FOI

orienterar

om

Nummer 5 2005

Telekrig

I detta OM-nummer ger FOI en orientering om området Telekrig. Det är ett område som har stor betydelse för varje försvarsmakt. Därför är det i stora delar omgärdat av hög sekretess såväl i Sverige som utomlands. Det bidrar till att det inte är lätt att hitta litteratur som täcker hela området.

Betydelsen och behovet av kunskap om telekrig ökar i och med att svenska förband i ökad utsträckning deltar i internationella insatser. FOI, och tidigare FOA, har bedrivit forskning inom området under lång tid. Teknik och systemlösningar som nu används inom Försvarsmakten har tagits fram. Några exempel är utrustning för signalspaning och störning (Snabbpejl, MOPS och Tarax). Den ökade fokuseringen på internationella insatser ställer krav på effektiva varnings- och motverkanssystem för skydd av plattformar och förband. Forskningen ger stöd för beslut om lämpliga tekniker och taktiskt uppträdande i olika hotscenarier.

Telekrig kan dels ses som ett hot och dels som en möjlighet för skydd. De offensiva delarna av telekrig som exempelvis avsiktlig radiostörning kan även karaktäriseras som ”icke-dödligt vapen”. Detta är väsentligt för hur tekniken utnyttjas och vilka möjligheter den ger i en breddad hotbild där såväl Försvarsmakten som det civila samhället kan behöva möta exempelvis terrorism. Forskningen inom telekrig har därför många utmanande och spännande uppgifter i framtiden. Jag hoppas att FOI med denna skrift ökar medvetenheten om betydelsen av telekrig och dess tillämpningar för ett säkrare samhälle.

Madelene Sandström
Generaldirektör

Nummer 5 2005

FOI orienterar om

Telekrig

Den här boken kan beställas från
TOTALFÖRSVARETS FORSKNINGSINSTITUT (FOI)

INNEHÅLL

INTRODUKTION 4

VÅGUTBREDNING 11

TELEKRIG MOT RADIOKOMMUNIKATIONSSYSTEM 17

TELEKRIG MOT LASERKOMMUNIKATIONSSYSTEM 31

TELEKRIG MOT RADARSYSTEM 37

TELEKRIG MOT ELEKTROOPTISKA SYSTEM 53

HPM OCH STÖRNING AV NAVIGERINGSSYSTEM 67

TILLÄMPNINGAR OCH NÄRLIGGANDE VERKSAMHETER 70

SKAPA KUNSKAP OCH INSIKT 82

TELEKRIG I BREDDAD HOTBILD 84

FÖRKORTNINGAR 88

LITTERATURLISTA 91

Redaktion: Lars Berglund, Göran Kindvall. **Medverkande experter:** Börje Andersson, Jan Arnsby, Börje Asp, Mats Bäckström, Fredrik Eklöf, Anders Eneroth, Leif Festin, Staffan Gadd, Rolf Gustavsson, Roland Heickerö, Peter Johansson, Peter Klum, Rolf Persson, Magnus Pettersson, Peter Stenumgaard. **Teckningar:** Martin Ek. **Layout:** Karina Sterntorp, Access Marketing AB. **Bild omslag:** Midjourney 2023.

Inledning

Syftet med denna skrift är att ge teknisk information om telekrig och sätta in telekrig i sitt sammanhang för att på så sätt förmedla översiktlig kunskap inom området. Läsaren skall inte behöva ha teknisk bakgrund för att kunna tillgodogöra sig innehållet. För att underlätta förståelsen finns förklarande bilder till den löpande texten samt faktarutor som utgör fördjupningar.

Med telekrig avses militär verksamhet som utnyttjar det elektromagnetiska spektrumet för att bekämpa, förvanska eller exploatera motparters inhämtning, bearbetning eller delgivning av information samt skydd mot ogynnsamt utnyttjande av det elektromagnetiska spektrumet.

En vanlig indelning av området är i följande delområden: elektronisk stödverksamhet (ES), elektronisk attack (EA) samt elektronisk protektion (EP).

Den elektroniska stödverksamheten har som syfte att upptäcka, identifiera och lägesbestämma elektromagnetiska källor. Elektronisk attack innebär utnyttjande av elektromagnetisk energi i syfte att nedsätta eller förstöra en motparts systemfunktioner eller stridsförmåga. Med elektronisk protektion menas de åtgärder som minskar effekten av motståndarens telekrigföring samt åtgärder för att undvika elektromagnetiska konflikter. En likartad och vanligt förekommande indelning är ESM (Electronic Support Measures), ECM (Electronic Counter Measures) och ECCM (Electronic Counter Counter Measures).

ES	Taktisk signalspaning	
	Varning	radar-, laser-, UV- och IR-varnare
EA	Telemotmedel	störsändning, skenmål
	Vilseledning	falsk signalering, skenmålsgenerering
	Elektromagn.vapen	HPM-vapen, laservapen
EP	Teleskydd	störskydd, HPM-skydd, laserskydd
	Emissionskontroll	

Figur 1. Begrepp och indelning för telekrig.

Då offensiv telekrigföring är en ickedödlig och graderad verkansform kan den med fördel utnyttjas vid internationella insatser.

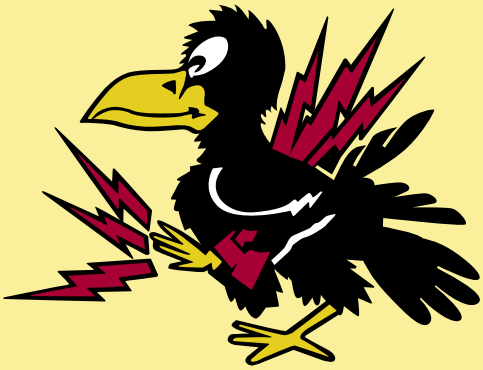
Elektromagnetiska signaler påverkas av vågutbredningsförhållanden och den miljö de uppträder i. Detta beskrivs kortfattat i avsnittet elektromagnetisk vågutbredning.

Denna skrift beskriver i huvudsak telekrig mot kommunikations- och sensorsystem. System mot vilka telekrig kan verka ges en översiktlig beskrivning. Telekrigåtgärder presenteras uppdelat i elektronisk stödverksamhet (ES), elektronisk attack (EA) och elektronisk protektion (EP)

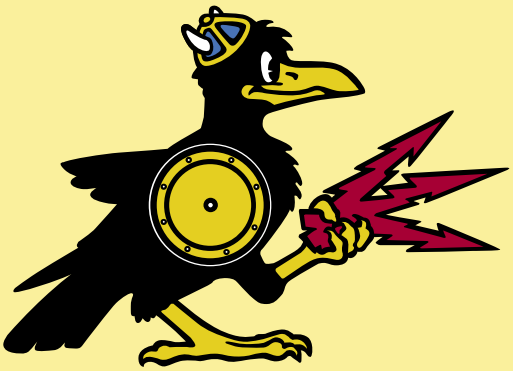
Därutöver tas vissa andra telekrigrelaterade områden upp, t.ex. HPM och navigationskrigföring. Tillämpningar av telekrig presenteras på såväl förbandsnivå som för egenskydd. Även angränsande tillämpningar redovisas, dock utan att de för den skull är telekrig. Vidare beskrivs hur telekrig kan tränas och övas för att skapa kunskap och insikt.

Utöver detta tas frågor kring framtida tillämpningar av telekrig upp, såväl avseende nya tekniska lösningar som nya sätt att utnyttja tekniken. I de senare ingår t.ex. hot mot civila system.

Symboler



Figur F1. Internationell telekrigsymbol.



Figur F2. Svensk telekrigsymbol.

Såväl internationellt som i Sverige har ”kråkan” (egentligen en korp) kommit att bli en symbol för telekrig och telekrigare. Detta har sin bakgrund i att det amerikanska flygvapnet under 2:a världskriget använde varnar- och motmedelssystem mot radar. Dessa system gavs kodnamnet ”Raven” (korp) och operatörer för systemen kallades för ”Ravens”. Efter kriget skapades ett utbildningsprogram i USA för telekrigoperatörer. I samband med detta byttes benämningen från korp till kråka, som således refererar till motmedelsoperatör.

Exempel från naturen

I naturen förekommer telekrig och övrig signalkrigföring i stor omfattning. Den vanligaste sensorn är ögat, och ett vanligt skydd inom naturen är signaturanpassning till omgivningen. Detta leder till att bytesdjur i många fall har kamouflagefärgad päls eller fjäderdräkt. Kameleonten är känd för att ändra sin färg beroende på sin omgivning. Skorpionfisken (som är en av de giftigaste fiskarna i världen) utnyttjar också sin förmåga att likt kameleonten ändra färg efter omgivningen på sin jakt efter byte. Svalstjärtsfjärilslarven efterliknar fågellort för att på så sätt slippa bli byte. En vilseledningsåtgärd kan vara att som kungssnoken (som är ofarlig) till sin teckning efterlikna korallormen (som är giftig). Inom biologin används begreppet batesisk mimikry för djur som inte är giftiga som härmar ett giftigt djur. Även motmedel utnyttjas i naturen. Ett exempel på detta är bläckfiskar som kan utnyttja bläck som läggs ut vid fara, oftast kombinerat med undanmanöver. Somliga djuphavsbläckfiskar kan avge ett fluorescerande ämne för att förstöra mörkerseendet hos motparten.

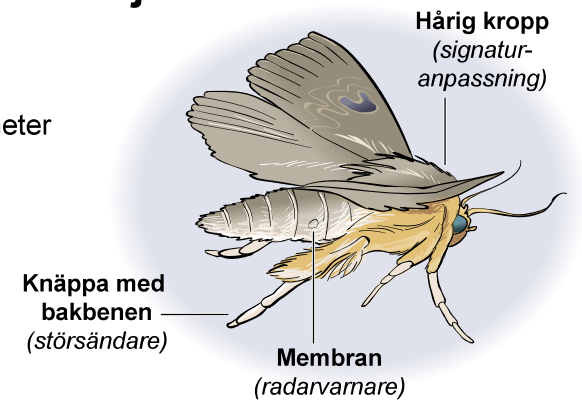
Ett exempel på signalkrigföring från naturen är att närma sig bytet mot vinden för att bytet inte skall känna vittringen av det jagande djuret. Skunken i sin tur använder sig av sensormättning. Kattdjurens smygande och ugglornas tysta flygande är sätt för att bytesdjur inte skall kunna utnyttja sin hörsel. Men inom akustiken är kanske duellen mellan fladdermusen och nattfjärilen den som närmast påminner om telekrig, se figur 2.

Duell mellan fladdermus och nattfjäril - medel och motmedel

Nedan beskrivs den akustiska duellen mellan fladdermus och nattfjäril vilken har många likheter med telekrigföring.

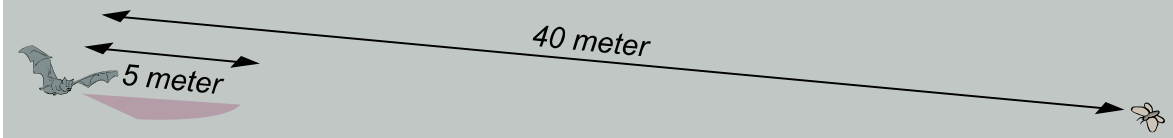
Fladdermusens vapen vid jakt är en ultraljuds-radar med kort våglängd på ca 1 cm. Med hjälp av sin ljudradar kan fladdermusen detektera byten på ca 5 meters avstånd.

Nattfjärilen har hår på kroppen vars längd är en fjärdedel av fladdermusens använda våglängd. Det gör att nattfjärilen blir signaturanpassad.

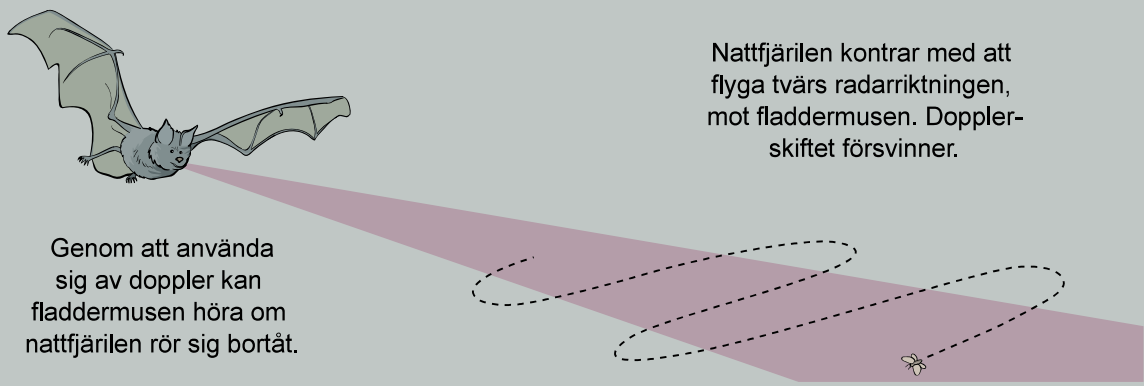


1. Avstånd

Avståndet mellan nattfjärilen och fladdermusen kan vara upp till 5 m för att fladdermusen skall kunna detektera nattfjärilen. Nattfjärilen har membran som känner av ljudet från fladdermusen på ca 40 meter.



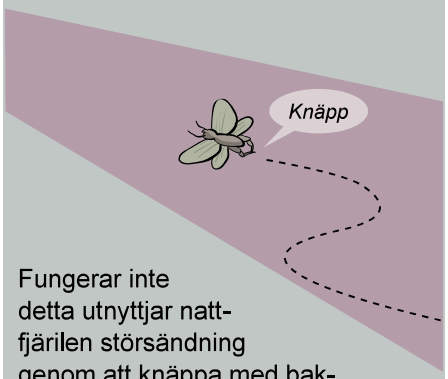
2. Manövreringsteknik mot doppler



Nattfjärilen kontrar med att flyga tvärs radarriktningen, mot fladdermusen. Doppler-skiftet försvinner.

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

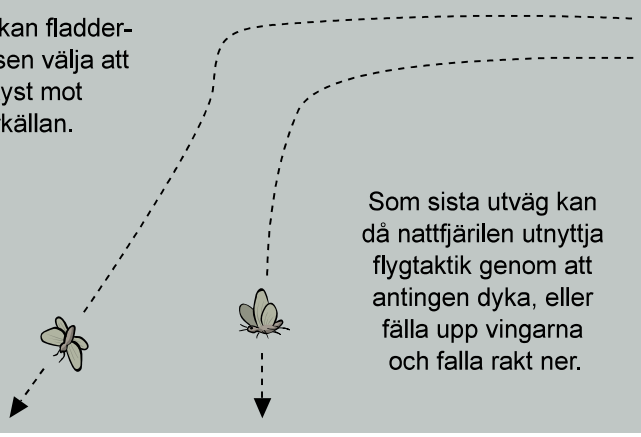
3. Störsändning



Fungerar inte detta utnyttjar natt-fjärilen störsändning genom att knäppa med bak-benen (avstånd ca 0,5 meter).

4. Flygtaktik mot radartystnad

Nu kan fladder-musen välja att gå tyst mot störkällan.



Som sista utväg kan då nattfjärilen utnyttja flygtaktik genom att antingen dyka, eller fälla upp vingarna och falla rakt ner.

Figur 2. Duellen mellan fladdermus och nattfjäril.

Exempel på telekrig i krig och konflikter

Användandet av remsor

Under 2:a världskriget diskuterades i Storbritannien hur man skulle kunna störa tyska radarstationer. En lösning var att utnyttja metallbelagda papper (remsor). Diskussioner fördes under 1940 och inledande prov genomfördes under 1941 under stark sekretess, för att inte tyskarna skulle få reda på något. Under 1942 var remsorna (eng. chaff) utvecklade och testade, men den brittiska ledningen under Churchill tillät inte att remsorna användes. I Tyskland hade problematiken också studerats. I Tyskland användes begreppet ”düppel”. Test och prov hade genomförts under 1942, även här under stark sekretess. Av rädsla att britterna skulle använda remsor om Tyskland började använda det förbjöd Göring fortsatt utveckling av remsor.

I Storbritannien gavs tillstånd att använda remsor i samband med bombningen av Hamburg den 23 juli 1943. Koden för användandet av remsor var ”Open the Windows”. I bombningen av Hamburg sattes 795 bombflygplan in. 92 miljoner aluminiumremsor släpptes i samband med bombningen (motsvarar ca 40 ton). Förlusterna för britterna var 12 flygplan (1,5%). Det normalt förväntade antalet förluster var vid denna tid ca 6 %.

Falklandskriget

Under Falklandskriget 1982 kom remsor att utnyttjas mot radarsökande robotar av typ Exocet. Den 26:e maj avfyrades två Exocetrobotar från flygplan mot brittiska fregatten HMS Ambuscade. Fregatten som upptäckt hotet innan robotarna avfyrats, hade redan hunnit lägga ut remsor. Robotarna låste på remsmolnet, och HMS Ambuscade gick fri. När robotarna passerat remsorna återgick de till sökfas och fann då RORO-fartyget Atlantic Conveyor som träffades och sänktes. Atlantic Conveyor hade inga telekrigsystem och innehöll mycket materiel som britterna hade behövt.

Bekaadalen

Bekaadalen 1982 brukar ofta framhållas i samband med att telekrigföringens möjligheter diskuteras. Den israeliska sidan utnyttjade då skenmålsrobotar för att lura luftvärnsradar att dra igång. Radarsignalerna kunde mätas in och signalsökande robotar sattes in mot de syriska radarstationer som var i gång. Vidare utnyttjade israeliska jaktpiloter det faktum att de syriska jaktflygplanens radarvarnare hade ”blinda” sektorer. Utöver detta störddes kommunikationen mellan de syriska flygplanen och stridsledningen ut av israelerna, vilket bidrog till att fler syriska flygplan blev nerskjutna. Denna konflikt var i detta avseende ganska asymmetrisk, d.v.s. israelerna var överlägsna avseende telekrig.

Desert Storm

Desert Storm innebar ett genombrott för rymdbaserade system (för övervakning och navigering), kryssningsrobotar, signaturanpassningsteknik som medel mot luftförsvaret och avancerad radar i kritiska roller (flygburen markövervakning, bekämpning av luftförsvaret). Styrda vapen (laserstyrda, elektrooptiska, signalsökande) kom också att få stort genomslag.

Desert Storm gav sensorer möjlighet att verka fullt ut genom stora skjutavstånd m.m. T.ex. hade de amerikanska stridsvagnarna sensorer vilkas räckvidd i mörker klart överträffade de irakiska stridsvagnarnas sensorer. Detta innebar att de amerikanska stridsvagnarna kunde skjuta innan de irakiska stridsvagnarna ens upptäckt hotet.

Telekrig användes av den allierade sidan genom att flygburna plattformar utnyttjades för att störa radar (F-4G Wild Weasel, EA-6B Prowler etc.) och kommunikation (EC-130H Compass Call och EA-6B) på den irakiska sidan.

F-117A flög aldrig in över Irak under Desert Storm utan understöd av EA-6B, som störde. Besättningarna i F-117A var dock inte alltid så glada åt EA-6B i Irak. När störningen sattes in började irakierna skjuta “vilt” med luftvärnskanoner. D.v.s. telekriginsats sågs som tecken på flyganfall. Detta är en av de indirekta effekter som kan vara svåra att förutse.

Signalsökande robotar kom att få stor effekt. Mer än 1000 st. HARM (High speed AntiRadiation Missile) avfyrades. Detta ledde till att endast 5% av de irakiska radarsystemen var på efter 6 dagar (inledningsvis var alla system på).

Kosovokriget

Kosovo blev något annorlunda, eftersom vädret kraftigt kom att försvåra utnyttjandet av elektrooptiska sensorer. Det var dåligt väder med mycket regn. Laserutpekningen, som fungerat så bra

under Desert Storm, fungerade inte lika effektivt i Kosovo. Laser- och elektrooptiskt styrda vapen kan inte fungera i dåligt väder. Alternativet var radar (radarsystem är mindre väderberoende). En erfarenhet från Kosovo som brukar lyftas fram i USA är behovet av GPS-styrning för att nå tillräcklig vapenprecision.

Koalitionen lyckades inte slå ut det jugoslaviska luftförsvaret, bl.a. på grund av att de utnyttjade skenmål. Radarsystemen var dessutom avstängda. Det jugoslaviska luftförsvaret var också ett redundant system med välutbildade och väl övade operatörer och disciplinerad taktik. Förmodligen hade den jugoslaviska sidan dragit lärdomar från Desert Storm.

Oförmågan att nå effekt mot luftförsvaret under de 78 dagarnas krig kom att påverka Nato-flygets uppträdande. Detta ställde krav på kontinuerlig bekämpning av luftförsvaret och krävde ISR (Intelligence, Surveillance and Reconnaissance) och SEAD (Supression of Enemy Air Defence) hela tiden. Nato-flygplan fick inte flyga under 15000 fot (4500 meter). Dessutom blev kriget mycket påfrestande för besättningar i EA-6B. Även stealthbombaren B-2 understöddes av dessa telekrigflygplan. Flyginsatserna mot den jugoslaviska armén blev effektiva först sedan UCK börjat sin offensiv.

Svenska exempel på tillämpad telekrigföring

Erfarenheter från internationella insatser med telekrigförband

Svenska telekrigförband har deltagit i fredsfrämjande insatser. Exempel på uppgifter har varit att övervaka stridande parters vapendepåer, eller deras gruppering, förehavande och rörelser i ett område.

Med sina sensorer har telekrigförbandet kunnat komplettera övervakningen i det elektromagnetiska spektrumet och skapat ”normalbilder” samt rapporterat avvikelser. Detta har bidragit till att öka förmågan till ”force protection” och givit en bättre överblick i det egna området. Detta skapar förutsättningar för en långsiktigare planläggning som kan utnyttjas då det krävs snabba insatser. Den information som telekrigresurserna bidrar med ger ett bättre underlag för beslut om insatser.

Figur 3. Signalspaningsenhet i Kosovo. Foto: Försvarsmakten/Jan Dahlén.

Vid insatser som till sin karaktär är mer fredsframtvingande, kan telekrigresurser ges en mer aktiv roll. Förutom att genom övervakning understödja planering innan insats, kan telekrigförband aktivt påverka andra parters ledningsförmåga. Vidare kan telekrigresurser fortlöpande under insatsen på olika sätt bidra till vår lägesuppfattning.

Figur 4. 37E, telekrig-Viggen. Foto: Försvarsmakten/Lars-Åke Siggelin.

Erfarenheter från internationella övningar med telekrigförband

Sverige har vid flera tillfällen medverkat med flygburen offensiv telekrigföring (37E, telekrig-Viggen) vid den tyska telekrigövningen ELITE (Electronic warfare LIve Training and Exercise). Det taktiska uppträdandet och den tekniska utrustningen har haft god effekt mot jaktflyg och luftvärn. Resultat och erfarenheter från övningarna belyser de möjligheter telekrigföringen erbjuder såväl vid SEAD som för att försämra lägesuppfattningen för en motståndares jaktflyg.

I SEAD-fallet kan den flygburna offensiva telekrigföringen skapa ett ”fönster” som andra SEAD-förband utnyttjar för att bekämpa luftvärnssystemen.

Vad gäller jaktflyg kan flygburen offensiv telekrigföring försvåra motståndarens lägesuppfattning och därmed deras användning av långräckviddiga vapensystem. Vid övningarna har samverkande förband, tack vare understöd från 37E, kunnat lösa sina uppgifter mer effektivt.

Informationsarenan

För att beskriva kampen om informationsöverläge används begreppet informationsoperationer. Det handlar i korthet om att utnyttja och påverka en motståndares information samtidigt som egen information skall skyddas.

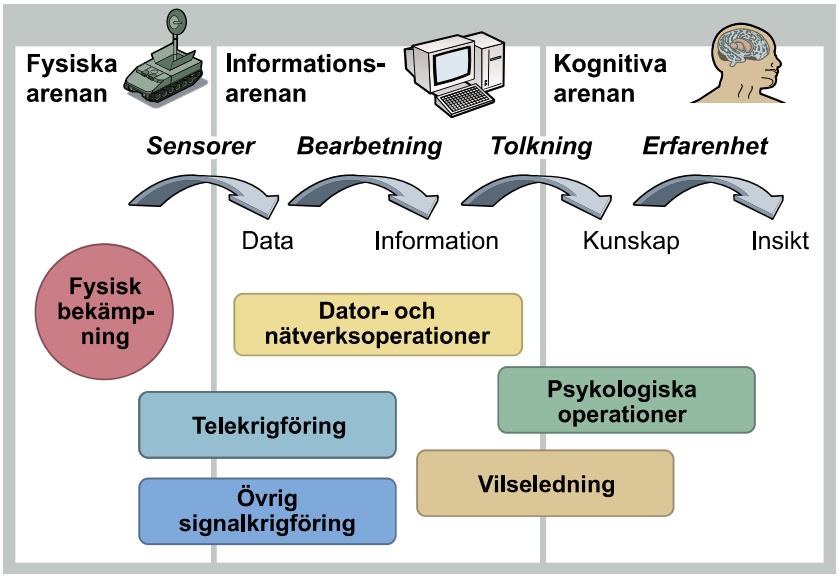
Inom Försvarsmakten utgör informationsoperationer ett stöd för att uppnå uppsatta militära mål på militärstrategisk, operativ eller taktisk nivå.

