikutvecklingen något långsammare. USA är drivande i framstegen inom laservapen-



Figur 88. Fordonsburet laservapen CLWS (Compact Laser Weapon System).

området, både större och mindre företag är involverade i utvecklingen. I Europa pågår utveckling framför allt i Tyskland, Frankrike och Storbritannien. Flera demonstrationer har hållits med olika tekniker. En annan aktör som ligger långt

framme är Israel som historiskt har samarbetat med USA inom området. Ryssland och Kina är två andra nationer som bedöms ha teknisk förmåga att ta fram laservapen och flera demonstrationer har ägt rum.

Övrig signalkrigföring

Telekrigföring har kommit att hänföras till det elektromagnetiska spektrumet snarare än till en viss typ av taktisk verksamhet. Inom det hydroakustiska området förekommer till exempel verksamhet som har stora taktiska likheter med telekrig. Vissa typer av sensorer faller utanför telekrigsområdet, främst akustik, hydroakustik, seismik och magnetik. De samlas under benämningen övrig signalkrigföring.

Ju högre krav på egenskydd och signaturanpassning, desto viktigare blir det att hantera även dessa områden tillsammans med det som normalt karakteriseras som telekrigföring. Ett system som signaturanpassats inom IR och radar kan kanske ändå upptäckas om det bullrar i det akustiska området. Krav finns således på att hantera telekrig och övrig signalkrigföring i en och samma kontext. ■

Skapa kunskap
och insikt

En förutsättning för att få effekt av telekrig är att det finns kunskap och insikt om möjligheter, begränsningar, metoder och verktyg från högsta ledningsnivå ner till enskild soldat. Dessutom måste det finnas en vana vid att se telekrig som en integrerad del i att lösa uppgifter. Det måste bli naturligt att ”tänka telekrig”. Det gäller både förband som har resurser för telekrig och de som kan utsättas för telekrig.

Det krävs utbildning både av enskilda individer och förband för att klara detta. Det är också nödvändigt att telekrig finns med som en naturlig del vid övningar. För att säkerställa att olika materielsystem fungerar i ett aktuellt område vid en insats är det viktigt att de insamlade uppgifterna (datasatser) är uppdaterade och relevanta. Datasatser och underlag ska analyseras och testas såväl i laboratoriemiljö som genom prov och försök.

Kunskap om telekrigsföring bör ingå i alla utbildningssteg så att officeren i sin befattning kan bedöma möjligheter och hot, både för eget förband och dess materiel. Lika viktigt är det att förstå motståndarens möjligheter att verka mot våra egna förband.

För att tillgodose behoven tillhandahåller Försvarsmakten årligen en orienterande kurs om telekrig för försvarsanställd personal. Centrala kurser och utbildningar inom officersyrket har dock minskat under 00-talet. Försvarsmakten borde i stället fördjupa utbildningen utifrån ett omvärldsperspektiv och hur telekrig används.

Sverige satsar på statlig forskning inom telekrig vid FOI för att skaffa kunskap inom områden med hög integritet och där det finns få publikationer om erfarenheter och innovation. Forskningen utgör grunden för att bygga upp kompe-

tensen och kompletterar den civila delen, som främst finns inom försvarsindustrin.

Forskare deltar i hela kedjan, från forskning tills dess att utrustningen för telekrig programmeras. På så sätt kan forskningsresultat och annan kunskap användas såväl vid prov och försök som vid validering och verifiering. Men kompetensen hos forskarna används också vid upphandling och kurser samt vid föreläsningar på olika nivåer, både på skolor och förband. Det skapar en närhet mellan olika instanser som är involverade i utvecklingen och upprätthåller därmed funktion och förmåga i våra telekrigssystem.

Telekrigssystemen behöver ständigt uppdateras mot aktuella hot och målsystem, eftersom signalmiljön varierar i olika operationsområden över tid. Funktioner tas fram och testas, både med nationella resurser och i internationella samarbeten, och programmeras sedan i systemen. Verksamheten kräver en omsorgsfull granskning och kontroll för att programmerade funktioner ska få verkan. Ett felaktigt utfall eller felaktig signal kan skapa en helt motsatt effekt än den avsedda. Verksamheten är en förutsättning för fungerande system, som personalen har förtroende för. Det är framför allt viktigt när det gäller skydd av plattformar, fordon och personer samt varnar- och motverkanssystem (VMS) och olika former av skydd mot fjärrutlösning av bomber. Men det är också av stor betydelse för att den taktiska signalspaningen ska kunna ge detaljerat underlag och information till lägesbilden.