Bakom intresset för informationsoperationer ligger de nya typer av krigföring som är eller blir möjliga genom den tekniska utvecklingen. Det handlar om datavirus, logiska bomber, datainträng i nätverk, attacker mot infrastrukturen m.m. IT-relaterad krigföring är också potentiellt ett område där det kan vara möjligt för många nationer/aktörer att uppnå en kvalificerad förmåga.

Verkansförmågor inom ramen för informationsoperationer är psykologiska operationer (psyop), vilseledning, telekrigföring, dator- och nätverksoperationer (Computer Network Operations, CNO), övrig signalkrigföring och fysisk bekämpning. Övrig signalkrigföring är i flera avseenden snarlikt telekrig och presenteras närmare i avsnittet *Tillämpningar av telekrig och närliggande områden.*

Den fysiska världen omfattar markarenan, den maritima arenan och luftarenan och det är här huvuddelen av den militära verksamhet sker. Informationsarenan är ett abstrakt begrepp som motsvarar den sfär där information skapas, behandlas, lagras och förmedlas. Det är från denna arena som information vidarebefordras till olika användare och här kommuniceras även ledning och kontroll. Informationsarenan utgör i detta avseende ett eget stridsrum men är också en förutsättning för verkan inom den fysiska arenan.

I det mänskliga kognitionsområdet behandlas information till kunskap och förståelse. Allt innehåll i den kognitiva arenan passerar ett filter som kallas mänsklig varseblivning. Då filtret är uppbyggt av individens världsåskådning, personliga kunskaper och färdigheter, erfarenhet och andra individuella egenskaper är den mänskliga kognitionen unik för varje individ.



Figur 5. Illustration av vilka arenor som verkansförmågorna avser ge effekt inom, samt kopplingen mellan de olika arenorna.

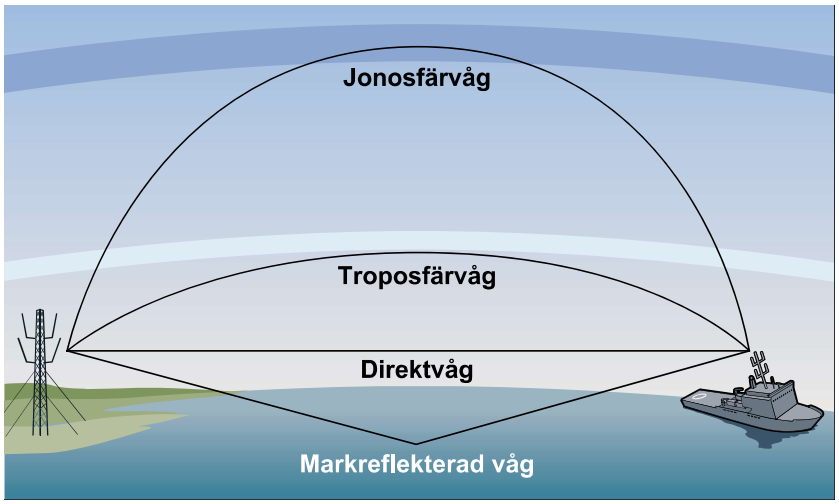
Ett sätt att illustrera kopplingen mellan de olika arenorna, samt indikera på vilken arena som de olika verkansförmågorna ger verkan, visas i figur 5.

I informationsoperationer har telekrig således en självklar funktion att fylla. Det är därför viktigt att utveckla förmågor och kompetenser inom telekrig för att Försvarsmakten i framtiden skall kunna möta och hantera nya hotbilder både i Sverige och vid internationella insatser.

Elektromagnetisk vågutbredning

Elektromagnetiska vågors utbredningsförhållanden har avgörande betydelse för funktionen hos många system. En utveckling mot bättre prestanda och ökad komplexitet i moderna system gör att den elektromagnetiska vågutbredningen blir en begränsande faktor i större utsträckning än tidigare. God kännedom om egenskaperna för vågutbredning och störbakgrunden fordras för att man skall kunna göra en realistisk bedömning av systemfunktionen i verklig miljö. Utbredningsmediet är generellt svårt att modellera och beskriva, vilket inbjuder till enkla genvägar som kan resultera i orealistisk uppskattning av systemprestanda, ibland som rena glädjesiffror eller i form av undervärderade systemegenskaper. Utbredningsmediet är och kommer att vara den gränssättande faktorn i dagens och morgondagens radio-, radar- och elektrooptiska system.

Utbredning av radiovågor



Figur 6. Strålgång i troposfär och jonosfär. Observera att jonosfärvåg och troposfärvåg ej uppträder samtidigt.

Reflektion, spridning, transmission och diffraktion är de grundläggande utbredningsmekanismerna, vars betydelse beror på topografi, markbeklädnad och atmosfär (inklusive brus). De ger alla upphov till fenomen som påverkar systemprestanda.

En radiovåg som utbreder sig från en sändare kan nå en mottagare via flera olika utbredningsvägar. Nära jordytan kan man urskilja en direktvåg, en markreflekterad våg samt en ytvåg. Direktvågen och den markreflekterade vågen sammansätter sig till atmosfärvågen. Ytvågen kan bara existera tätt utmed marken och är av betydelse bara 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 ca 10 km höjd, och jonosfären, som sträcker sig från ca 40 km till ca 1000 km höjd. Troposfärskikten uppkommer genom att vertikala temperatur- och fuktighetsförändringar ger variationer i luftens brytningsindex. Dessa påverkar atmosfärvågen från ca 30 MHz och uppåt i frekvens. Den reflekterade vågen från dessa skikt benämns troposfärvåg. De jonosfärskikt som uppkommer genom joniserande strålning från solen reflekterar vågor främst med frekvenser från 30 MHz och nedåt. Den reflekterade vågen kallas jonosfärvåg.

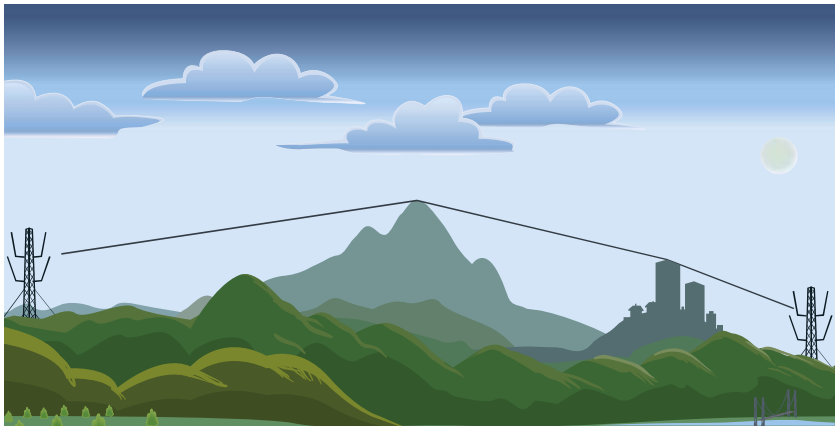
Markens inverkan

När en radiovåg träffar en yta reflekteras den, dels genom spridning och dels genom spegelreflektion. Reflektionskomponenten

motsvarar den spegelreflektion som ytan skulle ge om den vore fullständigt jämn, dock med amplituden reducerad med hänsyn till ytans ojämnheter. Vid reflektion gäller det bekanta spegelvillkoret, d.v.s. den reflekterade vågens vinkel mot ytan är lika stor som den infallande vågens. När ytan är ojämn sprids vågen i olika riktningar och man får flera lober som bestäms av ytans struktur och den infallande vågens riktning.

Vågutbredning i skuggzonen bakom till exempel byggnader och berg sker genom att radiovågorna diffrakteras (böjs av) kring det skuggande hindret. Detta får till följd att kommunikation även vid höga frekvenser kan upprätthållas bakom hinder, se figur 7.

Skog och annan vegetation påverkar vågutbredningen i hög grad. Inverkan sker i form av ren dämpning men även genom polarisationsvridning och uppkomst av flervägsutbredning (d.v.s. vågen utbreder sig samtidigt utmed flera utbredningsvägar). Effekten på utbredningsdämpningen vid olika frekvenser i kuperad terräng visas i figur 8.

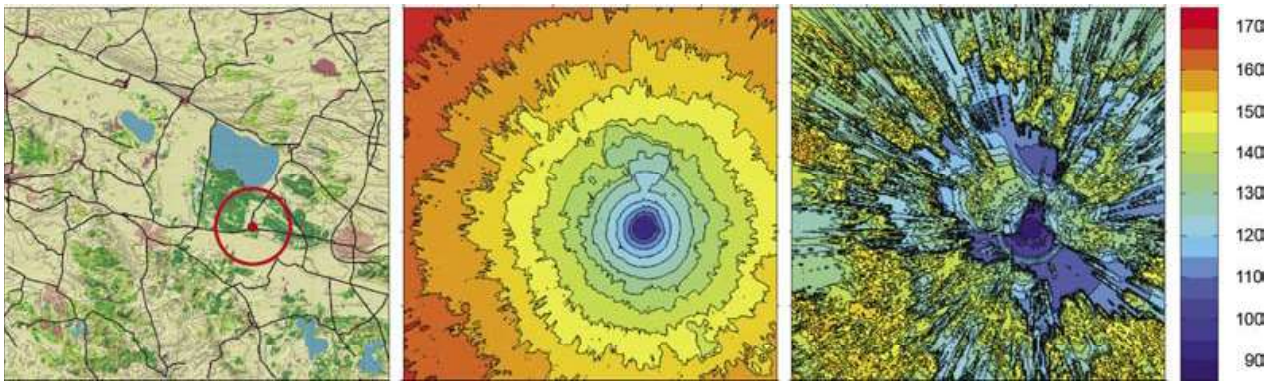


Figur 7. Diffraktion över terränghinder och byggnader.

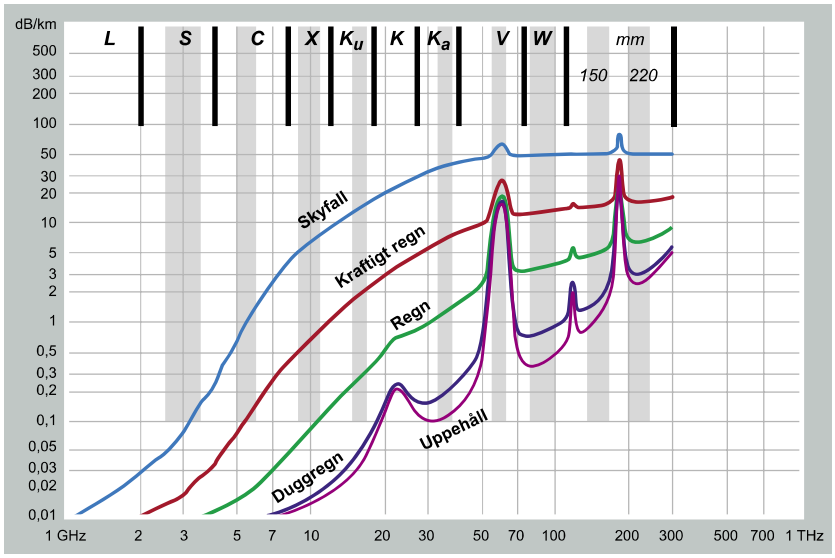
I kuperad terräng påverkas utbredningen av reflekterande ytor i form av större stenblock, bergssidor, kullar, åsar, raviner och liknande. I stadsmiljö finns det rikligt med reflekterande objekt, både stora och små. Det kan vara hus, broar, stolpar, elektriska ledare, fordon samt träd. Stora och jämna ytor ger upphov till distinkta och kraftiga flervägskomponenter av reflektionstyp medan mindre och ojämna ytor bidrar till en spridningssignal.

Vid förflyttning i rummet av sändare och/eller mottagare kommer signalstyrkan att variera. Man särskiljer två olika typer av rumsvariationer, fädning, dels en i rummet storskalig variation, dels en lokal variation. Den storskaliga fädningen bestäms huvudsakligen av terrängens utseende mellan sändare och mottagare.

Om stationerna är högt placerade, på kullar eller berg, reduceras transmissionsförlusten medan placering djupt nere i dalgångar ger förhöjd transmissionsförlust. Den lokala rumsvariationen ger upphov till transmissionsförlustvariationer med rumsliga max-till-max-avstånd av storleksordningen en halv våglängd. Orsaken till denna fädning är att radiovågen i verkligheten är sammansatt av en direktvåg och ett stort antal vågkomponenter (med olika amplitud och fas) som reflekteras från olika terrängföremål. Om någon eller flera av flervägskomponenterna färdas en



*Figur 8. Terrängens inverkan på mediets utbredningsdämpning vid 50 MHz (mitten) och 1800 MHz (höger) i ett 25*25 km terrängavsnitt på Revingehed. Sändaren är placerad vid den röda pricken på kartan. Sändarantennhöjderna motsvarar typiska höjder för en högantenn för Ra180 (50 MHz) och en mikrocell för GSM (1800 MHz).*



Figur 9. Specifik dämpning från gaser och nederbörd i området 1-300 GHz. Kurvan med minsta dämpning motsvarar uppehåll, därefter, med stigande dämpning, duggregn (ca 0,25 mm/h), regn (ca 4 mm/h), kraftigt regn (ca 25 mm/h) samt slutligen skyfall (ca 150 mm/h).

betydligt längre sträcka än direktvågen uppstår tidsdispersion (utspridning i tiden av mottagen signal), vilket i sin tur ger upphov till exempelvis frekvensselektiv fädning (radiokanalen påverkar signalens ingående frekvenskomponenter olika) och intersymbolinterferens (digitala symboler utsända vid olika tidpunkter kommer fram till mottagaren samtidigt och stör varandra). Båda fenomenen resulterar i problem för mottagaren att tolka signalen korrekt.

Troposfärens egenskaper

Troposfären inverkar som nämnts ovan på radiovågors utbredning från ca 30 MHz, med ökande inverkan uppåt i frekvens. Detta kan generellt ge stora ökningar av räckvidden i vissa höjdskikt, alternativt underräckvidder (betydligt kortare räckvidder), depolarisation och diverse spridningsfenomen. Effekten på sambands- och signalspaningssystem yttrar sig bland annat som interferenser och fädning. För radarsystem gäller bland annat att sannolikheten för upptäckt och falska ekon påverkas. Vidare uppstår diverse inmätningsfel där höjdmätningsfel dominerar.

Radiovågors utbredning i troposfären kan ske längs skikt som kallas ledskikt och vilka har stor betydelse för vågutbredningen. Den avgörande faktorn för uppkomst av ledskikt är luftens brytningsindex. Allmänt gäller att luftens brytningsindex avtar linjärt med höjden. Avvikelser från detta, anomalier, förekommer tämligen ofta inom vissa delar av den lägre troposfären, speciellt sommartid. Skikt med markant avvikelse är i regel relativt tunna, oftast 100 m eller mindre. För att ett ledskikt skall uppstå fordras att främst temperatur och fuktighet har sådan höjdvariation att brytningsindex avtar kraftigt med höjden. För detta krävs att temperaturen ökar och/eller fuktigheten avtar med höjden.

En temperaturinversion (kraftig temperaturökning med höjden inom ett begränsat höjdintervall, normalt avtar temperaturen med höjden) ger därför upphov till ledskikt.

En dominerande faktor vid ledskikt är luftfuktigheten. Den i dessa sammanhang helt dominerande inversionen är den som under en stor del av året förekommer över havsytan (havsinversion) och som kan ge upphov till så kallade avdunstningsskikt med höjder upp till några tiotal meter. Avdunstningsskiktet har i regel mycket homogen fördelning över stora havsytor, vilket är gynnsamt för ledskiktsutbredningen.

Den tredje huvudtypen av inversion som kan medföra ledskikt är strålningsinversionen. Denna uppstår endast över land under klara nätter, då utstrålningen medför kraftig avkylning av markytan. Strålningsinversionen förekommer i likhet med havsinversioner inom relativt tunna skikt närmast jordytan. På vissa av svenska marinens fartyg används mjukvaran LBM (Lokal BrytningsindexModell) för att utifrån uppmätta väderparametrar (ytvattnets temperatur, lufttemperatur, luftfuktighet samt vindhastighet) beräkna om ledskikt förekommer eller ej. Då ledskikt påverkar utbredningen för radar och radio (ger längre räckvidder) anpassas taktiken efter resultatet.

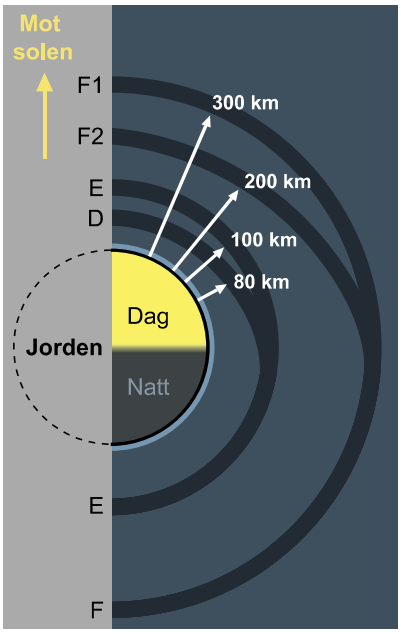
Gaser i atmosfären och olika former av nederbörd ger extra dämpning som i allmänhet ökar med ökande frekvens, se figur 9. Vid frekvenser under 10 GHz kan man dock i allmänhet försumma denna dämpning. Gasdämpning orsakas av syre- och vattenångeabsorption med kraftiga toppar vid t.ex. 22 respektive 60 GHz. Nederbördsdämpning ökar med ökande regnintensitet.

Jonosfärens inverkan

Radiovågor under en viss frekvens kan inte tränga igenom de joniserade skikt på höjder mellan 40 och 1000 km som utgör jonosfären. Den s.k. plasmafrekvensen är ett direkt mått på tätheten av fria elektroner i jonosfären. Dessa uppstår genom joniserande strålning från solen, men även genom partikelstrålning, den så kallade solvinden. Plasmafrekvensens maxvärde kallas kritiska frekvensen och ligger inom 3 – 30 MHz. Radiovågor på lägre frekvenser än denna är alltid instängda under jonosfären. Detta gör att man kan få radiovågen att utbreda sig bortom jordytans krökning genom reflektion och avböjning i jonosfärskikten.

Solens strålning varierar med årstid, tid på dygnet och solaktivitet, vilket resulterar i variationer i kritiska frekvensen. Med solaktivitet avses variationer i solens strålning. Denna variation är flera tiopotenser större för den joniserande strålningen än för strålningen inom det synliga bandet. Strålningen uppkommer i samband med eruptioner på solens yta, vilka förekommer i anslutning till mörka ytor på solen, solfläckarna. Solfläckstalet är ett mått på förekomsten av dessa fläckar på solen. Det har en periodisk variation med en cykel på ca 11 år.

Atmosfärens och solstrålningens sammansättning gör att jonosfären får en struktur som består av ett antal joniserade skikt med något olika egenskaper, se figur 10. D-skiktet (på ca 80 - 100 km höjd) svarar för de direkta förlusterna för radiovågen medan E-, F1- och F2-skikten (på ca 100 - 300 km höjd) ger den avböjning som möjliggör utbredning bortom horisonten. 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 ca 2000 km och motsvarande via F-skiktet ger

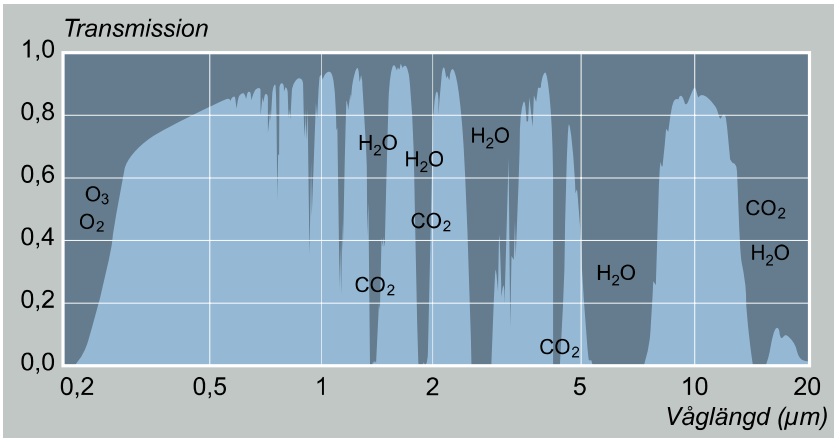


Figur 10. Jonosfärskikt.

ca 4000 km. Med flera reflektioner kan man få räckvidder som täcker hela jordytan. Vid större avvikelser från den normala jonosfären talar man om jonosfärstörningar. Dessa har sin uppkomst i händelser på solen, förknippas ofta med norrsken och kan exempelvis ge kraftigt ökad absorption som kan slå ut all HF-kommunikation. 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

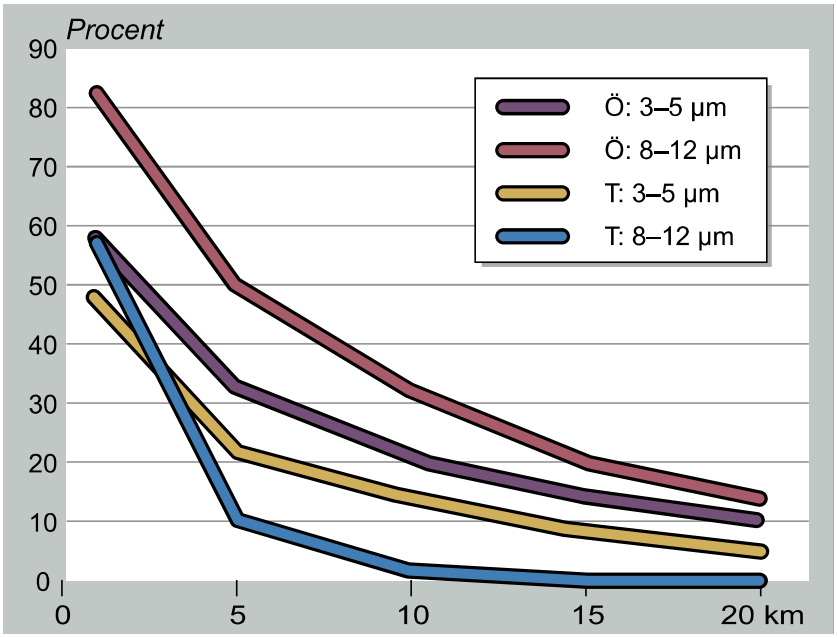
Optisk vågutbredning i atmosfären påverkas av en mängd fysikaliska processer, vilket innebär att räckvidd och prestanda för optiska system beror av atmosfärens tillstånd, d.v.s. av vädret, tidpunkten, det geografiska läget och höjden. Atmosfärens transmission är också i högsta grad våglängdsberoende, vilket framgår av figur 11. Vissa våglängdsband – s.k. fönster – har låg dämpning och utnyttjas för elektrooptiska system som skall verka i atmosfären.



Figur 11. 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.

I figur 11 syns längst till vänster UV-bandet som övergår i det visuella området (VIS) vid 0,4 µm och som i sin tur övergår i det nära infraröda (NIR) vid 0,7 µm. Därefter följer de tre IR-banden (2-3, 3-5 och 8-14 µm) och man kan se att de är tydligt avgränsade spektralt.

Våglängdsområdena 3 - 5 µm och 8 - 12 µm har delvis olika egenskaper, men framför allt stora likheter. De utnyttjas i mycket stor utsträckning för sikten, övervakning, m.m. Vid val av våglängdsområde bör hänsyn tas till geografisk plats och väder-situation. Anledningen är att vattenångedämpningen, som starkt begränsar transmissionen, är temperatur- fuktighets- och våglängdsberoende. För att illustrera detta visas i figur 12 transmissionen i två våglängdsband för Östersjön respektive tropiskt farvatten. Detta visar att ett elektrooptiskt system anskaffat för användning i Sverige kan vara direkt olämpligt att använda vid internationella insatser med annan atmosfär.



Figur 12. Transmission för Östersjön (Ö) och tropiskt farvatten (T) vid två för respektive farvatten typiska vädersituationer.

Man kan dela upp de olika fenomenen som påverkar prestanda hos elektrooptiska system i: absorption, spridning (och reflektion), emission, turbulens, brytning (refraktion) och polarisation. Dessa olika effekter behandlas nedan.