Inom forskning och teknikutveckling vid FOI och FMV används i stor utsträckning labbutrustningar och simulatorer. Vissa har genom åren avknoppats till rena utbildningssystem, som

används för utbildning, planering och analys. Det är ett värdefullt mervärde från forskningen och en god bas för kompetensuppbyggnad och förståelse på olika nivåer inom Försvarsmakten.

Utbildning inom telekrig kan bedrivas mycket effektivt om eleverna har tillgång till interaktivt kursmaterial. Då kan de prova olika lösningar och därigenom få en känsla för problemet och vilka medel som kan vara lösningen. Simuleringsmodeller tillsammans med ett visualiseringsverktyg är en mycket bra start för detta utbildningsmaterial, men det krävs ofta en anpassning av forskningsmodellerna för att ta fram relevanta och pedagogiska scenarier.

Ett bra exempel på en kombination av utveckling, utbildning, träning och analys är utvecklingen av marinens verktyg ”Simuleringar för Telekrigsutbildning med Robotar och Motmedel” (STURM). Marinens personal får med verktyget prova olika typer av motmedel mot flera olika sjöhotrobotsystem. Verktöget är en vidareutveckling av forskning och analyser som kompletterats med utbildning i telekrigsinsatser mot sjörobotsystem. Sammantaget ger utbildningspaketet goda möjligheter till träning och ökad förståelse för aktuella dueller samt indirekt möjligheter till utveckling av stridsteknik och taktik. Detta sker inom ett område där det ofta är svårt att öva med realistiska hot och insatser.

Soldater måste också, som en naturlig del såväl av grundutbildning som av övningar, ges vana att agera i en miljö där telekrigföring ingår. Det är viktigt att inse att telekrigföringen är en realitet så fort man till exempel sänder och lyssnar med radio eller spanar med radar.

Ett ökat internationellt engagemang för svenska förband inom Nato kräver utbildning i procedurer och arbetsmetoder för staben vad gäller samordning av underrättelsetjänst, telekrigföring och ledningssystem. Även om många detaljer och resultat är hemliga är möjligheten till samarbete om sådant som metoder viktig att ta vara på. Telekrigsåtgärder kan omedvetet drabba både allierade och civila, vilket kan få fatala konsekvenser. Det ökande behovet av internationella övningar speglar också behovet av att öva med civila myndigheter och aktörer. Dagens och morgondagens signalmiljö är i mycket stor utsträckning alstrad av civila system.

I Försvarsmakten får personal som uppfyller kriterier för tjänstgöringstid och befattning ett specialutbildningstecken som symbol för deras erfarenhet, se figur 89. ■



Figur 89. Specialutbildningstecken m/02 för Telekrig.

Avslutning

Det osäkra omvärldsläget gör det svårt att göra långsiktiga bedömningar om utvecklingen inom telekrigsområdet. Den tekniska utvecklingen påverkar samhällsfunktioner där mer och mer teknik blir trådlös, samtidigt som allt fler civila applikationer, till exempel kommunikation, navigering och IT-infrastruktur, ofta saknar skydd mot störningar.

Störning av satellitbaserade system, som GPS, genomförs i allt högre grad även utanför konfliktområden och har noterats även i Östersjön. För civil sjöfart och flygtrafik innebär det inte bara problem, utan kan även innebära fara.

Kriget i Ukraina har visat hur civila system används i militära syften. Civil mobiltelefoni utnyttjas av båda sidor för såväl positionering av motståndare som för påverkansoperationer. Vidare utnyttjas sociala medier för att sprida budskap från bägge sidor.

Telekrig är en förutsättning för de flesta grundläggande förmågor. Signalspaning ger underlag för underrättelser medan elektronisk attack är en del i ett system med varierande grad av verkan och skydd. Tillsammans med elektronisk protektion ökar detta skyddet och uthålligheten såväl för sensor- och kommunikationssystem som för plattformar av alla slag.