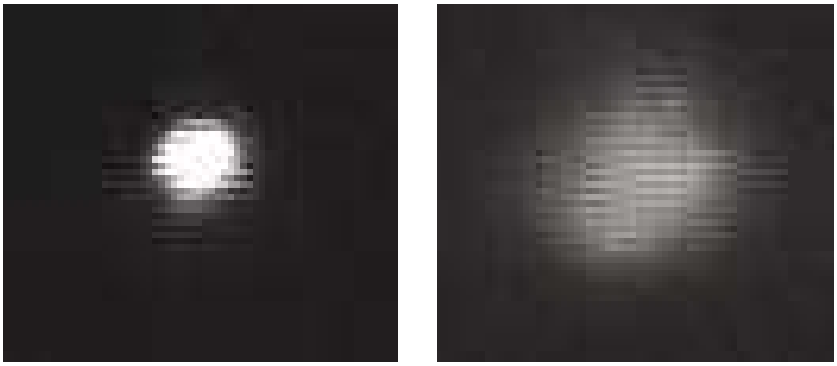
Atmosfären innehåller gaser och partiklar som dämpar den elektromagnetiska strålningen genom absorption och spridning, som inom optiken brukar sammanfattas i begreppet extinktion (utsläckning). Spridningsdelen kan delas in i molekylspridning (Rayleighspridning) och aerosolspridning. Aerosoler är partiklar som svävar i atmosfären och påverkar dämpningen inom hela spektrumet, men framför allt i UV-området (0,1 – 0,4 µm) och det visuella området (0,4 – 0,7 µm). Molekylspridningen kan oftast försummas, utom i UV-området. Absorp-

tionsdelen kan i sin tur delas in i linje- och kontinuumabsorption. 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.

Atmosfärsgaserna, 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 varierar starkt, speciellt vattenånga och ozon (O_3). Koncentrationen av koldioxid (CO_2) har en årstidsmässig variation och den långsiktiga trenden visar en ökande koncentration.

Den viktigaste absorbenten är vattenånga och det är också denna som har den största variationen bland atmosfärsgaserna. Vattenånga och koldioxid har kraftiga absorptionsband inom IR-området (0,7 – 14 µm). Inom IR-området bidrar även den s.k. kontinuumabsorptionen för bl.a. vattenånga till stor transmissionsnedsättning. Halten av ozon är mycket liten i atmosfären, men begränsar starkt transmissionen i UV-området. På hög höjd i atmosfären är ozonhalten högre och av stor betydelse då gasen hindrar solens skadliga UV-strålar att nå marken. Vid korta våglängder dämpas strålningen även av syre som begränsar transmissionen längst ner i UV-området. Generellt kan atmosfärsdämpningen sägas avta exponentiellt med avståndet.

En gas som absorberar starkt vid en viss våglängd, ger även stark utstrålning, emission, vid samma våglängd. Denna emission i atmosfärens gaser ger bakgrundsstrålning inom det optiska området. För att kunna detektera ett mål fordras en viss kontrast mot bakgrunden. Om denna har stark bakgrundsstrålning eller innehåller stor intensitetsvariation, försvåras måldetektionen. Så är fallet t.ex. vid sjöklotter, där rörelser i havsytan kan spegla in solen fläckvis.

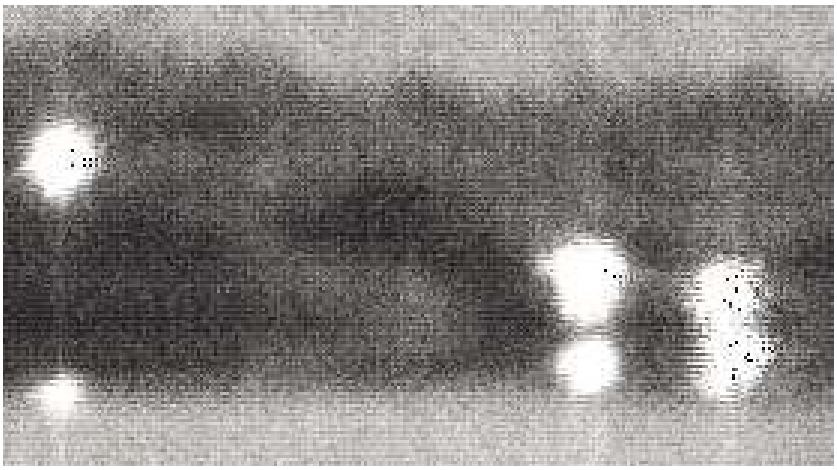


Figur 13. Avbildning av en punktkälla vid låg respektive hög turbulens.

Med turbulens menas luftrörelser som skapar en inhomogen struktur, med celler av olika storlek, där luften har olika brytningsegenskaper. Strålningen som passerar dessa celler kommer att påverkas både i riktning och intensitet. Turbulensen kan variera kraftigt med tiden. Turbulens ger bildskärpenedsättning i optiska system, vilket illustreras i figur 13. En turbulent atmosfär kan exempelvis ge scintillation där intensitetsfördelningen hos en laserstråle kan få ett fläckigt utseende och i bildgenererande system kan s.k. dansande bilder uppträda.

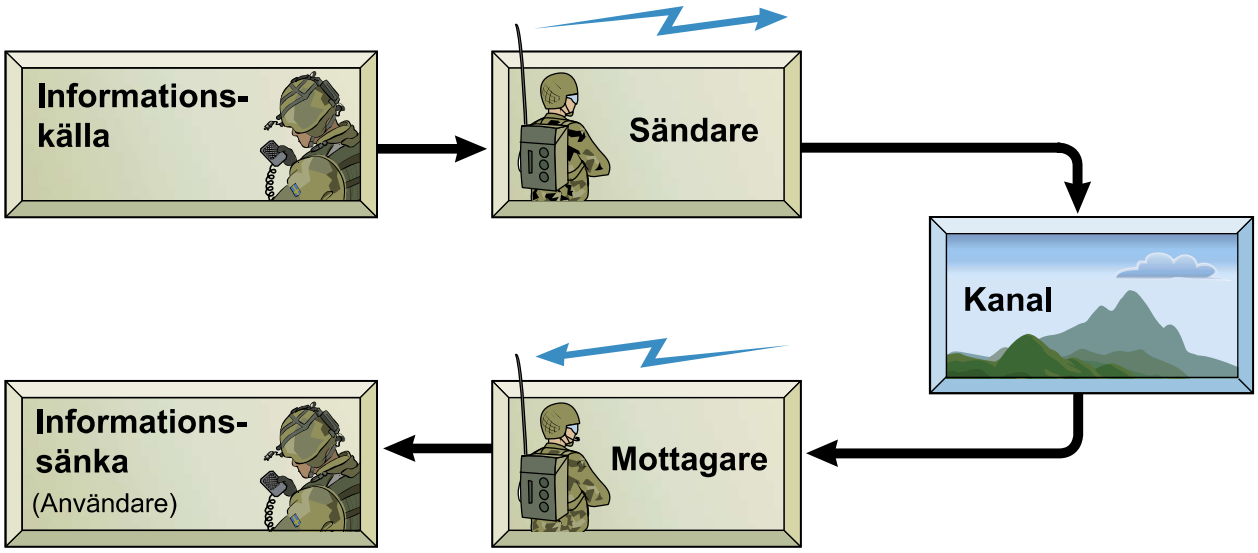
Brytning - eller refraktion - beror på att luftens brytningsindex varierar med höjden. I det optiska området är det framför allt temperaturen som spelar in. Temperaturen som funktion av höjden visar från tid till annan stora förändringar. Vid mirage (hägringsfenomen) uppträder extra mål som en spaningsutrustning felaktigt kan låsa på, se figur 14.

Polarisationen i atmosfären är särskilt tydlig i UV-området eftersom spridningen i molekyler blir polariserad. Spridning i cirrusmoln blir polariserad p.g.a. spridning i iskristaller.



Figur 14. Hägringseffekter över hav.

Radiokommunikationssystem



Figur 15. Generellt kommunikationssystem.

Ett generellt kommunikationssystem består av fem delar – informationskälla, sändare, kanal, mottagare och informationssänka (användare). Kommunikationssystemets uppgift är att överföra information från källan till användaren så felfritt som möjligt. Ett radiosystem karakteriseras av att informationsöverföringen sker med hjälp av elektromagnetiska vågor över kanalen.

Sändare

En elektromagnetisk våg kan karakteriseras med fyra parametrar – amplitud, frekvens, fas och polarisation. Om alla fyra parametrarna hålls konstanta kommer vågen att vara en ren oscillerande ton som kan representeras med en sinussignal. En icke-varierande ton innehåller ingen information men vågen kan moduleras genom att kontrollerat variera någon eller några av dessa parametrar (det är emellertid ovanligt att polarisationen varieras). Genom att göra detta kan information transporteras från ett ställe till ett annat. 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 modulationsprocessen ändras någon karakteristisk egenskap (amplitud, frekvens eller fas) hos den högfrekventa bärvågen proportionellt mot basbandssignalens momentana amplitud. Beroende på vilken egenskap som ändras kallas modulationsformerna för amplitudmodulation (AM), frekvensmodulation (FM) och fasmodulation (fasmodulation är ganska ovanlig som analog modulationsform).

Vid digital modulation är basbandssignalen digital, d.v.s. en ström av bitar där varje bit antingen är en 1:a eller 0:a. Flera bitar kan då bilda symboler, t.ex. kan en grupp om tre bitar bilda symboler som kan anta åtta olika värden (2^3 = 8). Symbolvärdet används för att bestämma någon av de karakteristiska egenskaperna för bärvågen.

Digitala sändare innehåller nästan alltid också källkodare och kanalkodare. Källkodning innebär att överflödig information plockas bort 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 varandra. Det tar då mindre plats att koda skillnaden mellan värdena istället för att koda varje bildelements värde för sig. Kanalkodarens uppgift är att tillföra extra information till signalen så att eventuella fel som uppstår i mottagaren p.g.a. att signalen har störts när den överfördes på kanalen, kan upptäckas och rättas. Enklaste formen av kanalkodning är att upprepa signalen tre gånger och låta mottagaren ta majoritetsbeslut på varje detekterad databit. Med hjälp av avancerad matematik kan bättre kanalkoder skapas.

Det finns ett flertal varianter, både för digitala och analoga grundmetoder, som inbegriper olika typer av filtrering och optimering av ytterligare egenskaper i signalens utformning. Ofta försöker man begränsa signalens utbredning i frekvens så att signalen inte i onödan skall störa andra signaler. Även kombinationer av grundmetoderna är vanliga och så länge det finns en entydig relation mellan den modulerande signalen och en viss kombination av amplitud, frekvens och fas som är tillräckligt skild från alla andra kombinationer kan signalen detekteras av mottagaren.

Antenn

Antennens uppgift är att anpassa den ledningsbundna energin som alstras av sändaren till icke ledningsbunden strålningsenergi (sändarantenn) alternativt att ta emot signalerna och överföra dem till en mottagare (mottagarantenn). Antennen kan således ha som uppgift att avge eller uppta energi.

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 radioenergin koncentreras i rummet. För fasta radiolänkar används dessutom ofta höga master placerade så att radiolänkkedjor bildas för att överbrygga stora avstånd bortom horisonten.

Figur F3. Rörlig radiolänkstation. Foto: Försvarets Bildbyrå/Michael Berggren.

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

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 enklast tänkbara antennen strålar lika mycket i alla riktningar, en så kallad isotrop antenn. En isotrop antenn är endast en hypotetisk punkt i rymden och går inte att realisera i verkligheten, men används som en matematisk referensantenn. Verkliga antenner omges inte av ett homogent strålningsfält utan uppvisar ett mer eller mindre utpräglat riktningsberoende. En verklig antenns förstärkning definieras som förhållandet mellan antennens effekttäthet i riktning med maximal strålning och effekttätheten hos en isotrop antenn. För normala antennkonstruktioner är det relativt enkelt att beräkna strålningsdiagrammet, men i verkligheten är en antenn alltid monterad på någon form av mekanisk struktur, vilket gör det svårt att beräkna hur antennen kommer att stråla för en given installation.

En tumregel för praktiska sändarantenner är att fysiska storleken av antennen bör vara av samma storleksordning som våglängden för bärvågen som antennen matas med. Detta för att så mycket som möjligt av den inmatade energin skall övergå i elektromagnetisk strålning.

Mottagare

I kanalen kommer signalen att utsättas för oförutsedda störningar vilka huvudsakligen karakteriseras av brus, fädning och interferenser. Brus kommer från atmosfären och

	Frekvens-område (MHz)	Band-spridning	Kanal-bandbredd	Högsta datatakt
Ra180 *(Truppradio)*	30–88	Frekvenshopp (FH)100 hopp/s	25 kHz	16 kbit/s
HF2000 *(Kortvåg)*	1,5–30	–	3 kHz	3,6 kbit/s
RL371 *(Radiolänk)*	1350–1850	FH, adaptiv	125 kHz	2048 kbit/s
Link 16 *(Taktisk länk)*	960–1215	FH, 77000 hopp/s Direktsekvens (DS)	3 MHz	115,2 kbit/s
2G *(GSM 900)*	D: 935–960 U: 890–915	–	200 kHz	14,4 kbit/s
3G *(WCDMA)*	D: 2110–2170 U: 1920–1980	DS	5 MHz	384 kbit/s
RAKEL *(Tetra)*	D: 390–400 U: 380–390	–	25 kHz	28,8 kbit/s
WLAN *(IEEE802.11)*	2400–2484	Orthogonal Frequency Division Multiplex (OFDM) (64)	20 MHz	54 Mbit/s
Bluetooth	2402–2480	FH	1 MHz	723,2 kbit/s
DAB	174–240	OFDM (1536)	1,536 MHz	1,7 Mbit/s
DRM	1,5–30	OFDM (228)	9 kHz	55 kbit/s

Tabell 1. Några systems egenskaper. Frekvenshopp och direktsekvens förklaras i avsnittet om elektronisk protektion. Orthogonal Frequency Division Multiplex (OFDM) är en modulationsteknik som upptar litet frekvensutrymme i förhållande till den datatakt som tekniken medger. OFDM innebär att informationsmängden som skall sändas delas upp i flera parallella dataströmmar, var och en med en lägre datatakt än den ursprungliga. Var och en av dataströmmarna moduleras sedan med någon av grundmetoderna (amplitud, frekvens och fas) på en egen bärvåg och alla bärvågor skickas sedan samtidigt över kanalen. Om vissa krav på separation mellan bärvågorna är uppfyllda blir den resulterande signalen speciellt tålig mot flervägsutbredning och fädning.

rymden in via mottagarantennen samt från de ingående komponenterna i mottagaren. Fädning är då signalens amplitud varierar över tiden, t.ex. på grund av att sändare eller mottagare rör på sig. Interferenser är andra signaler som kommer in via mottagarantennen, antingen avsiktliga eller oavsiktliga.

Mottagarens uppgift är att utföra de omvända operationerna mot sändaren. Mottagaren tar emot den analoga signalen som består av utsänd signal, brus och interferenser som dessutom kan fäda. Demodulatorns uppgift är att ur den sammansatta signalen bestämma vilken av alla möjliga signalalternativ som är den troligaste att sändaren sände och översätta det beslutet till information. Alla operationer som görs på sändarsidan är till för att öka sannolikheten att mottagaren tolkar den mottagna signalen rätt.

Systemexempel

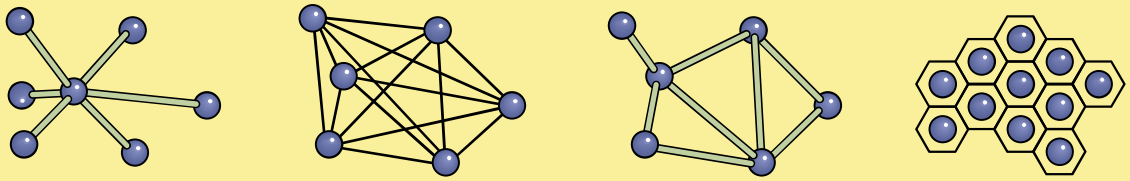
Tabell 1 visar några viktiga egenskaper för ett antal militära och civila kommunikationssystem.

Framtiden

Tekniktrenden inom militär radioutveckling går mot s.k. mjukvaruradio. Med hjälp av olika radiofunktioner i mjukvara kan radion anta olika profiler och kommunicera på olika sätt anpassat för skilda förutsättningar. En radios profil brukar ofta benämnas vågform. Utvecklingen går mot en radio som klarar av flera samtidiga vågformer. Detta skapar höga krav på bland annat processorkapaciteten. För att kunna implementera en sådan radio måste även hårdvaruarkitekturen vara flexibel. Samma hårdvara skall kunna återanvändas för olika kommunikationslösningar.

Radionät

Ett radionät är ett antal radionoder där varje nod oftast både kan sända och ta emot signaler. Nätets konfiguration är olika beroende på dess tillämpning. 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 helt centralstyrt, vilket gör det sårbart. Om den centralt styrande noden slås ut kommer nätet att sluta fungera.



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

En annan form av nätstruktur är ett broadcastnät där alla kan höra alla men bara en i taget kan sända. Detta är ett fullständigt förbundet nät och alla noder i nätet har en koppling till alla andra noder. Även detta nät är relativt enkelt att styra och inte heller lika sårbart som det centraliserade eftersom en centralt styrande nod saknas. Däremot kan det krävas hög uteffekt för att kunna nå en mottagare som befinner sig långt bort från sändaren.

Nät som bara är delvis förbundna men ändå kan förmedla trafik mellan godtyckliga noder kallas för flerhoppsnät. De tidigare nämnda näten är av typen enkelhopp, vilket betyder att kommunikationen sker direkt mellan sändare och mottagare. I ett flerhoppsnät kan noder som befinner sig utom räckhåll för varandra ändå kommunicera genom att informationen vidareförmedlas via mellanliggande noder. Den största nackdelen med ett flerhoppsnät är att styrningen av trafiken i nätet blir mer komplex.

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

För att mjukvaruradion skall vara realiserbar krävs standardisering, öppna arkitekturer och öppna väl definierade gränssnitt. Optimalt skall samma plattform kunna användas för samexistens mellan militära, civila och kommersiella kommnikationssystem. Detta innebär att befintliga radiosystem, det så kallade arvet, och nya radiosystem skall kunna samexistera på samma plattform. Detta kräver genomtänkta lösningar, men också att befintliga resurser utnyttjas mer kostnadseffektivt.

Mjukvaruradions utveckling är avgörande för interoperabiliteten, exempelvis för internationell samverkan och i fredsfrämjande insatser. I sådana sammanhang finns behov av att kunna kommunicera med lokala myndigheter och civila organisationer via offentliga kommunikationsnätverk och radiostandarder. Med en mjukvarudefinierad radio går det, ungefär som med en vanlig dator, att ladda olika applikationer. Detta ger en flexibel och säker radiolösning som är väl anpassad för försvarets framtida kommunikationsbehov.

Elektronisk protektion

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

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

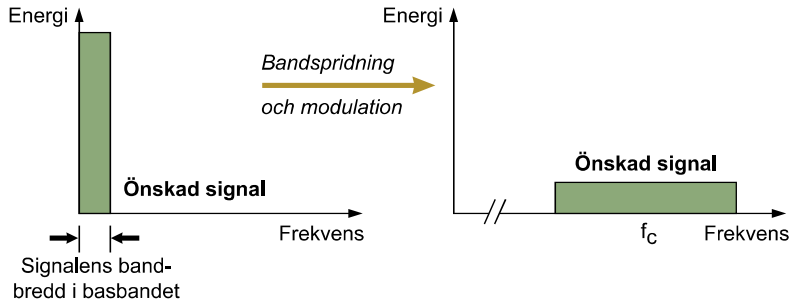
Frekvenshopp

Frekvenshopp (Frequency Hopping, FH), innebär som namnet antyder att bärvågsfrekvensen hela tiden byts (hoppar) på ett slumpartat sätt. Om frekvensbytena sker tillräckligt fort och systemet hoppar över tillräckligt stort frekvensband kan ett ganska gott skydd mot alla typer av störare erhållas. Med fort menas att hoppen måste ske ungefär lika snabbt som tiden det tar för signalen att gå mellan sändare och mottagare, för att förhindra s.k. följestörning där störaren först måste hitta aktuell frekvens för att 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.

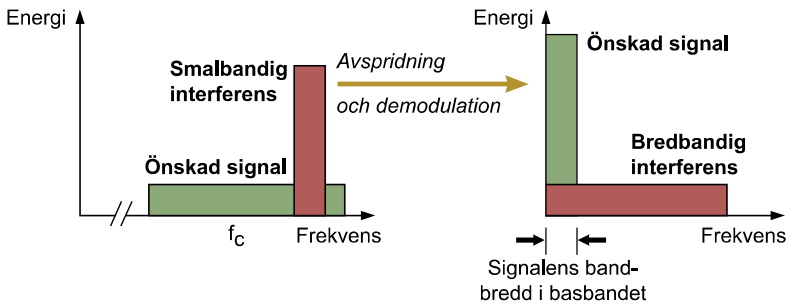
Direktsekvens

Direktsekvens (Direct Sequence, DS), innebär att en högfrekvent kod används för att sprida ursprungssignalens effektinnehåll över ett bredare frekvensområde än ursprungssignalens bandbredd. Vid mottagaren ”avsprids” sedan signalen och ursprungssignalen återfås medan alla andra (störande) signaler sprids. Genom att välja rätt spridningskod blir den utsända signalen bruslik med låg effekttäthet. Effekttätheten kan bli så låg att signalen döljs i det naturliga bruset, vilket minskar sannolikheten för att signalen skall upptäckas. Figur 16 och17 förklarar principen för direktsekvens.

I civila mobiltelefonsystem 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 DS-kod. Mottagare som känner till en viss sändares unika kod kan särskilja denna från de övriga sändarna, vilka upplevs som brus.



Figur 16. 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 17. 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.

Smygradio

Med smygradio menas att kommunikationen är svår att upptäcka. En metod för att åstadkomma detta är att gömma sig i bruset m.h.a. stor bandspridning med direktsekvens, tillsammans med riktantenner och effektkontroll. Riktantennerna används för att endast stråla i den riktning där mottagaren finns och effektkontroll används för att inte utstråla mer effekt än vad som precis behövs för kommunikationen. En annan metod går ut på att härma redan existerande signaler.

Ett alternativ till direktspridning är Ultra Wide-Band (UWB), även benämnd impulsradio, eftersom sändningen sker med extremt korta radiopulser. Typiskt är en pulslängd mellan 0,1 och 10 ns. Impulsradioteknik är tålig mot smalbandiga interferenser och flervägsutbredning och lämpad för korthållskommunikation, beroende på låga uteffekter, korta räckvidder samt hög spridningsvinst. UWB-teknikens fördelar är bl.a. höga datatakter, små användarterminaler och 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 använder samma frekvensspektrum som existerande teknik, vilket är möjligt eftersom signaleffekten sprids ut över ett stort frekvensområde. Eftersom UWB sänder med låg uteffekt över ett stort frekvensspektrum fås en låg effekttäthet och andra samexisterande radiosystem kommer att uppfatta UWB-signalen som brus.

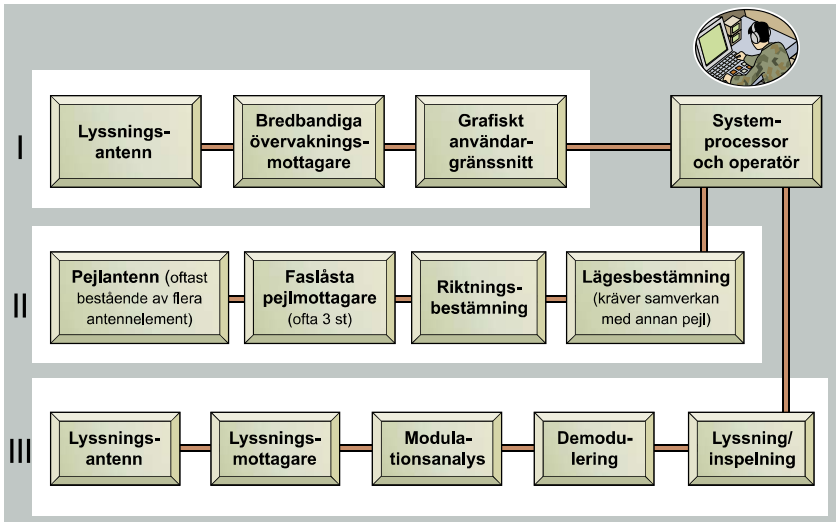
I vissa frekvensområden dämpas radiosignaler extra mycket med avståndet, vilket möjliggör smygkommunikation. Detta beror på att signalen är i resonans med molekyler i luften, varvid energin i radiosignalen mycket snabbt absorberas. Radiokommunikation på 60 GHz lämpar sig t.ex. väl för smygradio eftersom radioenergin här absorberas av syremolekyler i luften. Kommunikation som utnyttjar 60 GHz-området har kort räckvidd (ca 100 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 dess risk för upptäckt. Även en avsiktlig störare tvingas närmare sändaren eftersom denna oftast stör med samma frekvens och har samma korta räckvidd.

Elektronisk stödverksamhet

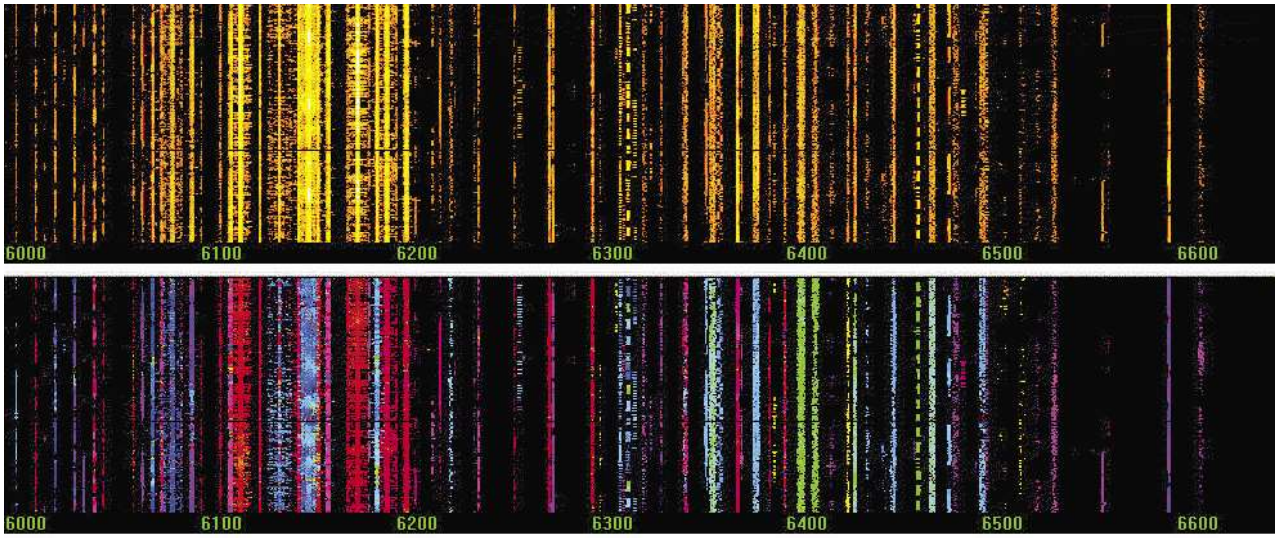
Uppbyggnad av ett radiosignalspaningssystem

Ett signalspaningssystem består av flera samverkande delar. I figur 18 visas ett principiellt blockschema över ett signalspaningssystem med bredbandig övervakningsfunktion, smalbandig signalanalys och pejlfunktion.

För att finna vilka signaler som är intressanta att spana på har operatören bredbandiga digitaliserande mottagare med ett grafiskt användargränssnitt som presenterar samtliga radiosignaler i de övervakade frekvensbanden (block I i



Figur 18. Principschema över ett signalspaningssystem. De tre blocken har olika uppgifter. Dessa är, uppifrån och ner: I. Övervakning runtom; II. Lägesbestämning; III. Signalanalys.



Figur 19. Presentation av radiosignaler inom ca 600 kHz av kortvågsbandet, med centrumfrekvensen 6325 kHz. I den övre delbilden färgkodas signalerna med avseende på amplitud så att en starkare signal framträder med ljusare färg. I den undre delbilden visar färgen respektive signals infallsriktning, (N-gul, Ö-röd, S-blå, V-grön).

figur 18). Det är dock även möjligt att utnyttja smalbandiga mottagare med t.ex. channel scan. För smalbandig signalanalys, lyssning och inspelning har systemet smalbandiga mottagare och hjälpmedel, t.ex. i form av automatisk modulationsklassificering (block III i figur 18). För riktnings- och lägesbestämning finns dessutom ett antal faslåsta pejlmottagare och en pejlantenn (block II i figur 18).

Det blir allt vanligare att övervakning och pejling integreras så att pejlmottagarna även uppfyller övervakningsuppgiften. Detta kräver att pejlmottagarna är bredbandiga och snabbt kan svepa över den övervakade bandbredden. Det grafiska användargränssnittet kan i det här fallet inte bara presentera vilka signaler som finns i bandet utan även vilka riktningar som de olika signalerna infaller ifrån, se figur 19.

En ensam pejlenhet har mycket sällan möjlighet till lokalisering av en sändare eftersom det endast i undantagsfall går att uppskatta avståndet till en sändare. Därför är samverkan med andra pejlenheter av största vikt vid lägesbestämning. Inom ett mobilt, taktiskt signalspaningssystem upprättas sambandet oftast med hjälp av radiolänk. Oavsett hur kommunikationen realiseras utgör den en förutsättning för ett väl fungerande system.

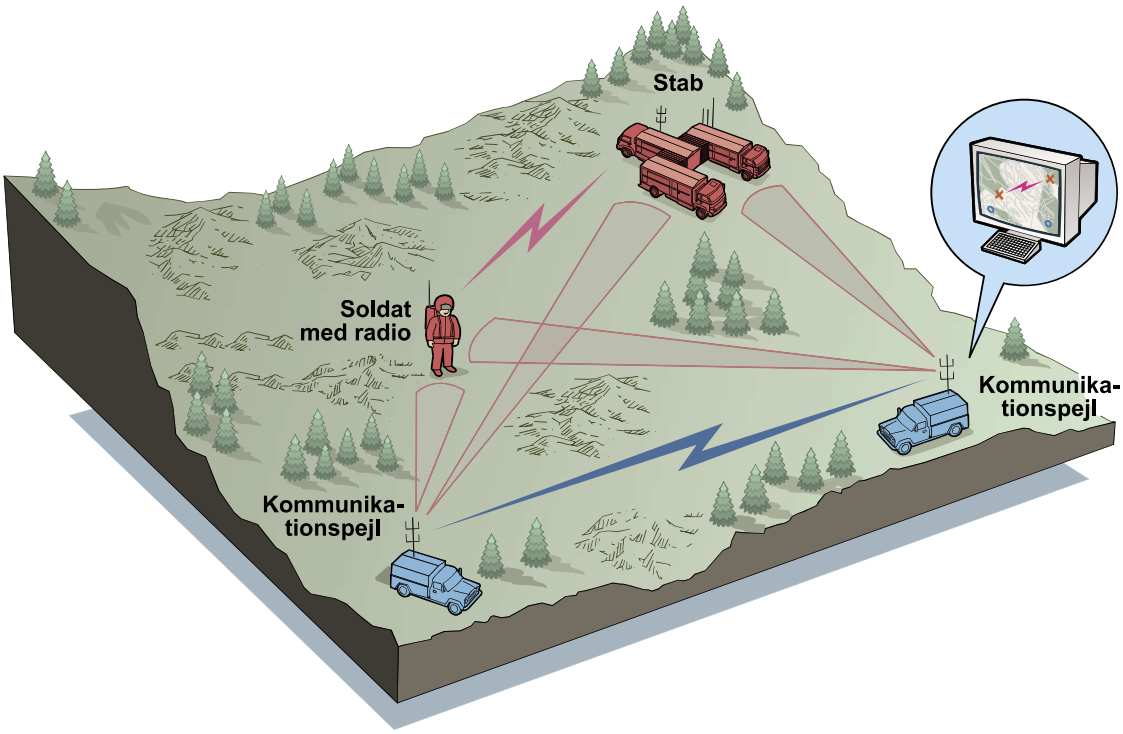
Syfte med taktisk signalspaning mot radiokommunikation

Radiokommunikation är ofta det mest praktiska sättet för rörliga militära förband att upprätthålla det nödvändiga sambandet för ordergivning och informationsflöde. För ett förband som önskar hålla sin kommunikation dold har radiokommunikation vissa oönskade egenskaper, exempelvis kan andra förutom den tänkta mottagaren ta emot radiosändningen och eventuellt utvinna den information som överförs. Den transmitterade elektromagnetiska vågens utbredningsriktning kan också bestämmas och källan kan därför lägesbestämmas, exempelvis genom krysspejling med hjälp av samverkande radiopejlar.

Taktisk signalspaning mot radiokommunikation syftar till att utnyttja motpartens emitterade radioenergi för att utvinna så mycket kunskap som möjligt. Även om kommunikationsinnehållet är krypterat så att informationen inte kan tas fram kan taktiskt viktiga slutsatser dras, se figur 20. Vanliga uppgifter för ett taktiskt signalspaningssystem är:

- Lägesbestämning av en radiosändare
- Typbestämning av en radiosändare,
- Knytning av radiosändare till plattform eller plattformstyp.
- Analys av motsidans kommunikationsstruktur
- Analys av informationsinnehållet i sändningen.

Ett exempel på ett signaleringsförfarande som inbjuder till analys av kommunikationsstrukturer (även kallat analys av radionät) är då



Figur 20. Lägesbestämning av motsidans radiokommunikation sker genom krysspejling 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.

ett fartyg sänder information till de övriga fartygen i samma grupp och dessa genom en kort sändning kvitterar det mottagna meddelandet. En taktisk signalspaningsenhet som uppfattar detta förfarande kan direkt se var fartygen befinner sig och hur många fartyg som finns i gruppen. Med hjälp av analys av vilken typ av sändning som används tillsammans med tidigare kunskap om sändarsystem på motsidans plattformar kan även sändningarna ge kunskap om vilket hot denna fartygsgrupp kan utgöra för egna enheter i närområdet.

Vid taktisk signalspaning mot radiokommunikation liknar arbetssättet det som används inom teknisk signalspaning (TES). Istället för att utvinna informationsinnehållet och därav dra slutsatser om motsidans avsikter tittar man på de tekniska parametrarna hos radiosändaren och försöker med hjälp av analys av radionät, förkunskaper om sändartyper på olika plattformar etc. bidra till den lägesbild som ligger till grund för taktiska beslut. Detta är till stor del en följd av den utbredda användningen av krypterade radiosändningar; tiden för dekryptering och informationsutvinning ur signalerna överstiger den tid inom vilken informationen är taktiskt användbar (från minuter upp till några timmar).

Den taktiska signalspaningens bidrag till den gemensamma lägesbilden kan vara var motståndaren har sina enheter, hur motståndarens enheter rört sig under viss tid eller om en enhet är central i motsidans sambandsnät.

Signalspaning mot kommunikation sker naturligtvis även under strategiska tidsperspektiv (dagar, veckor), där tiden medger djupare analys av de mottagna signalerna. I detta sammanhang talar man om kommunikationssignalspaning (KOS). Här kan ett större arbete läggas på exempelvis informationsutvinning, men även på det arbete som ligger till grund för det taktiska signalspaningsarbetet, exempelvis karakterisering av nya transmissionssystem samt analys av vilka plattformar sådana system är knutna till.

Spaningsräckvidder

Taktisk signalspaning mot kommunikation bedrivs huvudsakligen mot frekvensbanden HF (kortvåg), VHF (ultrakortvåg) och UHF, se figur 21.

Vid flygspaning från hög höjd kan stor spaningsräckvidd erhållas. Från 3000 meters höjd kan sändningar från ett fordon (antennhöjd ca 3 meter) uppfattas inom en radie på 250 km. Genom att mäta riktningen till sändaren i så-

väl horisontalplanet som i elevation kan ett signalspaningsflygplan lägesbestämma en markbaserad sändare utan samverkan med andra enheter.

Signalspaning från helikopter på 500 meters höjd har i motsvarande fall möjlighet att upptäcka en fordonsburen sändare inom en radie av cirka 100 km medan en markbunden signalspaningsenhet med pejlantennen i en 18-meters mast har ett spaningsavstånd på ca 30 km.

Beroende på jonosfärens inverkan ser vågutbredningen på HF-bandet väsentligt annorlunda ut än på de högre frekvenserna, se vågutbredningsavsnittet. Vid utbredning genom jonosfären bryts radiosignaler i den lägre delen av kortvågsbandet ner mot markytan igen, vilket 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 spaningsantenn från markhöjd. För radiosändningar från området nära mottagaren (ett antal 10-tals mil) får man vanligen inte tillbaka någon reflektion från jonosfären. Detta område ligger inom den så kallade skipzonen.

Målsignaler för radiosignalspaning

Fixfrekvenstrafik

De vanligast förekommande radiosignalerna utgörs fortfarande av smalbandiga fixfrekvenssändare. Hit kan all radiotrafik som sker med signalering på en fast frekvens räknas.

För signalspaning mot fixfrekvenssystem med långa sändningstider kan smalbandiga pejlar med hög känslighet användas. Genom att mottagarna är smalbandiga blir brusbandbredden liten vilket ger ett bättre signal/brusförhållande, varför inmätningen av riktningen till signalen kan göras mer noggrant.

Figur 21. De vanligaste målfrekvenserna för taktisk signalspaning ligger i frekvensbanden HF, VHF och UHF.

Ett specialfall av fixfrekvenssändare är s.k. snabbsändande radiosystem som bygger på att med en konventionell sändare framställa mycket korta signaler av storleksordningen 0,1 - 1 s. För att ett signalspaningssystem skall kunna hantera snabbsändande signaler effektivt krävs att bredbandiga mottagare används. Annars blir sannolikheten för att signalen skall uppträda inom spaningsbandbredden alltför liten.

Frekvenshoppande radiosändare

Frekvenshoppsteknik används för att försvåra störsändning och signalspaning. Signalen, som oftast är momentant smalbandig, byter centrumfrekvens hundratals, i vissa fall tusentals, gånger per sekund enligt ett i förväg bestämt mönster som är känt av mottagaren. Detta förfarande, liksom den kryptering som den överförda signalen oftast genomgått, minskar möjligheten för signalspanaren att komma åt signalinnehållet. Det är dock inte ett effektivt sätt att undgå lägesbestämning. Även snabba frekvenshoppare har ett begränsat antal kanaler där sändningen återkommer med till synes slumpmässiga intervall. Även en smalbandig pejl kan bevaka någon av de kanaler som används och samla på sig bäringsdata från de korta sändningar som faller inom kanalen. Då många samtidiga frekvenshoppande sändare vid olika tillfällen använder samma band är det av största vikt att de samverkande pejlarna är väl synkroniserade och att det förfarande som säkerställer att det verkligen är samma sändning som mätningen gjorts på fungerar. Denna kontroll kallas relativ identifiering. Ett för signalspanaren bättre sätt att lägesbestämma en frekvenshoppare är dock att pejla signalen på fler, helst alla, de använda kanalerna. Kan detta åstadkommas kommer bäringsfelet till sändaren att kunna reduceras genom medelvärdesbildning över de använda frekvenserna. För att kunna pejla signalen över ett stort antal frekvenser krävs ett bredbandigt pejlsystem eftersom signalspanaren inte på förhand känner till var i frekvens signalen kommer att dyka upp efter nästa frekvensbyte.

Direktsekvensspridda radiosändare

En av fördelarna med direktsekvensspridning är att den utsända signalens effekt är fördelad över en så stor bandbredd att effekttätheten i signalen blir låg jämfört med det omgivande bruset. 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. För att hantera den här typen av sändningar kan korrelationsteknik mellan två eller flera rumsligt separerade mottagare användas. Det brus som signalen gömmer sig i skiljer sig åt mellan

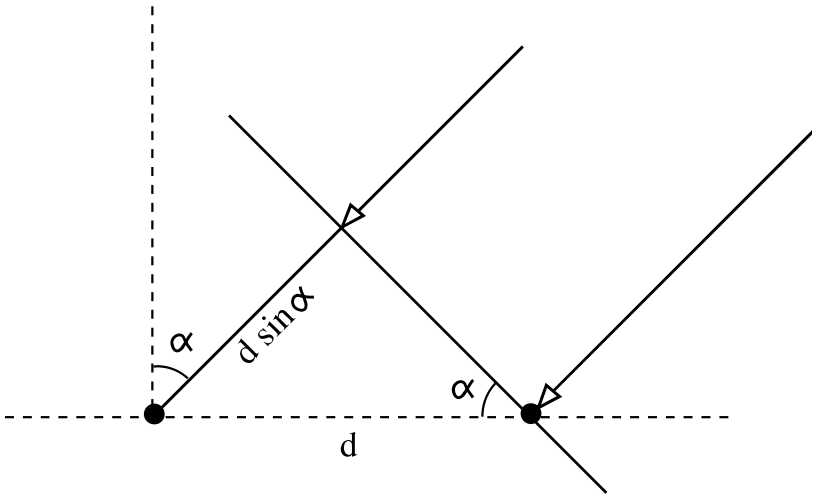
de båda mottagarplatserna och ger inget utslag vid korrelationen. En bredbandig bruslik signal som är likadan, fast med en viss tidsförskjutning, i de båda mottagarsystemen ger dock upphov till en kraftig korrelationstopp. På detta sätt kan tidsförskjutningen för de mottagna signalerna fastställas för de olika mottagarpositionerna, vilket i sin tur kan omvandlas till ett läge för sändaren.

Tekniker för riktnings- och lägesbestämning

Ett viktigt mål med taktisk signalspaning är, att hitta riktning till och läge för emittrar. Ett enkelt sätt, som numera inte är så vanligt, är att använda en riktantenn och vrida denna mekaniskt tills den mottagna signalen är som starkast. Med hjälp av en gradskiva och linjal kan sedan riktningen ritas in på en karta. Fås motsvarande information från en annan pejlstation kommer linjerna att skära varandra i en punkt som pekar ut den eftersökta sändaren. Genom att införa signalbehandling i systemet kan flera runtomstrålande antenner nyttjas för att få riktningen till målet, och genom ytterligare automatisering kan systemet presentera framtagna mållägen för operatören.

Riktningsbestämning

En enstaka riktantenn ger genom sin riktverkan en dålig momentan yttäckning, vilket gör att en kortvarig signal kan vara svår att upptäcka. Genom att använda sig av två i planet runtomstrålande antenner, till exempel vertikala dipolantenner, och placera dessa på ett lämpligt avstånd från varandra är det möjligt att mäta fasdifferensen mellan de mottagna signalerna och sedan bestämma



Figur 22. Skillnaden i gångväg som en plan infallande våg har till två antenner med avståndet d. Gångvägsskillnaden kan mätas som en tids- eller fasdifferens och utnyttjas till riktningsbestämning.

infallsriktningen för signalen, se figur 22. Kombineras två antennpar med 90° vridning dem emellan, kan riktningen bestämmas entydigt i ett plan.

Ett annat sätt att mäta infallsriktningen är att mäta fasskillnaden som fås när en signal tas emot av två antenner, s.k. interferometri. Denna metod ger riktningsfel som inte bara är beroende av avståndet mellan antennerna utan även av infallsriktningen. Dessutom kommer resultatet att bli mångtydigt om antennerna har ett inbördes avstånd som är längre än en halv våglängd.

Lägesbestämning

Krysspejling

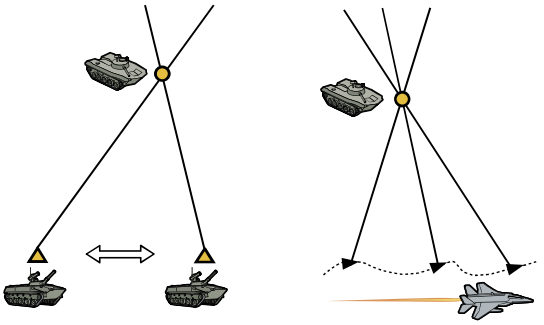
Det enklaste och mest självklara sättet att bestämma ett läge är att pejla riktningen till emittern från två olika punkter och se var linjerna som representerar riktningarna skär varandra. Metoden kallas för triangulering eller krysspejling, se den vänstra delen av figur 23. Felet i lägesskattningen varierar beroende på emitterns läge i förhållande till signalspaningsplattformarna. För att få en bra skattning av läget på långa avstånd bör pejlbasen, d.v.s. avståndet mellan signalspaningsplattformarna, vara så lång som möjligt. Med enkel geometri kan det konstateras att felen i inmätt emitterläge blir mycket stora nära pejlbasens förlängningar. De minsta lägesfelen fås när skärningen mellan de inmätta riktningarna är 90°.

Egentriangulering

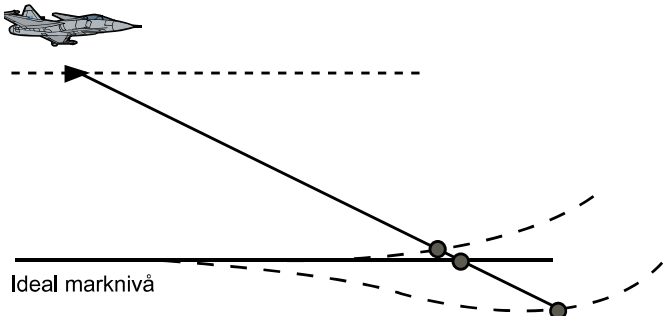
Det är möjligt att använda en ensam rörlig plattform för att bestämma en emitters läge. Förfarandet kallas för egentriangulering och bygger på att det är möjligt att genom egen rörelse skapa en mätbas, se den högra delen av figur 23. En förutsättning för detta är att signalkällan är stationär eller endast rör sig långsamt och att den sänder under en tillräckligt lång tid, eller att den är återkommande.

Vertikal triangulering

Genom att från en flygande plattform mäta både azimut och elevationsvinkel är det möjligt att med kännedom om flyghöjden bestämma var emittern befinner sig, se figur 24. Denna metod har vissa svagheter då marknivån inte är plan.



Figur 23. Två sätt att triangulera. Till vänster sker trianguleringen med två samverkande inmätare. Till höger sker en egentriangulering, där en inmätare genom att förflytta sig mellan mätningarna av infallsvinkeln kan bestämma läget för en fast emitter.



Figur 24. Vid vertikal triangulering kan markens variationer i nivå vara ett problem. I figuren ger de båda alternativa nivåerna (streckade) helt andra resultat än den idealt plana. Detta kan lösas med hjälp av höjddatabaser.

Precisionsmetoder för lägesbestämning

I många fall önskas en bättre lägesbestämning än vad som är möjligt med triangulering. 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 (Långbasinterferometri, Long Baseline Interferometry).

TDOA (Time Difference of Arrival)
TDOA eller tidsdifferensmätningar bygger på att mäta skillnaden i ankomsttid för en signal mottagen av två eller fler i rummet skilda mottagarstationer. Varje par av stationer ger en tidsdifferens, vilken i sin tur med lite geometriska beräkningar resulterar i en hyperbelgren på vilken emittern kan befinna sig. Dessa hyperbelgrenar kommer att skära varandra i den punkt som emittern befinner sig i, men i många fall även i någon punkt som ger ett falskt emitterläge. Problematiken med ett falskt läge kan lösas med en extra inhämtningsenhet.

DDOA (Doppler Difference of Arrival)
DDOA bygger som namnet anger på de frekvensförändringar som uppkommer när det finns en relativ rörelse mellan emitter och signalspaningsplattform. En dopplerdifferens mätt mellan två punkter resulterar i en isodopplerskillnadslinje. Denna beskriver alla punkter som kan ge upphov till den mätta dopplerskillnaden. 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)
Långbasinterferometri är en metod som bygger på mätning av fasskillnaden mellan två mottagarkanaler, men till skillnad från vid 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 interferometern blir mångtydig, d.v.s. flera infallsriktningar ger samma mätta fasdifferens. Genom att mäta fasdifferensen med täta intervall samtidigt som signalspaningsplattformen rör sig kan en historik över fasdifferenserna skapas. Ur historiken kan de fassprång, där fasläget byter från -180° till +180° eller vice versa, hittas. Genom att kompensera för fassprången kan fasens förändring beräknas, och ur denna kan slutligen ett läge bestämmas.

Elektronisk attack

Det går aldrig att helt förhindra kommunikation, men det går att försvåra och fördröja den så mycket att den saknar relevans när den kommer fram. För att lyckas i detta uppsåt måste störaren klara av tre uppgifter – upptäcka signalerna, generera en effektiv störsignal och använda denna på ett bra sätt.

För att en signal skall kunna störas måste den först upptäckas av störsändaren eller taktisk signalspaning. Om det ej går att påvisa signalering på en viss frekvens eller förekomsten av kommunikation på en utpekad plats, finns det ingen anledning att försöka störa. Detta är en av grundtankarna i smygradiokoncepten. Här försöker kommunikatörerna med olika modulations- och kodningstekniker hålla nere signaleffekten per frekvensenhet så att den taktiska signalspaningen inte får tillräckligt med energi för att detektera förekomsten av signalering.

När signalering påvisas eller antas pågå måste störsändaren generera en störsignal som är tillräcklig för att kunna slå ut informationen i mottagaren. Med andra ord måste målet vara inom störsändarens räckviddsområde. En störsändares räckvidd är inget absolut begrepp. Det är hela tiden frågan om ett styrkeförhållande mellan trafiksignalen och störsändaren. Detta brukar betecknas med RSR (relativ störräckvidd) och definieras som kvoten mellan störavstånd och trafikavstånd då förbindelsen precis blir utstörd. En störsändare minskar således endast radiostationernas förbindelseavstånd, men ambitionen är att minska det så mycket att radiokommunikationen blir taktiskt oanvändbar.

Det räcker dock inte att producera tillräckligt mycket och tillräckligt bra störeffekt i målet. Störningen måste även presenteras på rätt frekvens och vid rätt tidpunkt. Detta kan sammanfatta hela telekrigsproblematiken.