Ledningsplatser och förband behöver följaktligen ges en låg signatur, såväl fysiskt som digitalt och elektromagnetiskt, för att erhålla ett så komplett och anpassat skydd som möjligt. Kvalificerad telekrigsföring är en effekthöjare på bredden genom att skapa en bättre förståelse för motståndarens system och aktiviteter, bidra till att nedsätta dennes förmåga att observera och följa våra förband och plattformar samt skydda våra resurser från motståndarens telekrigsföring och vapeninsatser. ■

Bilagor

Förkortningar

AD	Analog till digitalomvandlare	ESM	Elektromagnetisk stödverksamhet (eng. Electromagnetic Support Measures)
AESA	Aktiv elektriskt styrd antenn	EUV	Extrem UV-strålning
AI	Artificiell intelligens	FDOA	Frequency Difference of Arrival
AM	Amplitudmodulation	FH	Frekvenshopp (eng. Frequency Hopping)
ASLU	Adaptiv sidolobsundertryckning	FLIR	Forward Looking InfraRed
AWACS	Airborne Warning and Control System	FM	Frekvensmodulation
CCD	1 Charge-Coupled Device 2 Camouflage, Concealment and Deception	FPGA	Field Programmable Gate Array
CEMA	Cyber och elektromagnetiska aktiviteter	GaN	Galliumnitrid
CESMO	Cooperative Electronic Support Measure Operations	GLONASS	Globalnaya Navigatsionnaya Sputnikovaya Sistema (ryska GNSS)
CLWS	Compact Laser Weapon System	GMTI	Ground Moving Target Indication
CMOS	Complementary Metal-Oxide-Semiconductor	GNSS	Global Navigation Satellite System
CRPA	Controlled Radiation Pattern Antenna	GPS	Global Positioning System
DA	Digital till analogomvandlare	GSM	Global System for Mobile Communications
DDOA	Doppler Difference of Arrival	HARM	High Speed Anti-Radiation Missile
DIRCM	Directed IR Counter Measures	HF	High Frequency
DRFM	Digitala radiofrekventa minnen	HPM	High Power Microwaves
DS	Direktsekvens (eng. Direct Sequence)	IR	Infrarött (eng. Infrared)
EA	1 Elektromagnetisk attack 2 Elektronisk attack	IRST	IR Search and Track
ECCM	Electronic Counter Counter Measures	ISR	Intelligence, Surveillance and Reconnaissance
ECM	Electronic Counter Measures	JSR	Förhållandet störsignal till nyttosignal (eng. Jammer-to-Signal Ratio)
EMKON	Kontrollerad emission (eng. Emission Control, EMCON)	KOS	Kommunikationssignalspaning
EO	Elektrooptik, elektrooptisk	LBI	Långbasinterferometri (eng. Long Baseline Interferometry)
EOB	Electronic Order of Battle	LBM	Lokal brytningsindexmodell
EP	Elektronisk protektion	LIDAR	Light Detection and Ranging
EPM	Elektromagnetisk protektion (eng. Electromagnetic Protective Measures)	LPI	Low Probability of Intercept
ES	Elektronisk stödverksamhet (eng. Electronic Support)	LTE	Long Term Evolution
		LWIR	Långvågig IR (eng. Long Wave IR)

MANPADS	Man Portable Air Defence Systems	SNR	Signal till brusförhållande (eng. Signal-to-Noise Ratio)
MASS	Multi Ammunition Softkill System	STAP	Space-Time Adaptive Processing
MC	Multi Constellation	SWIR	Kortvågig IR (eng. Short Wave IR)
MF	Multi Frequency	TDOA	Time Difference of Arrival
MIMO	Multiple Input Multiple Output	TES	Teknisk signalspaning
MTI	Moving Target Indication	TIR	Termisk IR
MWIR	Mellanvågig IR (eng. Medium Wave IR)	TKSE	Telekriststödenheten, förband i Försvarsmakten
NIR	Nära IR (eng. Near IR)	TRM	Sändar/mottagarmodul (eng. Transmit/Receive Module)
NVG	Bildförstärkare (eng. Night Vision Goggles)	TWT	Vandringsvågrör (eng. Travelling Wave Tube)
OFDM	Orthogonal Frequency Division Multiplex	UAV	Unmanned Aerial Vehicle
PAT	Pointing, Acquisition and Tracking	UCK	Kosovos befrielsearmé (albanska Ushtria Çlirimtare e Kosovës)
PCA	Polar Cap Absorption	UHF	Ultra High Frequency
PM	Fasmodulation (eng. Phase Modulation)	UMTS	Universal Mobile Telecommunications System
PPI	Plan Polär Indikator (eng. Plan Position Indicator)	UV	Ultraviolett
PRF	Pulsrepetitionsfrekvens	UWB	Ultra Wide-Band
PRI	Pulse Repetition Interval	VGPO	Velocity Gate Pull Off
PRS	Public Regulated Service	VHF	Ultrakortvåg (eng. Very High Frequency)
PVT	Position, Velocity & Time	VIS	Visuellt
RADAR	Radio Detection and Ranging	VMS	Varnar- och motverkanssystem
RAM	Radarabsorberande material	VSS	Vilseledning, signaturanpassning och skenmålsåtgärder
RCS	Radar Cross Section	5G NR	5 th Generation New Radio
RF	Radio Frequency		
RSR	Relativ störräckvidd		
RWR	Radar Warning Receiver		
SAR	Syntetisk aperturradar		
SAT	Signaturanpassningsteknik		
SDR	Mjukvaruradio (eng. Software Defined Radio)		
SEAD	Suppression of Enemy Air Defence		
SHF	Superhög frekvens		
SID	Sudden Ionospheric Disturbance		
SIGINT	Signals Intelligence, jfr SIGUND		
SIGUND	Signalunderrättelsetjänst, jfr SIGINT		
SIS	Signalspaning		