Störning av fixfrekvenssamband

För att vara effektiv måste störsändaren sända på rätt frekvens vid rätt tidpunkt och vara så nära mottagaren att störsignalen tränger undan trafiksignalen. Hur mycket störeffekt som behövs för att ”tränga undan” trafiksignalen är beroende av hur trafiksignalen är modulerad. Olika modulationssätt är olika svåra att störa. Medan det ibland kan vara tillräckligt att ha den starkaste signalen för att helt omöjliggöra kommunikation, kan i andra sammanhang (vid andra modulationssätt) båda signalerna uppfattas samtidigt inom ett visst nivåområde. För att helt dölja trafiksignalen måste störsignalen i detta fall vara mycket starkare.

Det är naturligt att välja olika moduleringsform vid kommersiella civila applikationer och militära kommunikationer. I det förra fallet är en ren fin signal att lyssna på det viktiga, medan det vid militära applikationer inte är ljudkvaliteten i sig utan istället förmågan till informationsöverföring även i svår miljö som efterfrågas.

Ju mer av signalen som är ”informationsbärande”, desto svårare är det principellt för störsändaren att blockera den. Detta pekar på att telegrafi är ännu svårare att störa och duktiga telegrafister är näst intill omöjliga att störa ut.

På samma sätt som en viss störsignal påverkar olika trafikmodulationer på olika sätt påverkar även olika störmodulationer en given signal på olika sätt. Generellt gäller att ju mer störsignalen liknar trafiksignalen, desto bättre blir störverkan.

En störsignal som är alltför unik går att extrahera i mottagaren och återmata i motfas. Görs detta på rätt sätt kan störsignalen fås att radera sig själv. Förfarandet kallas för ”cancellering” och används även för att samtidigt kunna sända och ta emot med samlokaliserade radiostationer.

Störning kan ske som t.ex. brus, pulsstörning eller repetitionsstörning. I det senare fallet återutsänds trafiksignalen fast vid fel tidpunkt, vilket skapar förvirring hos mottagaren.

För att skydda sig mot störningen använder kommunikatören olika former av kodning. Denna kan upptäcka alternativt korrigera utstörd information. Ju mer störskydd som önskas desto kraftigare koder måste tillgripas. Detta betyder att en större och större del av den överförda bitströmmen upptas av kodning, vilket i sin tur betyder att informationsmängden per tidsenhet minskar eftersom den totalt tillgängliga bandbredden oftast är begränsad. Denna minskade informationsöverföringskapacitet är precis vad störaren är ute efter.

Genom att göra informationskanalerna så smala som möjligt

ökar sannolikheten för att de är blockerade när viktig information snabbt måste fram.

Det är således svårt att i förväg beräkna störverkan mot en digital förbindelse såvida den inte är känd i detalj. Även om utrustningen är kartlagd under fredliga förhållanden 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 ej. Ett alternativt sätt är att studera motsidans agerande. De reaktioner som kan förväntas är:

- frekvensbyte
- förändringar i sändareffekt eller sändningssätt
- signaleringen upphör eller repeteras
- minskade förbindelseavstånd
- byte av modulationssätt eller sambandsmedel
- taktiska eller koordineringsmässiga missar.

En viss risk finns alltid i 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 att störningen ej har någon verkan och hoppas på att störaren väljer ett annat mål istället. Vid störinsats bör störaren även betänka att ... *Varje störpass är en utbildning av motståndaren i att skydda sig mot störning.* Störning bör därför sättas in restriktivt och endast då den kan ha förväntad taktisk verkan.

Störning av frekvenshopp

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

Vid följestörning måste störaren hinna mäta in den använda kanalen och leverera en störsignal till radiomottagaren innan trafiksändaren har lyckats sända över tillräckligt mycket information på den nya kanalen. Om störaren lyckas eller ej beror på hopptakt, kodning, störarens snabbhet och de geografiska avstånden mellan trafiksändare, trafikmottagare och störsändare. En tumregel för yttäckande system, typ arméradio, är att en följestörare kan hänga med upp till hopptakter på 500 – 1000 hopp/sekund. Vid snabbare hopptakter måste störsändaren komma in i förbindelsestråket mellan trafiksändare och mottagare för att hinna följestöra.

Störning av direktsekvens

Den mest effektiva generella störmetoden mot direktsekvens är bärvågsstörning, eventuellt pulsad på lämpligt sätt. Denna kan dock enkelt filtreras bort i mottagaren varför en normal störare alltid breddar sin störsignal, t.ex. med brus.

Störsändningsprinciper

De störsändare som används 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 störmetoden 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”.

Observera att det fortfarande går att sända ut från en yta som är belagd med närstörning, eftersom det endast är mottagningen som är blockerad.

Figur F5. Närstörssändare Tarax. Foto: Försvarsmakten/Patrik Persson.

Figur F6. Fjärrstörsändare.

Figur F7. Detalj av antenn, fjärrstörsändare.

Laserkommunikationssystem

Optisk kommunikation med laser har studerats alltsedan lasern uppfanns runt 1960. Ett antal försök med fri optisk kommunikation genomfördes på 1960- och 1970-talen. I brist på komponenter gick dock intresset nästan helt över till fiberkommunikation i mitten av 1970-talet. Den senaste tiden har dock ny teknik och nya komponenter liksom ökade behov av bandbredd medfört att intresset för fri optisk kommunikation åter tagit fart. Tekniken möjliggör snabb kommunikation med smygegenskaper, inte bara mellan fasta plattformar utan även mellan rörliga sådana, t.ex. helikoptrar, UAVer och fartyg.

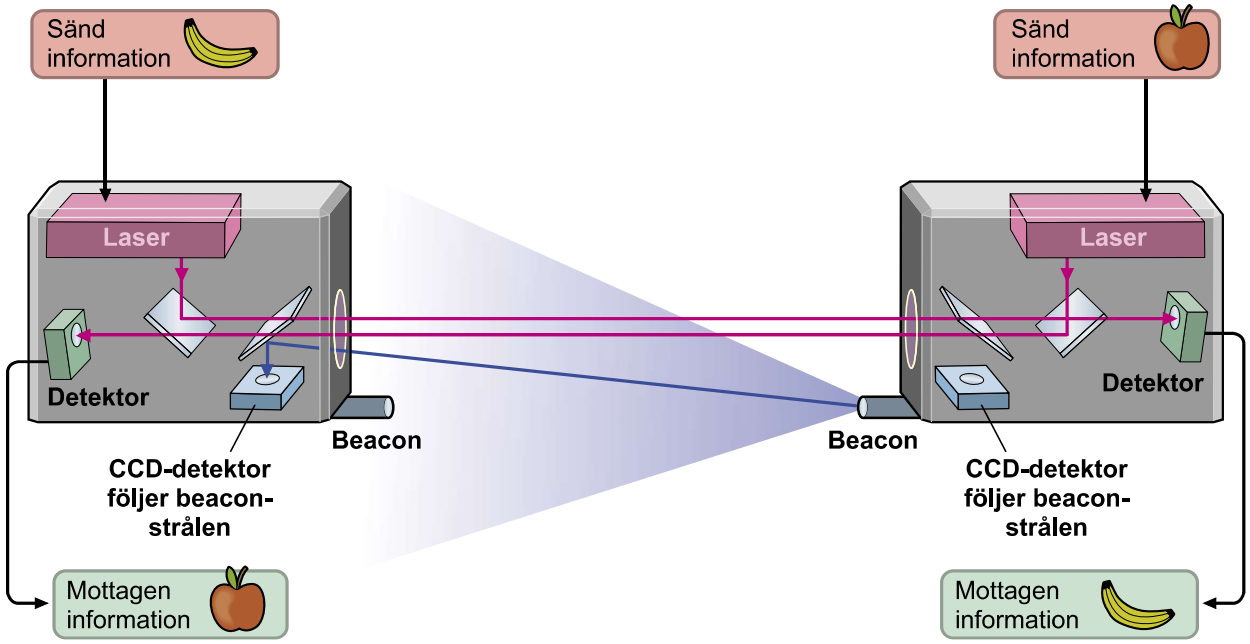
Några av fördelarna är:

- Hög överföringskapacitet. Potentiellt 10-tals Gbit/s.
- Smala sändar- och mottagar lober. Pejling, störning och avlyssning är ytterst svårt.
- Ingen frekvensplanering krävs.
- Kan i många fall kombineras med existerande laser- och optiksystem.

Fri optisk kommunikation kräver vanligtvis fri siktsträcka mellan sändare och mottagare.

Figur 25 visar hur en dubbelriktad länk för fri optisk kommunikation kan se ut. Båda sidorna är utrustade med sändar- och mottagarenhet. Full duplex, det vill säga samtidig kommunikation i båda riktningarna, kan erhållas med två närliggande våglängder. En separation i våglängd reducerar problem med överhörning mellan sändare och mottagare.

Informationen som skall sändas kodas och skickas sedan genom att modulera lasern. Normalt används så kallad On-Off-keying (OOK) som modulationsform, vilket innebär att lasern är på vid en logisk ”etta” och att lasern är av vid logisk ”nolla”. Lasersändaren riktas mot mottagarenheten. Samtidigt kan sändaren skicka en ”fyrsignal” (beacon) som detekteras av en detektor hos mottagaren och därmed möjliggör inriktning mot sän-



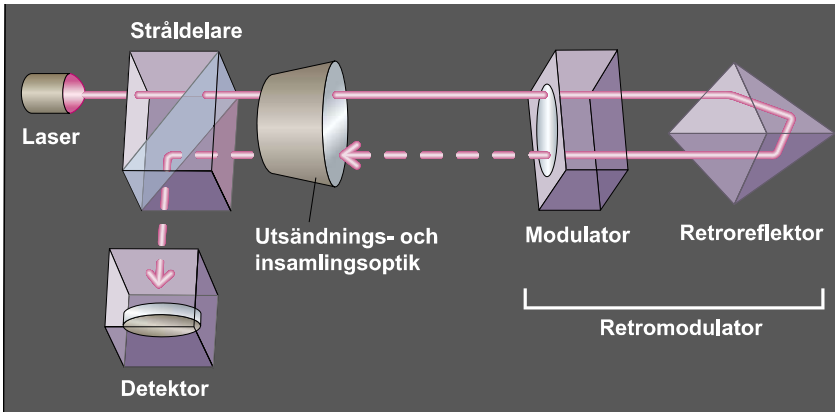
Figur 25. Länkprincip och ingående komponenter.

darenheten. För korta kommunikationsavstånd kan lobbredder på någon eller några grader tillåtas. För längre avstånd (km) krävs lobbredder i storleksordningen <1 mrad (1 mrad ≈ 0,06° ≈ 1 streck). Detta ställer höga krav på inriktning, stabilisering och följning.

Retrokommunikation

Retrokommunikation är en särskild typ av fri optisk kommunikation där lasern i länkens ena ände har ersatts med en så kallad retromodulator. Retromodulatorn innehåller två huvuddelar – retroreflektor och modulator. Retroreflektorn returnerar strålen tillbaka mot lasersändaren oavsett riktningen in mot den. En modulator av något slag sitter framför retroreflektorn. Denna tillför information till den tillbakareflekterade strålen. Vid lasersändaren detekteras sedan den modulerade strålen.

Optisk kommunikation med retroteknik har samma fördelar som annan optisk kommunikation när det gäller smygegenskaper och höga datatakter. Ytterligare fördelar är att retromodulatorn kan göras liten, lätt, effektsnål och stryktålig. Dessutom behövs ingen mekanism för att rikta in retromodulatorn, eftersom laserstrålen alltid returneras samma väg oberoende av från vilket håll den kommer in. Strålstyrning krävs därmed endast i den ena änden av länken. Varje retromodulator har ett visst synfält, inom vilket den kan arbeta, typiskt några tiotals grader beroende på typ och uppbyggnad. Genom att kombinera flera retromodulatorer är det möjligt att täcka ett större synfält.



Figur 26. Principen för retrokommunikation.

Retromodulatorns speciella egenskaper gör det möjligt att placera den på till exempel bojar, båtar, master, obemannade flygfarkoster, ballonger och enskilda personer (exempelvis på soldatens hjälm). Retromodulatorn kan vara användbar i tillämpningar där en laser med tillhörande strålstyrning inte kan monteras, t.ex. av utrymmesskäl eller på grund av svårigheter med effektförsörjningen.

Datatakten i en retrokommunikationslänk kan ökas ytterligare, t.ex. genom att använda flera laserstrålar och modulatorer, eller genom att samtidigt parallellt utnyttja flera våglängder. Kommunikation kan också ske i riktning mot retromodulatorn. Då krävs att laserstrålen moduleras redan när den lämnar lasern och att retromodulatorn kompletteras med en detektor.

Tillämpningar

Fri optisk kommunikation kan utnyttjas för kommunikation både mellan fasta och rörliga plattformar, exempelvis fordon, fartyg, ubåtar, helikoptrar, flygplan, UAVer och aerostater.

Kommunikation mellan fordon kan ske med låg röjningsrisk och höga datahastigheter. Överföring av bild- (TV/IRV) och varnarinformation från sensorer är möjlig. Kommunikationslänken kan också kombineras med exempelvis IK, laservarnare, laserradar och avståndsmätare. Problemet med fri

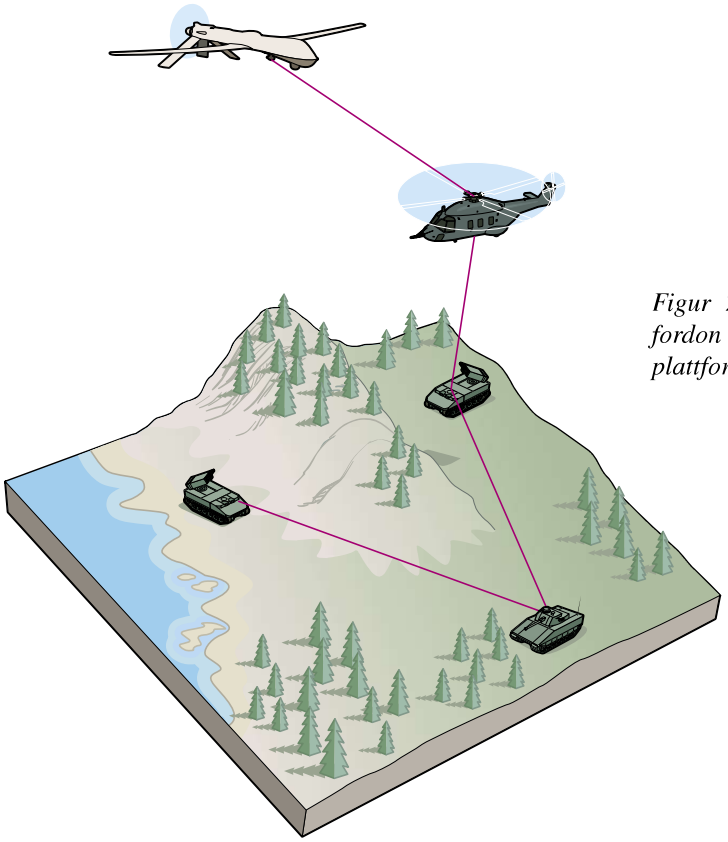
Modulatorer för retrokommunikation

Det finns olika typer av modulatorer som kan användas för retrokommunikation. En typ bygger på vätskekristallteknik. Laserstrålen moduleras genom att den passerar genom vätskekristallen och därmed påtvingas ett visst polarisationstillstånd. Fördelen med denna typ av modulator är främst att den går att tillverka till en låg kostnad. Begränsningen ligger främst i datatakten, som är några tiotal kbit/s.

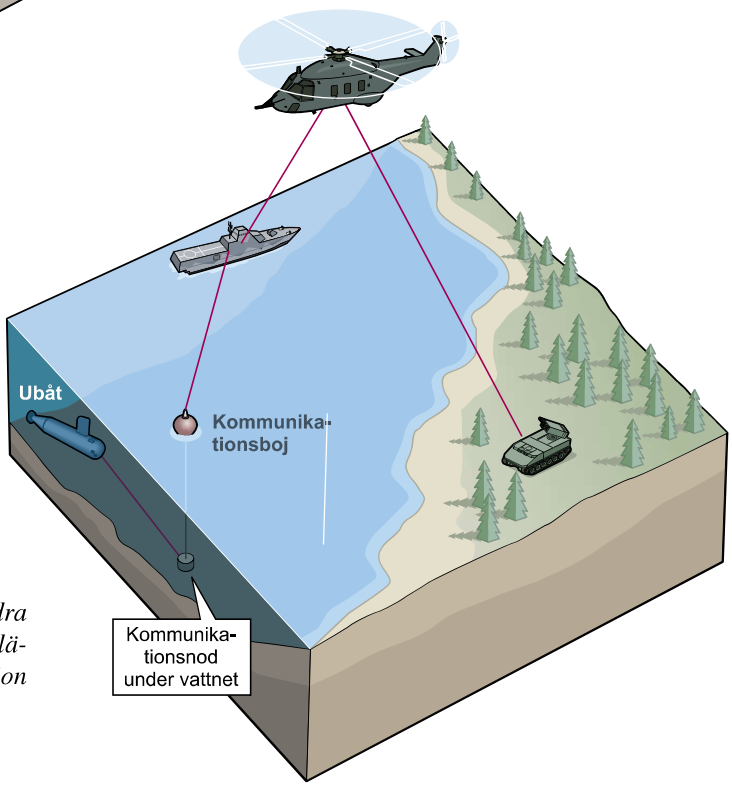
En annan typ av modulator, kvantbrunnsmodulatorn, är uppbyggd av tunna halvledarskikt och principen bygger på utnyttjande av den så kallade kvantbrunnseffekten. I detta fall är det laserstrålens intensitet som moduleras. Mycket stora datatakter kan uppnås, tiotals Mbit/s har visats och potential finns på upp mot 1 Gbit/s. Nackdelen med kvantbrunnsmodulatorn är främst att tillverkningen fortfarande är avancerad och kostsam.

sikt kan reduceras med relästationer och flygande plattformar såsom UAVer eller helikoptrar. Se figur 27. Det pågår även försök med indirekt kommunikation via atmosfärsspridning.

Vid fartygsoperationer är fullständig signaltystnad ofta av stor vikt då man inte vill röja sin position. Fri optisk kommunikation möjliggör röjningsfri kommunikation såväl mellan fartyg som från fartyg till helikopter eller land. Under gynnsamma väderförhållanden kan räckvidder på tiotals kilometer uppnås. För längre avstånd krävs någon form av relästationer. Fartygets optiska sensorer och dess gyrostabilisering kan med fördel användas i kombination med den optiska kommunikationslänken. Fartyg och flygfarkoster kan också tänkas utnyttja fri optisk kommunikation för kommunikation med bojar i vattenytan. Informationen från dessa bojar kan sedan vidareförmedlas till exempelvis ubåtar. Se figur 28.



Figur 27. Kommunikation mellan fordon med utnyttjande av flygande plattform som relästation.



Figur 28. Kommunikation mellan fartyg och andra plattformar. Genom utnyttjande av flygande relästation och kommunikationsboj kan kommunikation ske såväl med markförband som med ubåtar.

Elektronisk stödverksamhet

Laserkommunikationslänkar har normalt smala sändarlober, vilket medför att kommunikationen är svårupptäckt. Spridning i atmosfären kan eventuellt möjliggöra upptäckt även strax utanför sändarloben. Normalt krävs dock fri sikt till sändarenheten för att upptäckt skall vara möjlig, vilket innebär att enheten ändå kan upptäckas visuellt. I de fall ”fyrsignaler” (beacon) utnyttjas för fångning och följning kan kommunikationslänken lättare upptäckas då dessa sänder med bred laserlob och eventuellt sveper över stora vinkelområden. Det skall dock noteras att detta inte möjliggör avlyssning utan enbart upptäckt av länken.

Våglängder inom det visuella området skall självklart undvikas vid konstruktion av laserlänkar. Även våglängder som kan uppfattas av bildförstärkare eller CCD-kameror bör undvikas för att försvåra upptäckt. Våglängder vid 1,5 µm kan med fördel utnyttjas då det finns bra lasrar och detektorer för detta våglängdsband samtidigt som atmosfärstransmissionen är god. Ett framtida alternativ kan även vara att sända vid t.ex. 1,8 µm eller 2 µm.

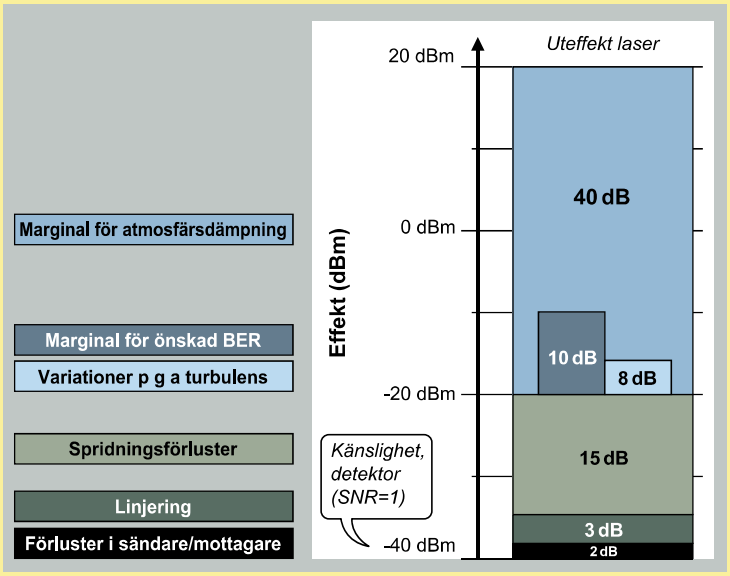
Det är också viktigt att utforma sändar- och mottagaroptik så att retroreflexer minimeras för att undvika upptäckt (undantaget länkar som utnyttjar retroteknik för kommunikation). Genom att utnyttja en optikspanare som får scanna över ett område kan annars positionen för sändaren och mottagaren avslöjas.

För att avlyssna en laserkommunikationslänk krävs avancerad utrustning som normalt måste placeras i eller strax utanför laserloben. Detta medför att den som försöker avlyssna länken sannolikt röjer sin egen position.

Om strålen är större än mottagaren kommer även en del av bakgrunden eller den kommunicerande enheten att belysas av lasern. Den lasereffekt som träffar enheten sprids ut diffust i alla riktningar. Rent teoretiskt skulle en riktigt känslig mottagare kunna riktas in från nära håll bredvid länkens mottagare och på så sätt avlyssna genom detektion av den diffust spridda strålningen. Avlyssnaren måste då veta positionen hos länken. Det är möjligt att avlyssning också kan ske snett bakom mottagaren om strålen är så bred att en del av den missar den kommunicerande enheten. Avlyssning kräver inte bara avancerad utrustning utan skulle också vara mycket svår att genomföra praktiskt.

Länkbudget för laserkommunikation

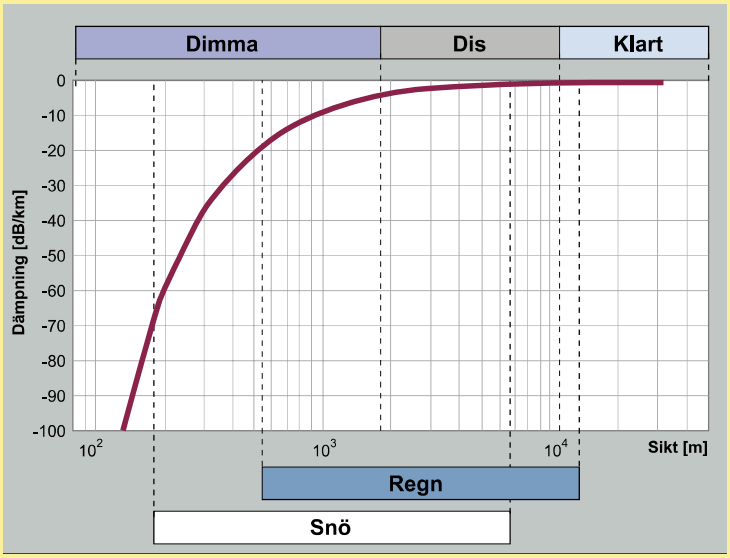
Det finns ett antal olika faktorer som påverkar hur bra tillgängligheten är hos ett laserkommunikationssystem. Tillgängligheten brukar anges som en procentsats över hur stor del av tiden länken kan fungera med en tillräckligt låg BER (Bit Error Rate, d.v.s. antalet felaktigt detekterade bitar i förhållande till antal bitar som skickats). De faktorer som främst begränsar tillgängligheten hos ett system är de atmosfärseffekter som laserstrålen utsätts för mellan sändare och mottagare. Andra faktorer av betydelse för länkens prestanda är överföringshastigheten, strålens divergens, mottagaroptikens storlek och hur exakt upplinjeringen av enheterna är i förhållande till varandra.



Figur F8. Exempel på länkbudget.

Den totala budget som kan avsättas till de förluster systemet förväntas ha begränsas av den sändande laserns uteffekt och vilken känslighet mottagardetektorn har. Känsligheten hos detektorn beror främst av hur hög bandbredd systemet byggs för. Länkar med överföringshastigheter på tiotals Gbit/s är idag fullt möjliga att konstruera, men detektorbruset är högre då än vid lägre överföringshastigheter.

Figur F8 visar ett exempel på hur en länkbudget kan se ut. Marginalen mellan sändarlaserns uteffekt och detektorns känslighet är i exemplet 60 dB, vilket skall fördelas på systemets och kommunikationskanalens möjliga förluster.



Figur F9. Dämpning vid olika väderförhållanden.

Om avståndet är relativt kort (några km) och mottagaren är stor (diameter på flera cm) är det atmosfärsdämpningen som begränsar tillgängligheten mest. Figur F9 visar en beskrivning av hur olika väderförhållanden orsakar dämpning av signalen. Det är främst dimma som kan orsaka signalbortfall, men även kraftiga snöfall eller regn kan dämpa signalen så pass att signalen inte är detekterbar. Transmissionen varierar dessutom med vilken våglängd lasern har (figur F9 är beräknad för 1,55 µm). Det har visat sig att transmissionen är relativt lika för de två mest använda våglängdsområdena – omkring 0,8 µm respektive 1,5 µm. Våglängder omkring 1,5 µm är säkra för ögat (vid måttliga effekter) och den goda utvecklingen av laserkällor vid denna våglängd drivs på bland annat av den stora marknaden för fiberoptisk kommunikation. Källor vid 1,5 µm är av dessa anledningar ofta att föredra.

Elektronisk attack

En eventuell störlaser måste normalt befinna sig inom ett ytterst begränsat område, ha god inriktningsnoggrannhet och dessutom sända med samma våglängd som laserlänken för att en effektiv störning skall vara möjlig. Störning med hjälp av laser är därmed mycket svår att genomföra.

Ytterligare en möjlighet är att införa någon form av hinder mellan sändare och mottagare, t.ex. kraftig rök. Detta medför sämre transmission och kan begränsa tillgängligheten för länken temporärt. Det förutsätter också att länken är upptäckt och lokaliserad.

Elektronisk protektion

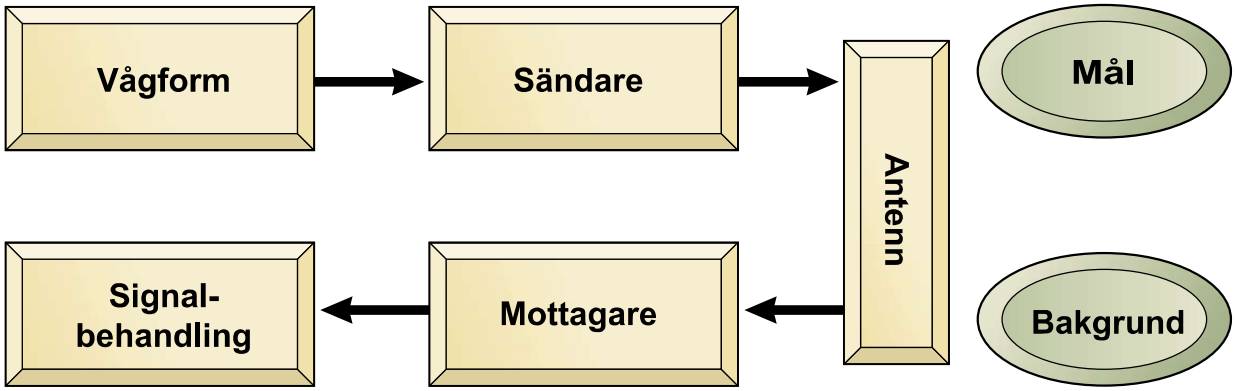
Mycket forskning och utveckling läggs ned på att utveckla laserkommunikationslänkar, både traditionella och sådana som utnyttjar retrokommunikation. Arbetet fokuseras mycket på komponentutveckling för att få länkar med bra prestanda. Hur dessa länkar skall skyddas är i viss mån ett oskrivet kapitel. Ofta har systemen ett bra inbyggt skydd, men en rad åtgärder kommer att krävas vad gäller kryptering av data och olika tekniska skydd för att minimera risken för upptäckt, störning och avlyssning. En möjlighet till skydd mot avlyssning kan exempelvis vara utnyttjande av flera våglängder (våglängdshopp), d.v.s. en motsvarighet till radioteknikens frekvenshopp.

Det effektivaste sättet att skydda en laserlänk mot störning är att se till att den inte upptäcks. Med smala synfält och liten optisk signatur är systemen svårupptäckta. Länkar som utnyttjar retroteknik för kommunikation kan vara lättare att upptäcka p.g.a. reflekterande egenskaper och stora synfält. För att minska risken för upptäckt i sådana länkar kan IK-funktioner integreras så att modulatorn enbart aktiveras om lasersändaren skickar ”rätt” kod. Detta innebär att modulatorenheten inte avger någon eller mycket liten optisk signatur då information inte överförs.

För att minimera bakgrundsljus från omgivningen krävs smalbandiga optiska filter framför mottagaren i en laserkommunikationslänk. Detta är också ett bra störskydd då ett störsystem (störlaser) måste använda samma våglängd som sändarenheten. För att erhålla en hög känslighet hos laserkommunikationslänkar utnyttjas fokuserande optik i mottagaren samtidigt som kravet på snabbhet medför en liten detektorarea. Dessa faktorer innebär med automatik att laserlänkens synfält är begränsat.

För extremt känslig information kan eventuellt kvantmekanisk nyckelöverföring utnyttjas. Detta är en metod för att på distans överföra kryptografiska nycklar. Kvantmekanisk nyckelöverföring är den idag enda kända helt säkra metoden för nyckelöverföring. Den mesta forskningen kring detta område har hittills handlat om fiberoptikbaserade system för överföring av nycklar. På senare tid har man visat att principen även fungerar i fria rymden. I framtiden kan kvantmekaniska system komma att användas tillsammans med optiska kommunikationslänkar som kanal för själva dataöverföringen.

Radarsystem



Figur 29. Blockschema för generiskt radarsystem.

RADAR (RAdio Detection And Ranging) är namn på utrustning och metod för att upptäcka, lokalisera och karakterisera objekt genom belysning med elektromagnetiska vågor. En radarsignal sänds ut och riktas mot ett mål med hjälp av en antenn. Signalen fortplantas med ljushastigheten genom atmosfären, reflekteras i målet och fångas upp av en mottagare varvid i första hand avstånd, riktning och hastighet kan bestämmas. Schematiskt kan ett radarsystem indelas i ett antal block med olika funktioner enligt figur 29.

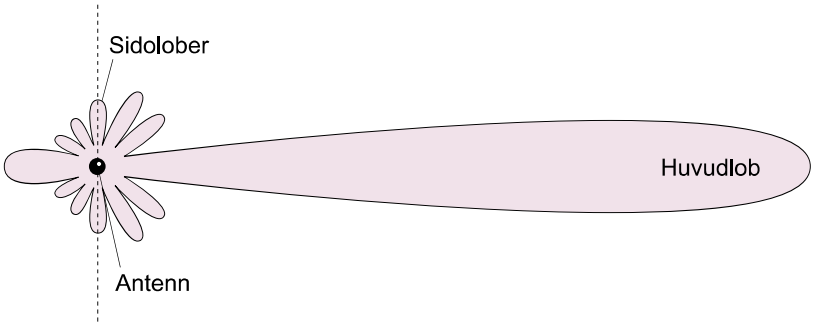
Avståndet till målet ges av signalens löptid från sändaren till målet och tillbaka till mottagaren. Riktningen till målet ges av höjd- och sidvinklar hos antennloben. Förmågan att särskilja mål i vinkel beror på antennens lobbredd. I figur 30 visas ett typiskt strålningsdiagram för ett radarsystem. Diagrammet gäller för såväl sändning som mottagning.

Ett måls närmandehastighet ges av frekvensskiftet (dopplerskiftet) i den mottagna signalen. Radarsystem arbetar vid olika frekvenser beroende på de egenskaper som önskas hos systemet. Tabell 2 visar olika radarband och deras användningsområden.

Vågform

En radarsignal består av en bärvåg (typiskt GHz) som moduleras på något sätt. Modulationen kan gälla bärvågens amplitud, fas, polarisation eller frekvens. Amplitudmodulering med pulsade signaler är vanligt förekommande och har givit upphov till begreppet pulsradar. Under pulstiden sänds bärvågen ut med hög effekt. De flesta militära spanings- och eldledningsradarstationer utnyttjar pulsade signaler. 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



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

Radarband	Frekvens	Radartillämpning, exempel	Räckvidd mot militära mål
HF	3–30 MHz	Ytspaning, fast installerad	OTH-radar, <3000 km
VHF	30–300 MHz	Markspaning från flygplan	SAR ser genom vegetation
UHF	300–3000 MHz	Överlappar L- och S-band	
L	1–2 GHz	Markbaserad mot luftmål	<500 km
S	2–4 GHz	Flygburen mot luft- och markmål	<500 km, även lågtflygande
C	4–8 GHz	Artillerilokalisering	
X	8–12 GHz	Spaning och eldledning från stridsflygplan	<300 km
K_u	12–18 GHz	Eldledning	<50 km
K	18–26 GHz	Eldledning, robotmålsökare	
K_a	26–40 GHz	Eldledning, robotmålsökare	<20 km
V	40–80 GHz	Bilradar 77 GHz	<1 km
W	80–110 GHz	Målsökare, bevakning, kontroll (t. ex. spaning genom kläder)	Kort
mm	30–300 GHz	Överlappar K_a–W-banden	Under utforskning

Tabell 2. Frekvens och olika radarband. Det finns andra sätt att dela in radarbanden, som exempel har NATO en annan indelning.

(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 närmandehastighet.

Korta pulser krävs för 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 modulera utsända pulser med olika fasskift eller olika frekvenser och sedan signalbehandla retursignalen kan både hög avståndsupplösning och lång räckvidd uppnås. Förfarandet kallas pulskompression.

Sändare

Sändarens funktion är att generera den elektromagnetiska signalen som skall belysa målet och förstärka denna så att utsänd effekt är tillräcklig.

Antenn

Radarantennens uppgifter är bl.a. att koncentrera den utsända signalen med önskad intensitet i en smal lob, att styra antennloben till önskad riktning, att undertrycka signaler från oönskade riktningar och att ge tillräcklig antennarea för att ta emot signalenergin från målet.

Mottagare

Mottagarens funktioner är bl.a. att förstärka av antennen uppfångade signaler (målsignaler och icke önskvärda signaler) inom det aktuella frekvensintervallet och att generera det största signal/brusförhållande på mottagarutgången genom filtrering.

Signalbehandlingen

Signalbehandlingens uppgift är bl.a. att beräkna primära mätdata från den mottagna radarsignalen. Denna beräkning sker vanligen från sammanställningen av flera utsända och mottagna radarsignaler som svarar mot den s.k. integrations tiden. Signalbehandlingen har även till uppgift att undertrycka klotter och störsignaler i den mottagna signalen för att öka signal/brusförhållande och därmed förbättra förmågan till målupptäckt. I moderna radarstationer sker signalbehandlingen digitalt.

Spaningsradar

Markbaserade radarstationer för luftövervakning är normalt stora, effektstarka och har lång räckvidd, mer än 300 km. Bärfrekvensen ligger på L- och S-banden. Antennsystemen är stora för att få smala lober och kunna särskilja mål i vinkel. Låg PRF och pulskompression används för entydighet och hög upplösning i avstånd. Ett exempel är PS-860 i det svenska försvaret. Systemet är en pulsad

S-bandsradar (3 GHz) som har räckvidden flera hundra kilometer. Pulsrepetitionsfrekvensen (i storleksordningen 1 kHz) och pulslängd (i storleksordningen tiotals µs) är varierbar.

Därutöver förekommer ett brett spektrum av landbaserade och sjömobila spaningsradarsystem med 3-D-förmåga (mäter målet i tre koordinater). Ett exempel visas i figur 31). Dessa arbetar på frekvenser mellan 3 och 10 GHz.

Figur 31. Svensk artillerilokaliseringsradar ARTHUR (ARTillery HUnting Radar) Foto: Försvarets Bildbyrå/Lasse Sjögren.

För flygburna spaningsradarsystem eftersträvas lång räckvidd (100-tals km), vilket kräver hög medeleffekt och för att begränsa atmosfärsdämpningen relativt låg frekvens. Antennstorleken är begränsad vid flygplansmontering men man önskar en relativt smal antennlob, vilket ställer krav på tillräckligt hög frekvens. S-bandet (2-4 GHz) blir en bra kompromiss mellan dessa olika krav.

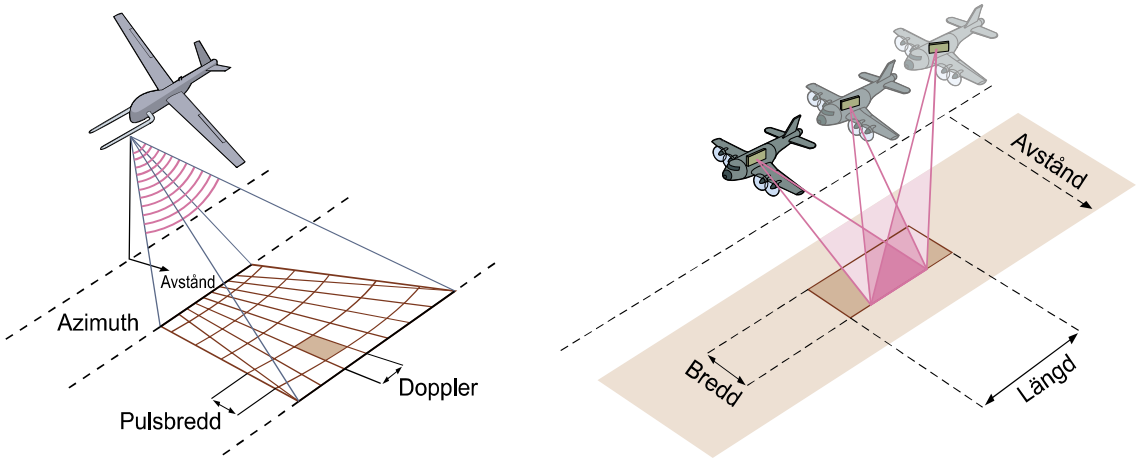
Ett exempel på ett spaningssystem är radarn i flygplanet AWACS (Airborne Warning And Control System). AWACS har förmåga att upptäcka och följa flygande mål och har personal ombord för att jaktleda stridsflygplan. PS-890 är ett svenskt radarsystem för mindre plattformar. Detta system har mer karaktären av traditionell spaningsplattform som skickar automatiskt bearbetade måldata till ett markbaserat ledningssystem.

Båda systemen har S-bandsradar. Genom att använda pulsad dopplerradar kan lågtflygande mål och markklotter diskrimineras.

Syntetisk aperturradar

Syntetisk AperturRadar (SAR) uppfanns redan 1951, men har fått sin renässans i och med den moderna digitaltekniken. Principen bygger på att, istället för att ha en stor antenn, 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 och avståndsoberoende upplösning (upp till 10 cm). Avbildningsprincipen definieras under antagande att det är en stationär scen som avbildas. Rörliga objekt på marken blir ofokuserade i den slutliga SAR-bilden. Jämför analogin med en vanlig optisk kamera med öppen slutare. Alla objekt som rör sig under den tid slutaren är öppen kommer att bli suddiga eller om de rör sig mycket snabbt rent av helt försvinna genom defokusering. SAR är beräkningskrävande men på senare tid har både snabba och generella algoritmer utvecklats.

Ett SAR-system kan opereras i ett flertal moder beroende på uppgift: SAR strip (”stripmap”), SAR spot (”spotlight”) och GMTI (Ground Moving Target Indication). De två förstnämnda SAR-moderna kan endast upptäcka och lokalisera mål som står stilla under integrationstiden. Skillnaden mellan strip- och spotmod är att antennens pekriktning är fast i stripmoden medan den i spotmoden justeras kontinuerligt för att hela tiden peka



Figur 32. Avbildningsgeometri för SAR. Till vänster stripmod, till höger spotmod.

mot ett visst målområde. Det senare gör att integrationstiden ökar och därmed blir bildupplösningen i flygriktningen finare i spotmoden. Priset man får betala för den högre upplösningen är att det avbildade områdets storlek samtidigt minskar. Se även figur 32.

GMTI-moden med vilken upptäckt och lokalisering av rörliga mål kan göras bygger på att 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. Detta skall ske med relativt hög uppdateringstakt (tiotal Hz) då målen i regel kan manövrera snabbt. Då det förutsätts att motståndarsidan kan sätta in motmedel är eldledningsradarsystem utrustade med flera olika störskydd. Radarn har smal antennlob för att kunna mäta in målet noggrant i vinkel, vilket också medför att antennen har en hög förstärkning. Systemmässigt innebär det att synfältet är begränsat, varvid en eldledningsradar i regel måste invisas från ett annat sensorsystem. Eldledningsradar förknippas oftast med luftvärnssystem där radarn förutom höjd- och sidvinkel 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). Dagens eldledningsradar är av typen pulsdoppler, vilka har snarlika egenskaper som nosradarn i flygplan. Nosradarn i de flesta jaktflygplan är förutom en spaningssensor även konstruerad för att låsa på samt följa mål.

Radarmålsökare

Radarmålsökare är den absolut vanligaste sensorn i sjömålsrobotar samt förekommer ofta som målsökare i långräckviddiga jakt- och luftvärnsrobotar. Dess uppgift är liksom eldledningsradarn att kontinuerligt mäta in målets position så att roboten kan styra mot målet. Det är viktigt att riktningen till målet kan mätas under dåliga väderförhållanden och att målets egenstrålning inte är en förutsättning för detta. 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 den s.k. monopulstekniken, vilken i sig utgör ett bra störskydd då både höjd- och sidvinkel mäts för varje puls. Principen implementeras genom att antennen består av flera s.k. ”sub-arrayer” och dithörande mottagarkanaler, vilka sedan jämförs. För sjömål utnyttjas två mottagarelement. När ett mål detekterats och följning påbörjats skapas en följelucka som i sidled är given av lobbredden för sändarenheten. I längdledd 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 km) måste sändaren vara placerad i roboten. För sådana radarjaktrobotar kan det skjutande flygplanet undanmanövrera och behöver inte ligga kvar och belysa målet. På senare tid har radarmålsökare utvecklats för markmål. Det är dock relativt svårt för en radar att diskriminera typiska markmål från falska mål, som stenar, träd eller hus. Dock kan hög avståndsupplösning tillsammans med dopplerinformation användas. Ett sätt att motverka störsändare som befinner sig i målet är att övergå till passiv följning och styra mot störkällan (”home on jam”). Radarmålsökare som styr mot andra radarsändare förekommer som ”signalsökande” robotar.

Elektronisk stödverksamhet

Alltsedan andra världskriget har radar varit ett viktigt verktyg i krigföringen såväl på marken som till sjöss och i luften. En direkt följd av detta är att även radarsignalspaning och radarvarning är väsentliga funktioner som utvecklats parallellt med radarsystemen.

Ett exempel på tidig taktisk användning av radarsignalspaning är den tyska satsningen på att effektivisera bekämpningen av brittiska bombflygplan som under långa perioder, i stort sett varje natt, i stora formationer flög in över Tyskland. Den tyska jakten utrustades med enkla anflygningsutrustningar, som angav riktningen till ett utvalt brittiskt bombflygplan. Anflygningsutrustningen drog fördel av att samtliga brittiska bombflygplan var utrustade med en larmradar vars uppgift var att varna för jaktanfall bakifrån. Först sent under kriget insåg man på alla nivåer inom ”Bomber Command” att larmradarn gjorde mera skada än nytta varefter bortmontering skedde. En sak var man då helt på det klara med: En radar är aldrig ofarlig, varken för målet eller för användaren.

Traditionellt har den defensiva funktionen radarvarning varit inriktad mot skydd av enbart den egna plattformen. För att snarast kunna vidta motåtgärder när exempelvis en hotande robot närmar sig är naturligtvis kort reaktionstid väsentlig. Radarvarnare måste momentant täcka in hela frekvensområdet i alla riktningar varför principer med avsökning i frekvens och vinkel och krav på samverkan med system på andra plattformar är mindre lämpade.

Figur 33. HMS Malmö, högst upp på fartyget sitter den gemensamma antennen för taktisk radarsignalspaning och radarvarining. Foto: Försvarsmakten.

För taktisk radarsignalspaning finns större möjligheter att öka systemkänslighet och inmätningsnoggrannhet genom att använda lägre momentan bandbredd och antenner med riktverkan. Det finns även möjlighet att utnyttja operatörer för att inrikta spaningen och på olika sätt förbättra den automatiska bearbetningen med manuella analyser. Den taktiska radarsignalspaningen arbetar i tidsperspektivet minuter vilket medger att samverkan sker med andra enheter för att exempelvis lägesbestämma en emitter.

Teknikutvecklingen, gällande framför allt digital signalbehandling, är och har varit sådan att gränsytan mellan varning och spaning blir alltmer otydlig. Radarvarnares egenskaper avseende känslighet och mätförmåga närmar sig vad som tidigare bara har erbjudits av taktiska system för radarsignalspaning samtidigt som varningsfunktionen stöds av den omvärldsuppfattning som dessa ger. Möjligheterna att flera system samverkar för själva varningsfunktionen har också ökat.

Ur användarens perspektiv är de primära uppgifterna för både radarvarnare och system för taktisk radarsignalspaning att:

- Upptäcka signaler från emitterande radarsystem.
- Identifiera eller klassificera de radarsystem som sänder.
- Bestämma riktningar till (och helst positionsbestämma) emitterande radarsystem.

Utöver detta bör systemen också ha möjlighet att inhämta parametrar för underlag till telekrigbibliotek.

Upptäckt

För att en radarsignal skall kunna upptäckas måste ett flertal grundvillkor som är nödvändiga för detektering vara uppfyllda samtidigt. Signalspaningssystemet eller varnaren måste exempelvis momentant bevaka den frekvens radarn utnyttjar för att radarsignalen skall kunna detekteras. Om signalspaningssystemet använder riktantenn och signalen är svag måste även antennen samtidigt peka mot radarn. Sannolikheten för att upptäcka en viss radarsignal minskar om varnaren eller signalspaningssystemet använder avsökning i frekvens- eller vinkelled, och i ännu högre grad om avsökning sker i både frekvens- och vinkelled. Upptäcktsegenskaperna påverkas således av hur mycket systemet momentant bevakar av det frekvens- respektive vinkelområde som systemet totalt täcker.

Som tidigare har konstaterats medför kraven på kort reaktionstid att radarvarnare ofta momentant täcker hela det önskade frekvensområdet och att systemets antenner, utan avsökning, täcker en stor del av sfären (luftfallet) eller halvsfären (ytfallet). Upptäcktssannolikheten för denna typ av radarvarnare anses därmed ofta vara i närheten av 100 %.

När villkoren för upptäckt är uppfyllda finns förutsättningar för att signalen från en viss radar kan detekteras, vilket innebär att en vald tröskelnivå överskrids och händelsen genererar data som går vidare i systemet. Sannolikheten för att detektering sker kan förhållandevis enkelt beräknas för varje enskild mottagen puls och problematiken är i princip densamma som hos en radar. Parametrar som påverkar sannolikheten är den mottagna signaleffekten och bruseffekten i mottagaren samt vilka amplitudfördelningar dessa har. Detekteringssannolikheten avgörs även av den tröskelnivå som är vald i mottagaren. En sänkning ökar sannolikheten för att en mottagen puls skall detekteras men samtidigt ökar risken för att tröskeln överskrids när bara brus finns närvarande. Tröskelnivån är därför en kompromiss som ger tillräcklig god sannolikhet för detektion utan att falsklarmsrisken är oacceptabelt hög.

Taktiska system för radarsignalspaning och radarvarnare presenterar eller rapporterar i princip aldrig upptäckt av enstaka pulser. För att upptäckt av en signal skall anses ha skett krävs normalt att flera pulser detekterats. Det krävs dessutom att de bedöms höra samman och inte är en samling pulser från olika radaremittrar. Möjligheterna att upptäcka en viss radarsignal påverkas därför av det aktuella systemets uppbyggnad, men även signalmiljön kan inverka genom att den interna pulssorteringen försvåras eller att bearbetningstiden ökar.

Eftersom möjligheterna att upptäcka en radarsignal beror av egenskaperna hos både signalspaningssystemet och radarsystemet samt påverkas av signalmiljön och vågutbredningen är det inte enkelt att beskriva vilken räckvidd man når med en radarvarnare eller ett system för radarsignalspaning. Om inte den egna målarean är mycket stor vinner dock i de flesta fall en plattform utrustad med en radarvarnare upptäcktsduellen mot en radar eftersom signalspaning utnyttjar envägsutbredning. I många situationer är även räckvidden mot radarns sidlober taktiskt användbar.

Kombinationen lång räckvidd och stor momentan vinkeltäckning medför att system för radarsignalspaning ofta har stor momentan yt- eller volymtäckning. De kan därför med fördel invisa elektrooptiska system eller syntetisk aperturradar eftersom dessa behöver ansenlig tid för att avsöka stora ytor.