Litteraturlista

Allmänt

Price, A., Instruments of darkness – The history of Electronic Warfare, Macdonald and Jane's Publishers Limited, 1977.

FOI orienterar om Sensorer, FOI, 2004.

FOI orienterar om Telekrig, FOI, 2005.

Telekrig – lärobok för armén, Försvarsmakten, M7746-168001, 1997.

Vågutbredning

Asp, B, Vågutbredning över mark och hav – kurskompendium, FOI-R--0038--SE, 2001.

Haglund, A., et al., Programmet LBM – En användarhandledning: Ett stöd för bedömning av radarräckvidd hos marinens fartyg, FOI-R--5658--SE, 2025.

Nelsson, C., et al., Results from Baltic 99 maritime measurements. Optical wave propagation and IR background, FOA-R--00-01771-615--SE, 2000.

Saunders, S. R., Aragón-Zavala, A. A., Antennas and Propagation for Wireless Communication Systems, 3rd Edition ISBN: 978-1-119-33220-6, september 2024.

Smith, F. G. (ed.), The Infrared & Electro-Optical Systems Handbook, Vol. 2: Atmospheric Propagation of Radiation, SPIE Optical Engineering Press, 1993.

Radiokommunikation

Ahlin, L, Zander, J., Slimande, B., Principles of Wireless Communications, Studentlitteratur.

Bergdal, H., et al., Signalspaningsteknik del 1, Grunder samt radiosignalspaning, FOI, 2001.

Bergström S., Nilsson S., Globala Satellitnavigeringssystem: En översikt över öppna signaler och tjänster, FOI-R--5610--SE, 2024.

Bolander, G., et al., Fri optisk kommunikation, En förstudie, FOA-R--99-01296-504--SE, 1999.

Eklöf, F., Pääjärvi L., Telekrig mot GNSS – årsrapport 2004, FOI-R--1415--SE, 2004.

Hansson, A., Grönkvist, J., Radionätsarkitekturer, FOI-R--3697--SE, 2013.

Mehrotra, A., et al., GSM System Engineering, Artech House, 1999, ISBN 0-89006-860-7.

Murthy, C. S. R., Manoj, B. S., Ad Hoc Wireless Networks – Architecture and Protocols, Prentice-Hall, 2005.

Proakis, J. G., Digital Communications, McGraw Hill.

Sklar, B., Digital Communications – Fundamentals and Applications, Prentice-Hall.

Radar

- Andersson, B., et al., Flygburen passiv lägesbestämning baserad på noggrann frekvensmätning, FOI-R--0329--SE, 2001.
- Andersson, B., et al., Precisionslägesbestämning med flygburna radarsensorer, FOI-R--0719--SE, 2002.
- Andersson, B., et al., Sensorsamverkan för radarvarning och taktisk radarsignalspaning, FOI-R--1335--SE, 2004.
- Bergdal, H., et al., Signalspaningsteknik del 2, Radarsignalspaning, FOI, 2002.
- Curland, J., McDonough, R., Synthetic Aperture Radar – System and Signal Processing, John Wiley & Sons, 1991.
- Hyberg, P., Kompendium i Radarmotmedelsteknik, FOA A 10052-1.1, 1993.
- Kingsley, S., Quegan, S., Understanding Radar Systems, SciTech Publishing, 1999.
- Robertson, S., Practical ESM Analysis, Artech House, 2019.
- Scheler, D. C., Introduction to Electronic Warfare, Artech House, 1986.
- Skolnik, M., Introduction to Radar Systems, McGraw-Hill, 2001.
- Stimson, G., Introduction to Airborne Radar, SciTech Publishing, 1998.
- Lärobok i telekrig för luftvärnet – Radar och radartaktik, Försvarmakten, M7741-850101, 2004.