Klassificering och identifiering

En viktig uppgift för taktiska system för radarsignalspaning och radarvarnare är att identifiera eller klassificera upptäckta signaler. Det blir därmed möjligt att presentera och rapportera vilken typ av radar systemet har upptäckt. Eftersom en radar använder olika vågformer beroende på mätuppgift är det även möjligt att avgöra den aktuella arbetsmoden. Informationen är betydelsefull för att exempelvis definiera hotnivån eller att välja lämpliga störmetoder.

Vid identifieringen är bland annat signalens bärfrekvens samt tidsavståndet mellan konsekutiva pulser, (den så kallade pulsgivningen) viktiga parametrar. Ytterligare information kan användas, exempelvis pulslängd, modulation på pulserna eller antennavsökningsmönster. Resultatet från parameterestimeringen jämförs med innehållet i systemets emitterbibliotek och i gynnsamma fall kan entydig identifiering göras. Olika radarsystem har dock

ofta likartade vågformer, 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 dellösning i detta arbete är att göra rätt urval av emittrar utifrån vad som bedöms kunna förekomma i aktuellt område. En omsorgsfull förberedande underrättelseverksamhet i form av signalspaning är av detta skäl nödvändig men emitterbibliotek behöver även uppdateras under pågående operationer.

En viktig aspekt av identifiering är att signalspaningssystem inte kan inriktas mot att bara hantera signaler från motsidans radarsystem. Den dominerande andelen signaler som tas emot härstammar från egna system eller från system som är neutrala eller civila. Dessa bidrar självfallet till omvärldsbilden men kan i vissa fall liknas vid klotter för en radar.

Om en inmätt signal inte kan matchas mot någon specifik emittertyp eller emittermod i biblioteket kan klassificering vara den kvarstående möjligheten. Klassificering kan sägas vara en grövre identifiering som endast avgör radarklass, exempelvis fartygsbaserad spaningsradar.

Säker identifiering har vid internationella insatser visat sig vara mycket betydelsefull för att undvika vapeninsatser mot den egna sidan eller civila. Bristande identifiering omöjliggör därför vanligtvis vapeninsats. Identifieringsförmågan är en av de verkligt atttraktiva egenskaperna hos radarvarnare och system för radarsignalspaning. Förmågan är genom den goda upplösningen överlägsen vad som kan åstadkommas med en radar samtidigt som väderberoendet hos elektrooptiska sensorer saknas. Signalspaningssystemets förmåga att avslöja arbetsmoden hos aktuell emitter är också unik och avslöjar status och intentioner.

På senare år har det blivit aktuellt med identifiering med en noggrannhet som medger individbestämning av emittrar. På engelska används beteckningen SEI – Specific Emitter Identification. Utvecklingen har blivit möjlig genom att system för radarsignalspaning i ökad grad utnyttjar digital signalbehandling. Nyansskillnader i mottagna vågformer kan därmed upptäckas och användas för att särskilja olika exemplar av samma radartyp. Möjligheterna bromsas till viss del av att radarutvecklingen samtidigt resulterar i att skillnaden mellan radarindivider minskar.

Framtida radarsystem kommer troligen även ha stor vågformsflexibilitet vilket inte bara försvårar individbestämning utan allmänt är en stor utmaning vid utveckling av identifierings- och klassificeringsfunktioner i kommande generationer av radarvarnare och system för radarsignalspaning.

Riktnings- och lägesbestämning

De flesta radarvarnare och system för taktisk radarsignalspaning har möjlighet att mäta radarsignalernas infallsriktning i en eller två dimensioner. Moderna radarsystem har ofta kapacitet att variera sina vågformsparametrar från puls till puls. I täta komplexa signalmiljöer är det därför betydelsefullt att riktningsbestämning av varje mottagen puls sker för att den interna funktion som separerar signaler från olika radarstationer skall kunna fungera utan sammanblandningar.

Metoder som används för riktningsbestämning av varje mottagen puls brukar benämnas monopulsmetoder och innebär en jämförelse mellan utsignalerna från ett antal parallella mottagarkanaler vars ingångar är anslutna till lämpligt utformade och inriktade antenner. Amplitudmonopuls och fasmonopuls är exempel på monopulsmetoder för riktningsbestämning, vilka ibland kombineras för att ge såväl entydighet som noggrannhet. Lobmaxpejling med sidlobsblockering är en annan metod som medger noggrann och säker riktningsbestämning med en rund- eller sektorsökande riktantenn även om dess sidlober är höga, vilket ofta gäller för bredbandiga signalspaningsantenner.

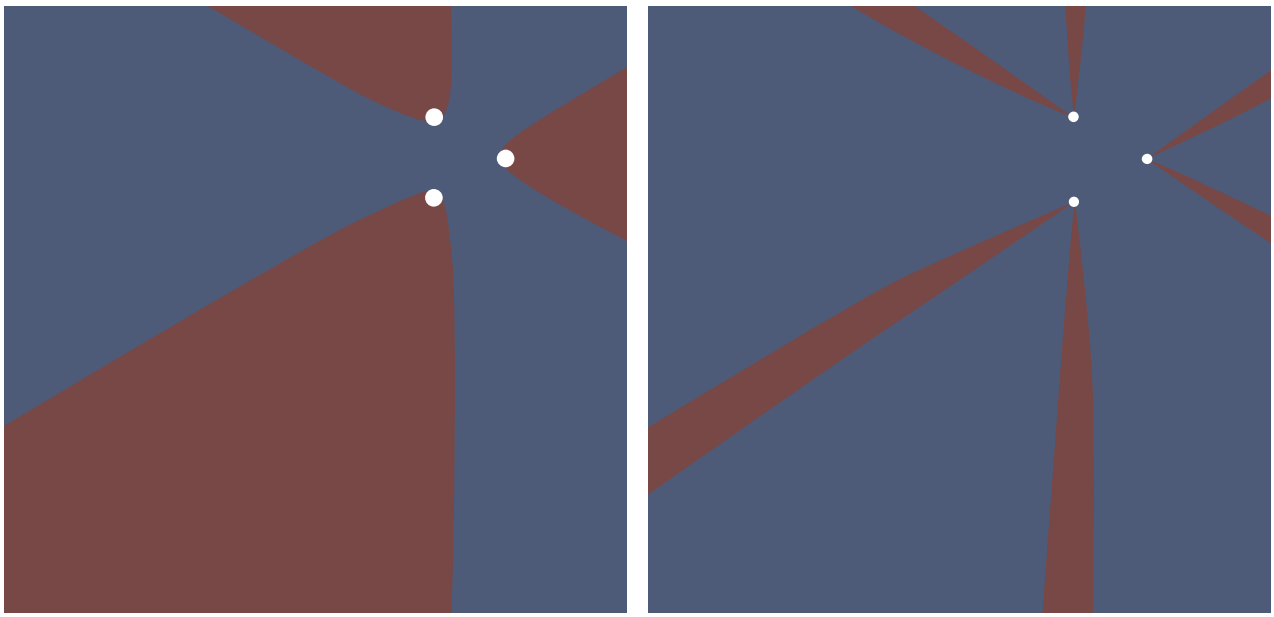
Vid radarvarningsfunktion är riktningsinformation ibland tillräckligt för att initiera undanmanöver och invisa motmedel. Riktningsbestämning är dock även ett av flera alternativ som kan ge underlag för att bestämma ett radarsystems position, en information som ofta har stort taktiskt värde. Lägesinformationen bidrar till den egna omvärldsuppfattningen och kan användas för att invisa vapensystem eller andra sensorsystem. I det senare fallet är emitterläget även en parameter som är lämplig för att lösa den associering som måste ske vid eventuell sensordatafusion.

Det är önskvärt att lägesbestämning sker snabbt, med stor noggrannhet och utan mångtydigheter. Dessutom är det önskvärt att lägesbestämning kan ske inom ett stort område utan att signalspaningssystemet flyttas, det vill säga att yt- eller volymtäckningen är stor. Helst bör lägesbestämningen ske i tre dimensioner, men ofta är två dimensioner tillräckligt, exempelvis om identifieringen visar att signalen kommer från en mark- eller ytbaserad emitter.

Det finns ett antal olika metoder för att lägesbestämma en emitter. Ett generellt problem är att radarvarnare och system för radarsignalspaning endast i undantagsfall kan mäta avståndet till emittern från en stationär inmätningsposition. Lägesbestämning sker därför normalt genom att använda mätningar från två eller flera geografiskt separerade inmätningspositioner, antingen producerade av en rörlig inmätare eller med hjälp av flera inmätare som samverkar. I det senare fallet kan lägesbestämningen ofta ske både snabbt och med god noggrannhet, vilket är en av de stora vinsterna vid sensorsamverkan. Vid sensorsamverkan är det viktigt att säkerställa att alla mätningar tas mot samma mål – relativ identifiering. Genom att taktisk radarsignalspaning har en unik förmåga att identifiera emittrar med hjälp av karakteristiken i den mottagna vågformen finns i de flesta fall goda möjligheter till robust relativ identifiering.

Triangulering, även kallad krysspejling, är en klassisk och välkänd lägesbestämningsmetod som baseras på riktningsmätningar tagna vid olika inmätningspositioner. Modernare metoder som i gynnsamma fall ger noggrannheter användbara för att invisa precisionsvapen är exempelvis TDOA – Time Difference Of Arrival – respektive DDOA – Doppler Difference Of Arrival. Metoderna utnyttjar olika mätegenskaper som finns inneboende i de mottagna radarsignalerna. TDOA ger därför noggrann lägesbestämning av radarsystem som har bra avståndupplösning medan DDOA är en noggrann metod mot radar som mäter målets hastighet med hjälp av dopplerprincipen. DDOA förutsätter rörelse, helst med hög hastighet, och fungerar därför bäst hos flygburna radarvarnare och signalspaningssystem.

Både TDOA och DDOA kan besväras av mångtydigheter på samma sätt som radarsensorer kan vara mångtydiga vid avstånds- respek-



Figur 34. Bilderna visar i brunt vilka områden som ger mångtydig lägesbestämning när tre samverkande inmätningsenheter bildar en liksidig triangel. I den vänstra figuren används enbart tidsdifferensmätning – TDOA. I den högra figuren har TDOA kompletterats med grov riktningsbestämning. Riktningsmätningen förmår inte lösa upp kvarvarande områden med mångtydighet eftersom ingen av de tre inmätarna i dessa områden ger tillräcklig vinkelseparation mellan sanna och falska emitterlägen. En lämpligt placerad fjärde inmätare skulle ge entydig lägesbestämning inom hela området.

tive hastighetsmätning. I signalspaningsfallet påverkas mångtydighetproblematiken av såväl vågformen som aktuell inmätningsgeometri, se exempel figur 34.

Oavsett om lägesbestämningen sker enskilt eller genom samverkan mellan flera inmätare ger ökande mättid potential för bättre lägesnoggrannhet. När flera inmätare tillsammans utför lägesbestämningen kan noggrannheten redan efter kort tid i gynnsamma fall medge invisning av precisionsvapen. Samverkansvinsten blir alltså störst när snabb inmätning krävs.

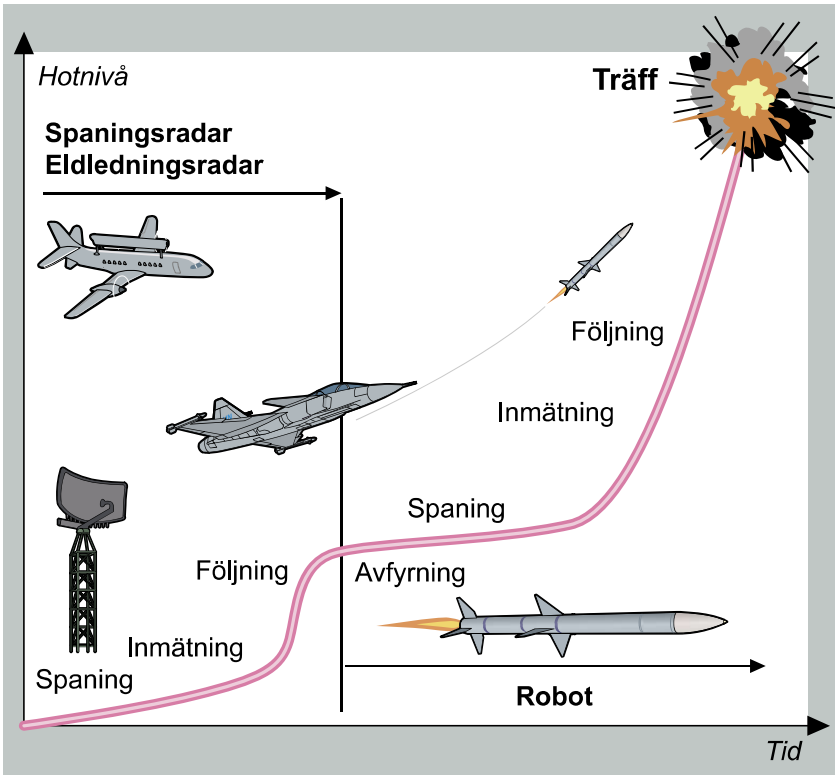
För att få en lägesbestämning som snabbt ger en entydig och noggrann radarposition oavsett typ av radarsignal är det gynnsamt om olika lägesbestämningsmetoder kombineras och används av samverkande, separerade inmätare. Denna insikt kommer troligen i hög grad att påverka framtida utveckling av radarvarnare och taktiska system för radarsignalspaning.

Elektronisk attack

En radarsensor har en mer eller mindre stark koppling till ett vapensystem. Det kan vara en spaningsradar med lång räckvidd som ger invisning till en eldledningsradar, vilken i sin tur leder en vapeninsats med en kommandostyrd robot mot en plattform.

Det kan också vara en målsökare som innebär ett mer akut hot och kräver snabb insats för att avvärja hotet. Syftet med att störa en motståndarens radarsensor är att degradera dess prestanda tillräckligt mycket så att inte vapensystemet får avsedd verkan. Det är också av stor vikt att motåtgärder sätts in så tidigt som möjligt i händelsekedjan, så att inte motståndaren kan avfyra sin robot. Man kan generellt säga att ju tidigare störning sätts in desto enklare är det att lyckas med störinsatsen.

Störningen kan vara maskerande (t.ex. brus), vilseledande (t.ex. avståndsavhakning) eller mättande (t.ex. många falska mål) beroende på typ av sensorfunktion. Störaktiviteter kan, utifrån den taktiska situation i vilken störningen sker, karakteriseras som bakgrundsstörning, medstörning, egenstörning och förgrundsstörning.



Figur 35. Hotnivån i en duell varierar från långräckviddig spaning till inmätning, robotavfyrning, målsökning och träff.

Bakgrundsstörning

Bakgrundstörning med bredbandigt brus är den absolut mest effektkrävande störmetoden, men i vissa fall är det den enda lösningen. Oftast sker störningen i radarns sidlob, varför effektbehovet blir mycket stort. Bandbredden motsvarar hotradarns systembandbredd (det vill säga hoppfrekvensbandbredden).

Detta störfall är vanligast för att maskera flygplan, då det är lättast att skydda små plattformar. Fartyg, som har en mycket stor målarea, är svåra att maskera på stort avstånd.

Medstörning

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

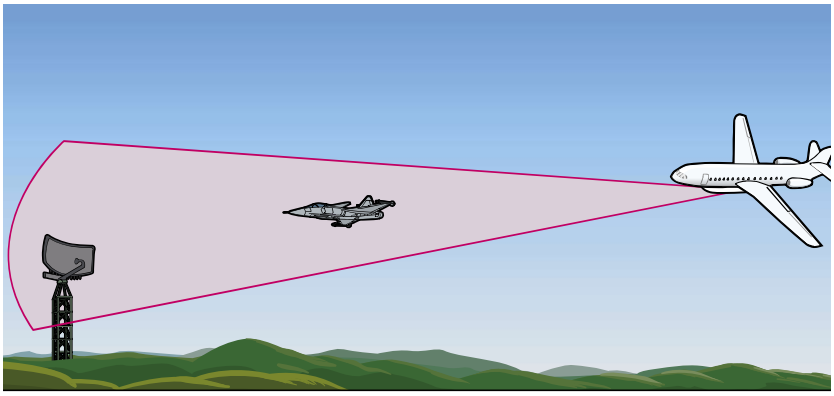
För att skydda ett anfallsföretag kan ett av flygplanen förses med en mer kvalificerad störsändare i form av en störkapsel. Denna kapsel har en betydligt större förmåga än de störsändare som varje flygplan har.

Egenstörning

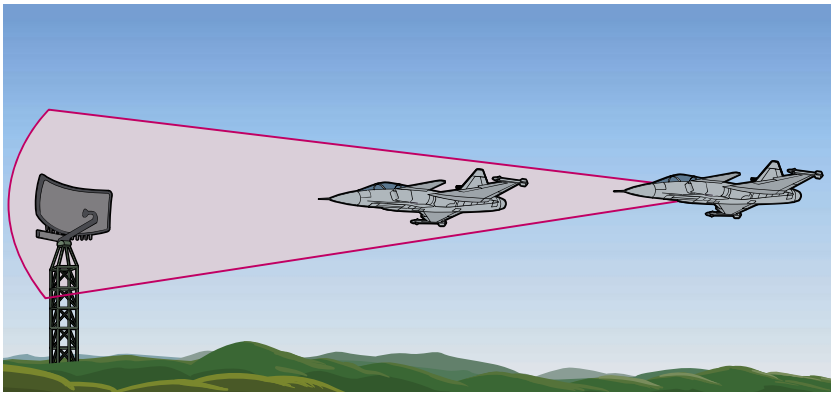
Egenstörning är det vanligast förekommande störfallet, när det gäller att skydda en enskild plattform (flygplan eller fartyg). Här är störutrustningen placerad på plattformen som skall skyddas och det är vanligtvis robotar som störs med högsta prioritet. En egenstörare har måttliga krav på uteffekt, då den oftast arbetar med huvudlobsstörning.

Förgrundsstörning

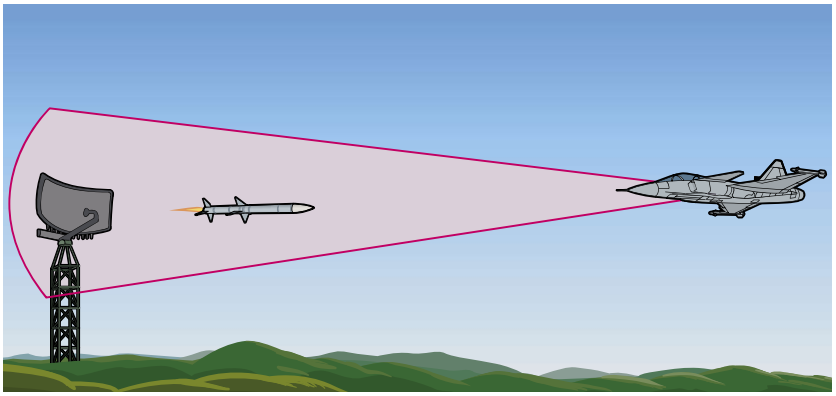
Med förgrundsstörare menas att störsändaren är placerad nära radarn (mycket närmare än skyddsobjektet). Denna typ av störsändare kan vara utplacerad i förväg, eller skickas fram med någon UAV. Denna störform är för maskering den i särklass mest effektiva. Ju närmare störaren är radarn, desto bättre kan skyddsobjekten maskeras. Både brusstörformer och generering av stora mängder falska mål förekommer. Generellt gäller att god störverkan kan uppnås med liten uteffekt.



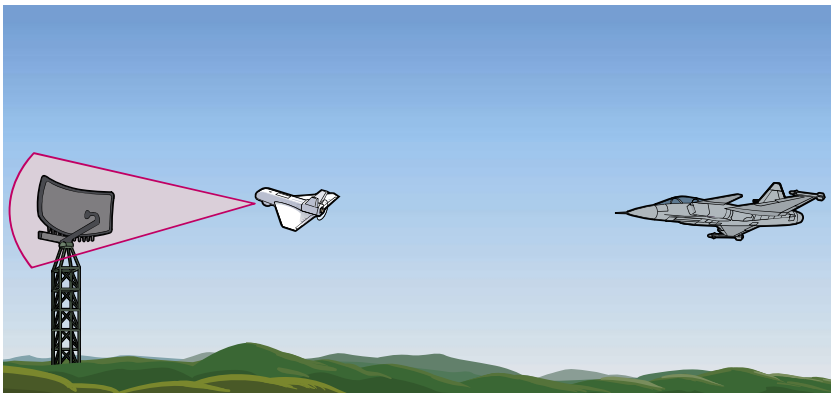
Figur 36. Bakgrundstörning.



Figur 37. Medstörning (eskortstörning).



Figur 38. Egenstörning.

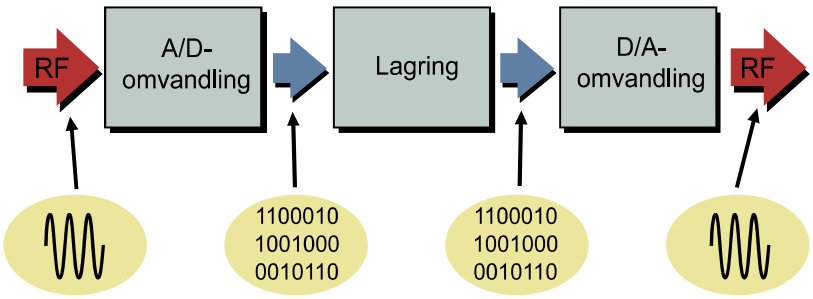


Figur 39. Förgrundsstörning.

Störning av spaningsradar

En spaningsradar av 3D-typ är främst avsedd för långräckviddig spaning mot luftmål. Radarn använder pulskompression med binärfaskodning för att få både god räckvidd och avståndsupplösning samt MTI för att särskilja rörliga mål från stillastående objekt.

Mot spaningsradarsystem är syftet att i första hand förhindra (alternativt fördröja/försvåra) detektering (upptäckt) genom att utnyttja maskerande eller mättande störning.



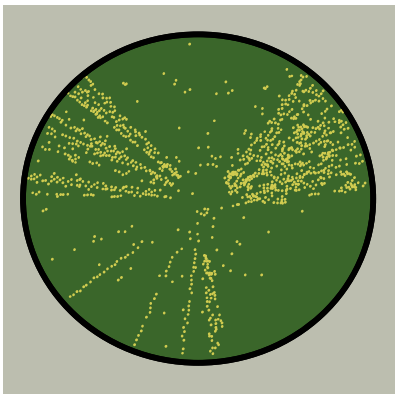
Figur 40. En nyckelkomponent när det gäller att skapa falska mål är Digitala Radio-Frekventa Minnen (DRFM). RF-signalen digitaliseras och lagras i minnen, och kan läsas ut ur minnet efter godtyckligt lång tid och godtyckligt antal gånger. En finess är att störningen blir bandbreddsanpassad, det vill säga störpulserna ser precis ut som riktiga ekon. Falskmålen drar samma nytta av radarns signalbehandlingsvinst som de riktiga målen.

Maskerande störning

Den vanligaste (enklaste) maskerande störformen är brus. Bruset höjer radarmottagarens egenbrus, vilket är dimensionerande för räckvidd, då signal/brusförhållandet SNR (Signal to Noise Ratio) är avgörande för möjligheterna att detektera mål, se figur 41. Beroende på hur radarn arbetar ställs olika krav på brusets bandbredd. Effekterna som brusstörning ger upphov till är enkla att beräkna. Till exempel kan radarns räckvidd under störda förhållanden enkelt beräknas då störövervikten JSR (Jamming to Signal Ratio) är känd, se figur 42. Bredbandigt brus är mer effektkrävande än smalbandigt. Radarns signalbehandlingsvinst gör i allmänhet radarn mindre känslig för brusstörning. Den enklaste formen av brusstörare består av en bredbandig brusgenerator med möjlighet att styra uteffekten. Det krävs ingen mottagarfunktion.

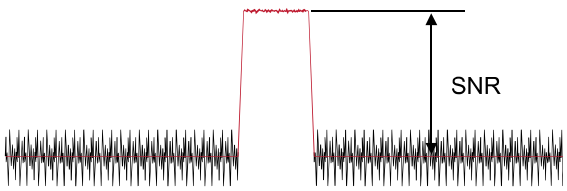
Mättande störning

I och med att det digitala RF-minnet (DRFM) introducerades blev det möjligt att skapa repeterstörformer som kan massproducera falska mål. Med synkron repeterstörning avses störning som 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, vilka gör ett riktigt mål svårt eller till och med omöjligt att upptäcka. Radarn har mycket hög mottagarkänslighet, vilket gör att kravet på uteffekt för störsändaren inte blir särskilt högt. Det viktiga är att störsystemets mottagare kan detektera radarn. I princip kan falskmål alltid skapas under förutsättning att störarens mottagare kan detektera radarpulserna.

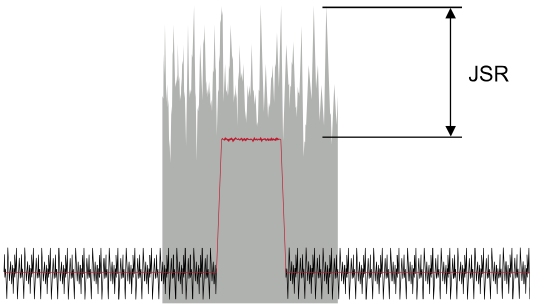


Figur 43. PPI till radar som är utsatt för mättande störning.