Elektrooptik

- Campana, S. B. (ed.), The Infrared & Electro-Optical Systems Handbook, Vol. 5: Passive Electro-Optical Systems, SPIE Optical Engineering Press, 1993.
- Fox, C. S. (ed.), The Infrared & Electro-Optical Systems Handbook, Vol. 6: Active Electro-Optical Systems, SPIE Optical Engineering Press, 1993.
- Jelalian, A. V., Laser Radar Systems, Artech House, 1991.
- Pollock, D. H., (ed.), The Infrared & Electro-Optical Systems Handbook, Vol. 7: Countermeasure systems, SPIE Optical Engineering Press, 1993.
- Strömberg, P., Pettersson, M., Laserstyrda vapen och laservarnare – en introduktion, Kurskompendium för Robusta Optroniksystem, FOI, 2003.

Laserkommunikation

- Brashears, T. R., Achieving 99% link uptime on a fleet of 100G space laser inter-satellite links in LEO, in Free-Space Laser Communications XXXVI, 2024, vol. 12877: SPIE.
- Dhruv, F., Kaushal, H., A Review of Pointing Modules and Gimbal Systems for Free-Space Optical Communication in Non-Terrestrial Platforms, Photonics, vol. 12, no. 10, 2025.
- Jahid, A., Alsharif, M. H., Hall, T. J., A contemporary survey on free space optical communication: Potentials, technical challenges, recent advances and research direction, Journal of Network and Computer Applications, vol. 200, 2022.

Moll, F. et al., Demonstration of High-Rate Laser Communications From a Fast Airborne Platform, IEEE Journal on Selected Areas in Communications, vol. 33, no. 9, pp. 1985–1995, 2015.

Sjöqvist, L., Kullander, F., Berneland, J., Håkansson V., Johansson, V., Förstudie laserkommunikation till drönare, FOI-D--1231--SE, 2023.

Younus, O. I. et al., Overview of Space-Based Laser Communication Missions and Payloads: Insights from the Autonomous Laser Inter-Satellite Gigabit Network (ALIGN), Aerospace, vol. 11, no. 11, p. 907, 2024.

Tillämpningar

Heikell, J., Electronic Warfare Self-Protection of Battlefield Helicopters: A Holistic View, Series E: Electronics Publications E18, Helsinki University of Technology, 2005.

Hultman S., et al., Provisorisk användarhandledning för duellsimulering mellan robot och fartyg, DSImSSo försöksversion 2.0, FOI-R--0055--SE, 2001.

Olsson, G., et al., VMS-funktion i nätverk för stridsfordonsförband, några typfall, FOI-R--1328--SE, 2004.

Specialområden

Bäckström, M., Lövstrand, K. G., Susceptibility of Electronic Systems to High-Power Microwaves: Summary of Test Experiences, IEEE Transactions on Electromagnetic Compatibility, Vol. 46, No. 3, August 2004, pp. 396–403.

Del Monte, L. A., War at the Speed of Light: Directed-Energy Weapons and the Future of Twenty-First-Century Warfare. University of Nebraska Press, 2021.

Linder, S., et al., Intersystem Interference Risks in the Future Swedish Defence, FOI-R--1405--SE, 2004.

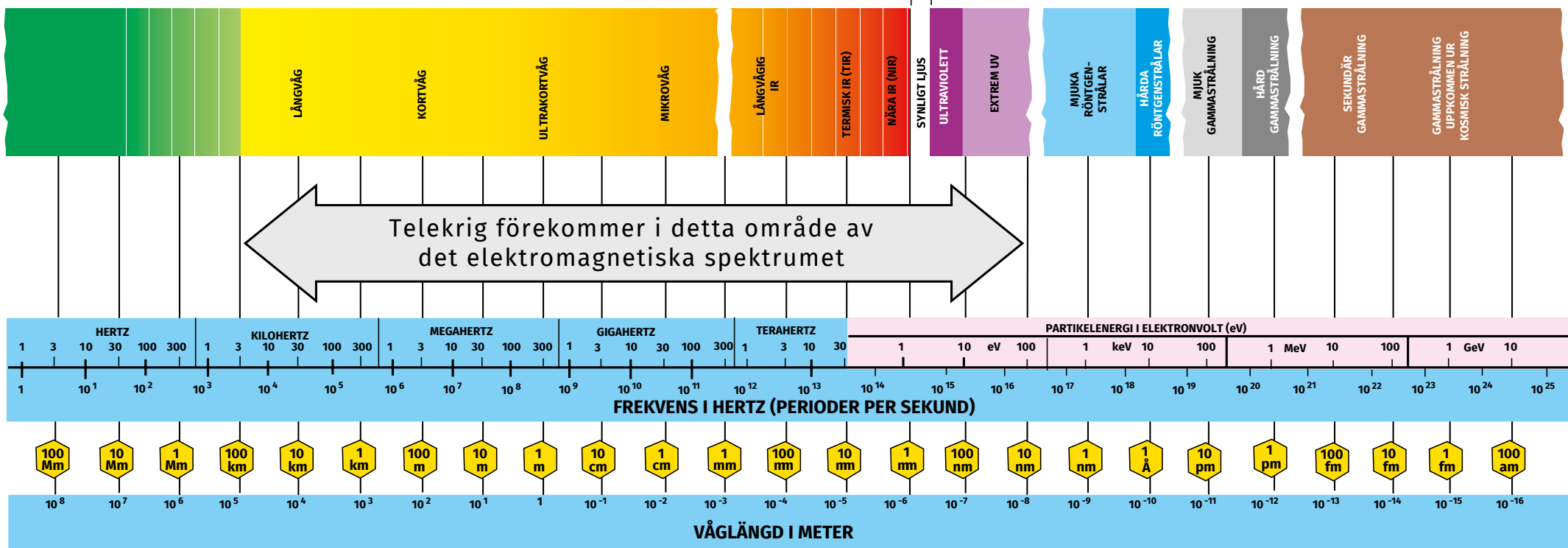
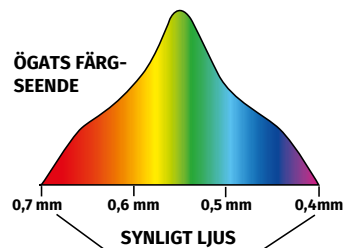
Stenumgaard, P., Utbildningskompodium – Telekonflikt, FOI Dnr 01-3924, 2000.

Stenumgaard, P., Telekonfliktforskning vid FOI 1995–2002 – Slutrapport, FOI-R--0682--SE, 2002.

FOI orienterar om: Elektromagnetiska vapen och skydd, FOI, 2001.

SAT-handbok Mark, FOI, 2003.

DET ELEKTROMAGNETISKA SPEKTRUMET



OMRÄKNINGSTABELL	BETECKNING	FÖR-KORTN.	10-POTENS	MULTIPLAR OCH DELAR
Ljushastigheten	tera-	T	10 ¹²	En biljon
$c = 3 \times 10^8$ meter/sekund	giga-	G	10 ⁹	En miljard
Våglängd i meter	mega-	M	10 ⁶	En miljon
$\lambda = \frac{c}{f}$	kilo-	k	10 ³	Ett tusen
Frekvensen i hertz	hekto-	h	10 ²	Ett hundra
$f = \frac{c}{\lambda}$	deka-	da	10 ¹	Tio
Energi i elektronvolt (eV)	deci-	d	10 ⁻¹	En tiondel
$E = h \times f$	centi-	c	10 ⁻²	En hundraedel
$h = 4,1 \times 10^{-15}$ eV $\times$ sekund (Plancks konstant)	milli-	m	10 ⁻³	En tusendel
	mikro-	μ	10 ⁻⁶	En miljontedel
	nano-	n	10 ⁻⁹	En miljarddel
	piko-	p	10 ⁻¹²	En biljondel
	femto-	f	10 ⁻¹⁵	En kvadriljondel
	atto-	a	10 ⁻¹⁸	En kvintiljondel
	Ångström	1 Å	1 $\times$ 10 ⁻¹⁰ m	En tiomiljarddel meter

Den här skriften ger en introduktion till området telekrig. Det handlar främst om militär verksamhet som utnyttjar det elektromagnetiska spektrumet för att påverka en motparts förmåga att inhämta, bearbeta eller dela information.

Skriften riktar sig särskilt till dig som har en yrkesroll där telekrig ingår, men även andra vars verksamheter kan påverka eller påverkas av telekrigföring.