En repeterstörsändare måste ha en mottagare i systemet, vilket innebär att risken för telekonflikt ökar. Det gäller att placera sändar-



Figur 41. Exempel på signal/brusförhållande.



Figur 42. Exempel på störövervikt (JSR).

och mottagarantennerna på lämpligt sätt för att få en maximal isolering mellan dem.

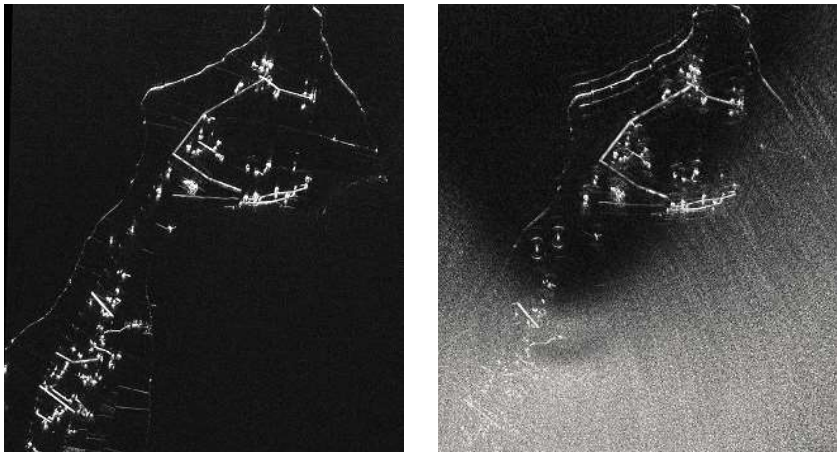
Störning av SAR

En Syntetisk Apertur Radar (SAR) används bland annat till att spana in på en motståndares område, för att till exempel få en bild av flyg- eller marinbaser. Där kan enskilda flygplan eller fartyg observeras. Långvågiga SAR-system kan till och med se genom olika slag av maskeringar och genom tät skog. Fordon eller grupperingsplatser kan därför lätt upptäckas med hjälp av SAR.

Ett sätt att skydda ett område från insyn från en SAR är att använda störsändning. SAR-principen innebär att radarn sänder koherenta (med känt fasläge) pulser under lång tid (100 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.

Maskerande repeterstörsändning

Med ett DRFM tas radarsignalen emot, lagras och repeteras sedan som en kontinuerlig pulsskur tills nästa radarpuls anländer. Då repeteras nästa störpulsskur med ett slumpmässigt valt fasskift. Det innebär att radarbilden blir defokuserad bakom störsändarens position. Genom att placera ut flera störsändare runt det skyddade området kan området skyddas från alla spaningsriktningar.



Figur 44. Till vänster visas en SAR-bild (ostörd) från ett fältförsök över norra Visingsö. Till höger motsvarande bild, men SAR-radarn har blivit utsatt för störsändning. Den utsända störeffekten är ca 10 W.

Även andra metoder att skapa störsignalen kan användas. Frekvensen och svepkarakteristiken på radarns pulser mäts in och genereras med en digitalt styrd oscillator.

Störning av målsökare

Om störningen av den målinmätande spaningsradarn misslyckas kommer robotar att avfyras. Har detta väl skett är det inte så mycket att göra innan robotens målsökare startar sändningen i en första spaningsfas. Dagens målsökare är till största delen av monopulstyp, vilket innebär att målsökaren mäter infallsriktningen från varje mottagen puls. Även om målsökaren blir störd kan den avgöra riktningen till störkällan 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 en plattform som skall skyddas, så kallad ”off board-störsändare”.

När målsökaren aktiverats börjar den med en spaningsfas, d.v.s. den gör ett eller några svep med antennen, för att hitta mål i det område som spaningsradarn angivit. I det här läget är det mycket viktigt att snabbt komma igång med störning, för att förhindra detektion och låsning på målet. Falska mål i sidolob i kombination med täckpuls eller kontinuerligt brus i huvudlob är exempel på störning i spaningsfasen.

Om störning i spaningsfasen misslyckas startar målsökaren följning på målet, d.v.s. målsökaren går in i följefas. Då gäller det att få bort följeluckan från målet med någon form av vilseledande störning, gärna i kombination med undanmanöver och remskastning. Den vilseledande störningen sker genom avhakning i avstånd, hastighet eller vinkel. Mot klassiska sjömålsrobotar är det avstånds- och vinkelavhakning som används.

Remsor

Remsor (eng. chaff) är ett av de äldsta radarmotmedlen. Remsor är radarreflekterande tunna trådar som skjuts eller fälls i mängd för att generera falskmål i syfte att förvilla en radar. Redan 1943 använde de allierade för första gången remsor för att skydda bombflygplan vid räder över Tyskland. Remsor har använts i alla konflikter sedan dess för att dölja uppdrag (maskerande effekt), skapa skenmål (påhakande effekt) eller för att få en radar att tappa följning (avhakande effekt).

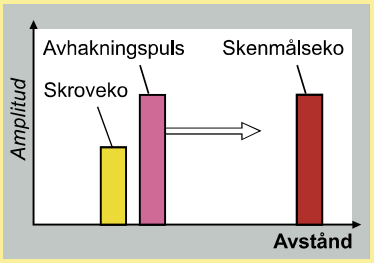
De första radarremsorna bestod av stanniolfolie uppstagat med papper, medan moderna remsor består av metallbelagda nylon- eller glasfibertrådar. En enskild modern remsa är ca 20-30 µm tunn och ytbelagd för att de tillsammans packade remsorna lätt skall separera då de skjuts ut eller fälls.

En remsa fungerar som en dipolantenn som reflekterar en del av den mottagna energin från en radar. Reflektionen är störst för de radarvåglängder som matchar längden på remsan. Vanligtvis används så kallade halvvågsresonanta remsor, vilket innebär att remsan klipps till halva den våglängd som den avser att störa. För att störa en 10 GHz radar (λ=3 cm), klipps remsan t.ex. till en längd på 1,5 cm. Figur 46 visar radarmålarean som funktion av frekvensen för en sådan remsa. Som synes fås resonanser vid 10, 20, 30 GHz, osv.

Genom att packa remsor med olika remslängder fås ett mer kontinuerligt spektrum. Packningen anpassas

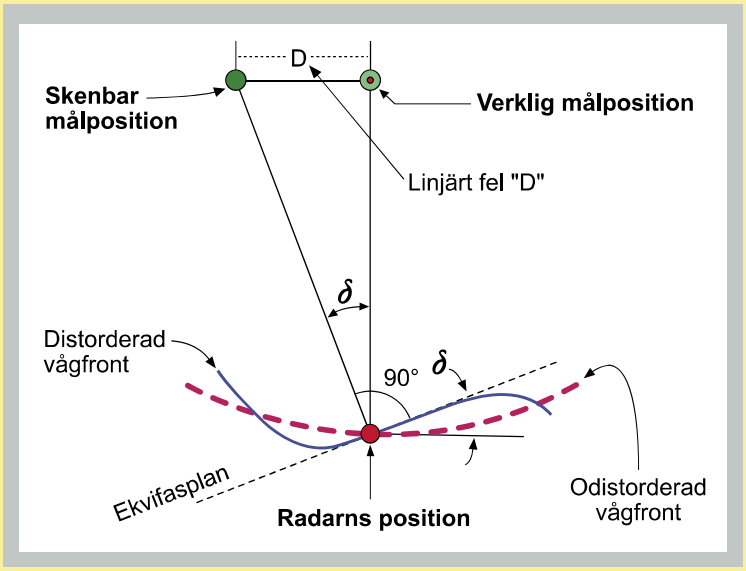
Avståndsavhakning

En kopia av radarpulsen med högre amplitud än fartygets skroveko fördröjs successivt för varje mottagen radarpuls. Om störformsparametrarna valts på lämpligt sätt kommer målsökarens följelucka att följa avhakningspulsen. När följeluckan dragits av målet finns det inget skroveko i följeluckan som konkurrerar med falskekot. Då kan störformer som kräver stora störövervikter sättas in, såsom korspolarisationsstörning eller cross-eye. Ett annat alternativ kan vara att utnyttja avståndsavhakning i kombination med remsor så att avhakningspulsen leder följeluckan till remsorna. Se exemepl i figur 47.



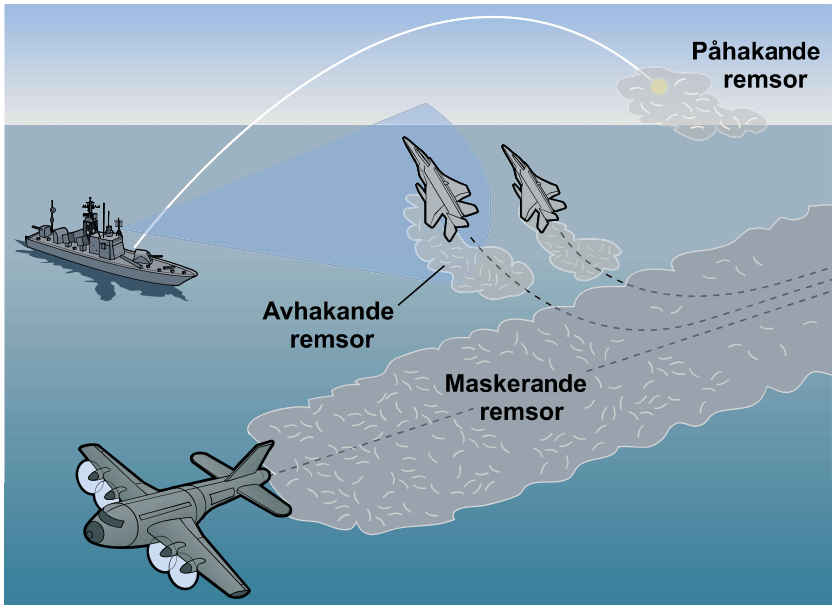
Figur F10. Avståndsavhakning, gul puls är eko från fartygsskrov, röd puls är eko från remsor. Avhakningspulsen ska dra målsökarens följelucka till remsmolnet.

Vinkelavhakning



Figur F11. Cross-eye-principen.

En av de vinkelvilseledande teknikerna är fasfrontstörning (cross-eye), vilken bygger på att två antenner producerar ett skenmål beläget vid sidan om antennsystemet. Anledningen är att antennerna sedan de tagit emot radarsignaler byter signaler innan dessa sänds ut igen, vilket ger upphov till en vridning av fasfronten som målsökaren försöker följa. Ifall vågfronten är sfärisk går roboten längs en radie mot målet i sfärens centrum. Vid fasfrontsstörning böjs roboten av från denna riktning genom att fasfronten deformeras lätt nära målsökaren. För att detta skall inträffa måste signalerna vara nästan lika starka och ligga i motfas. Signalerna tar då nästan ut varandra nära roboten, men samtidigt vrids fasytan så att målsökaren leds förbi målet.



Figur 45. Exempel på användning av remsor.

vid tillverkningen mot den troligaste hotbilden. Det förekommer även remsfällarsystem som klipper remsorna efter den våglängd som belyser skyddsobjektet.

Spridningsmekanismen är mycket viktig för att remsorna skall få avsedd störeffekt. Spridning sker inom flyget vanligast genom att utnyttja turbulensen bakom flygplanet. Remsorna fälls från en plats på flygkroppen som har kraftig turbulens (t.ex. vingspets), alternativt monteras anordningar på remsfällaren som genererar turbulens. Inom marinen utnyttjas granater för att skjuta remsorna till lämplig plats och där sprids remsorna med en sprängladdning. Fällda remsor har i regel en fallhastighet på ca 1 m/s, varför de kan ha effekt lång tid efter spridningen om de fällts från hög höjd.

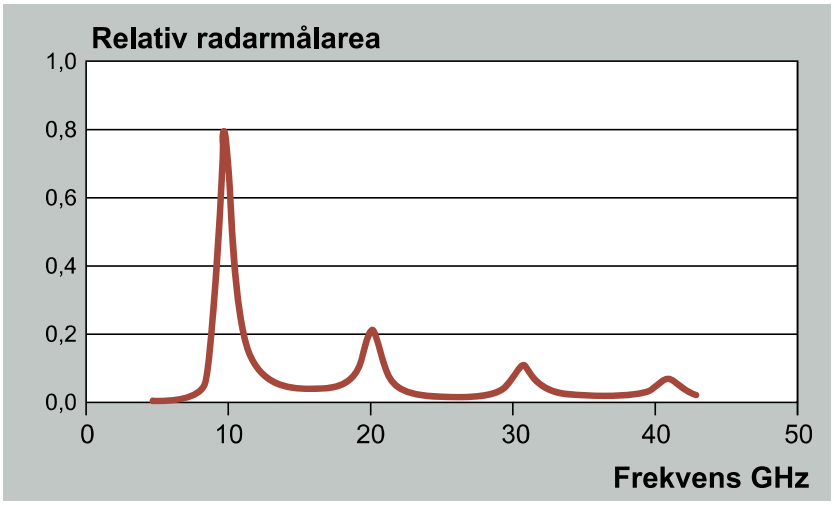
Givetvis har en mängd störskydd utvecklats under åren för att undertrycka remsstörning. Dopplerupplösning är effektivt för att filtrera bort remsor efter snabba flygplan, då remsorna snabbt bromsas upp och då får helt annan dopplerfrekvens än flygplanet.

Av samma anledning är MTI (Moving Target Indication) effektiv för att sålla fram rörliga mål från stillastående eller långsamt rörliga mål (remsor). Med hög upplösning, d.v.s. korta avståndsföljeluckor och smala antennlober, 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 sålla bort remsmolnet som en målkandidat.

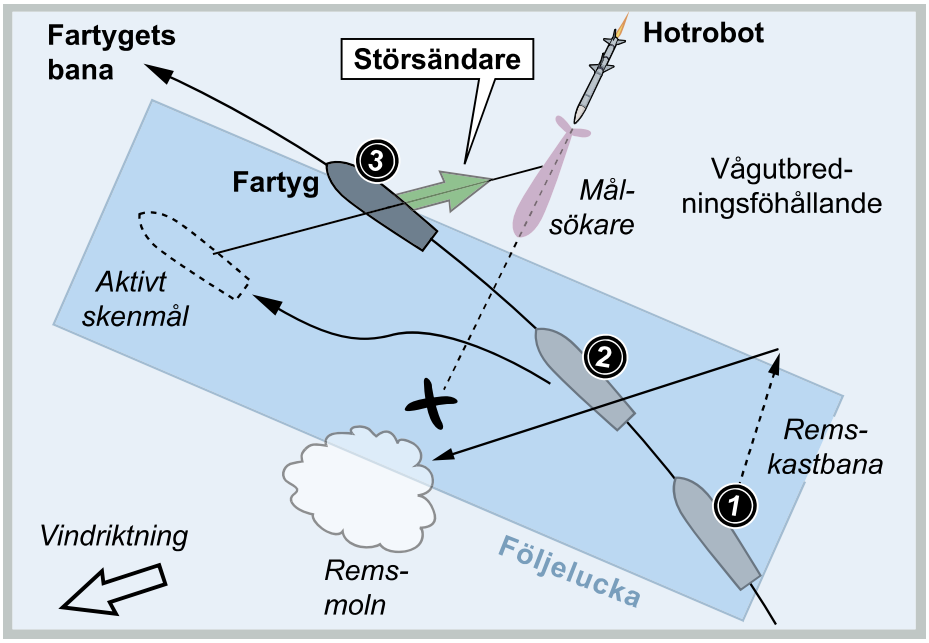
Fördelarna med remsor är att de är ett relativt billigt motmedel som genererar vinkelvilseledning och i många fall får en radarstation att utnyttja mindre gynnsamma filtreringsfunktioner. Om en radar på grund av remsfällningar måste använda sin MTI-funktion försämras radarns möjligheter att följa mål som rör sig i cirklar runt radarn.

Nackdelar med remsor är som nämnts att de snabbt stannar upp, och att modulationsanalysen kan identifiera remsorna. Andra nackdelar är remsornas miljöpåverkan samt att remsorna behöver tid för att utvecklas och generera en målarea.

För att komma till rätta med en del av nackdelarna används rem-



Figur 46. Radarmålarean som funktion av frekvens, för remsor med längden 1,5 cm.

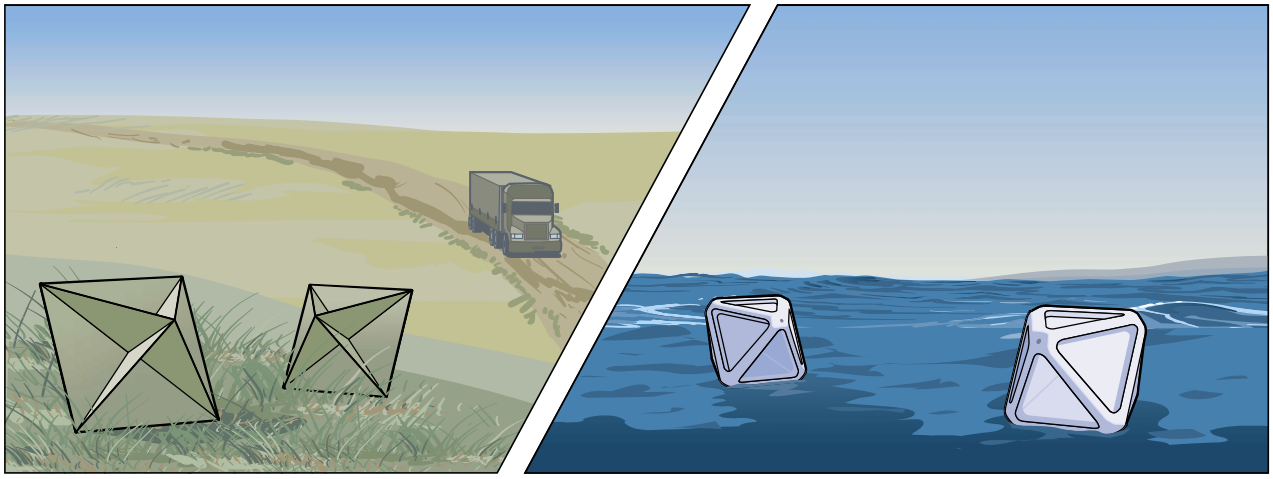


Figur 47. Ett avhakningsscenario uppdelat i tre faser. 1. Hotets riktning detekterat. Remsor läggs mot den relativa vindriktningen (för att remsmolnet skall passera över fartyget). En gir påbörjas för att minimera fartygets målyta. 2. En aktiv störsändare aktiveras för att dumpa hotets följelucka på remsorna. 3. Avhakningsögonblick. Konkurrens mellan fartygseko, störsändareko och remsmoln. Överväger effekten från remsor och störsändare har störningen lyckats. Störsändaren slås av och hotets följelucka dumpas på remsorna.

sor ofta i kombination med aktiv repeterstörsändning. Genom att med repeterstörsändaren generera avstånds- eller doppleravhakning lockas målsökarens eller följeradarns följe- eller dopplerlucka till att låsa över på remsmolnet (dumpning). Figur 47 visar ett marint avhakningsscenario där både störsändare och remsor används.

Oftast kan endast en begränsad mängd remsor tas med under ett uppdrag (speciellt för flygplan). Att kunna bedöma hur en remsfällsekvens skall utformas mot en följeradar är därför viktigt så att ett minimum av remsor används effektivt för att vilseleda radarn. Remsor är det vanligaste passiva radarmotmedlet, men det finns även andra motmedel som t.ex. hörnreflektorer. Genom att hänga upp eller placera ut dessa på flottar (”Rubber Duck”) kan stora skenmål genereras, se figur 48.

Genom att kombinera remsor med hörnreflektorer i sjöfallet fås mer fartygslika signaturer som försvårar ovan nämnda modulationsanalys.



Figur 48. Exempel på hörnreflektorer.

Elektronisk protektion

Störskydd av olika slag införs i radarsystemets olika delar (se blockschemat för ett generiskt radarsystem i figur 29) för att undertrycka signaler från störsändare och om möjligt blockera signaler från falska mål. Störskydden är ofta fast inprogrammerade i moderna radarsystem.

Störskydden förhindrar överstyrning av signaler i mottagaren samt ökar förhållandet mellan målsignalen och störsignalen. Även inmätning och följning av mål med hög robusthet och noggrannhet hjälper till att öka skyddsverkan.

Rörliga plattformar är ett störskydd mot falska mål om flera inmätningar från olika radarpositioner kan korreleras med varandra. Radarns placering relativt terrängen och vågutbredningsförhållanden kan användas som störskydd för att dämpa störsignaler från riktningar utanför radarns täckningsområde.

Koherenta vågformer innebär ett störskydd eftersom störsignalerna måste vara matchade till radarsignalerna för att få effektiv störverkan. Variabel PRF innebär ett störskydd eftersom störsändaren inte effektivt kan bilda falska mål på avstånd närmare radarn än det egna. Hoppfrekvensvågformer är ett viktigt störskydd eftersom maskerande brusstörning måste spridas ut över stor bandbredd, vilket ger försämrad störverkan.

Hög sändareffekt är ett grundläggande störskydd som ökar signal/störförhållandet. Låga sändarförluster är också viktigt och kan uppnås i aktiva elektriskt styrda sändarantenner där sändarförstärkarna sitter nära antennens strålningselement. Aktiva elektriskt styrda sändarantenner möjliggör också styrning av sändarens sändningsmönster och antennlob.

Hög antennvinst och smal huvudlob är ett viktigt störskydd för sändarantennen vid följning av mål medan vid sökning även en bredare huvudlob med lägre antennvinst kan användas. Detta är möjligt med elektriskt styrd sändarantenn som snabbt kan ändra strålningsriktning och lobform, vilket även är viktigt för att få opredikterbara sändningsmönster.

Mottagarantennens utformning är ett väsentligt störskydd. Stor antennarea och hög antennvinst med smal huvudlob ger högt signal/störförhållande och hög noggrannhet vid riktningsmätning. Låga sidolober ger högt signal/störförhållande och undertrycker störsignaler från sidolobsområdet. Adaptiv sidolobsundertryckning (ASLU) för mottagarantennen används för att undertrycka störning från diskreta riktningar i sidoloberna. Sidolobsblockering är ett vanligt störskydd mot pulsade störningar. Monopulsantenner eller digitala gruppantenner med flera mottagarkanaler kan upplösa vilseledande störning och motverka avhakning av målföljning.

Ett grundläggande störskydd i mottagaren är filtrering av mottagna signaler så att inte störsignaler utanför radarns signalbandbredd kommer in i signalbehandlingen. Mottagaren måste också begränsa och blockera starka störsignaler för att förhindra överstyrning och olinjära effekter som kan generera nya störsignaler inom mottagaren. Förstärkningsreglering och hög dynamik i mottagaren är också viktigt för att kunna filtrera och undertrycka störsignaler i den vidare signalbehandlingen.

De flesta störskyddsfunktionerna implementeras 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 telekrighotets utveckling. 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.

Elektrooptiska system

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

Tabell 3. Spektral indelning av det optiska spektrumet.

Elektrooptiska (EO) sensorer och system avser sensorer och system där optiska och elektroniska komponenter samverkar. Ett annat begrepp som ibland används är optronik (sammanslagning av orden optik och elektronik) och optroniska system. Det handlar således om elektromagnetiska vågor inom det optiska våglängdsbandet som omvandlas till elektriska signaler eller vice versa. Frekvensområdet för det optiska våglängdsbandet sträcker sig från 20 till 3000 THz ($20 \cdot 10^{12}$ till $3000 \cdot 10^{12}$ Hz). För att få hanterliga värden brukar istället våglängd användas. De ovan nämnda frekvenserna motsvarar våglängdsintervallet 0,1 till 14 µm (1 µm = 10^{-6} m, d.v.s. en tusendels millimeter).

Elektrooptiska system kräver fri siktsträcka för att kunna utnyttjas. Det finns två huvudtyper av elektrooptiska sensorer, passiva respektive aktiva sensorer. Passiva sensorer sänder inte ut någon egen strålning utan mäter reflekterad eller emitterad strålning från objekt och bakgrund. De system som bygger på detektion av reflekterad strålning är vanligtvis dagljussystem, medan de som bygger på emitterad strålning har dygnet runt-kapacitet. Exempel på passiva system är TV-kameror, IR-kameror och bildförstärkare. Aktiva EO-sensorer innehåller en aktiv strålningskälla, vanligtvis en laser, och en mottagare (detektor). Exempel på aktiva system är laseravståndsmätare, avbildande laserradar och optikspanare.

De flesta elektrooptiska system mäter intensitet. En stor skillnad mellan passiva och aktiva EO-system är att med de aktiva erhålls även avstånd. Många militära elektrooptiska system utnyttjar såväl passiva som aktiva delsystem.

Elektrooptiska system är vanligtvis avbildande i ett plan. Det finns

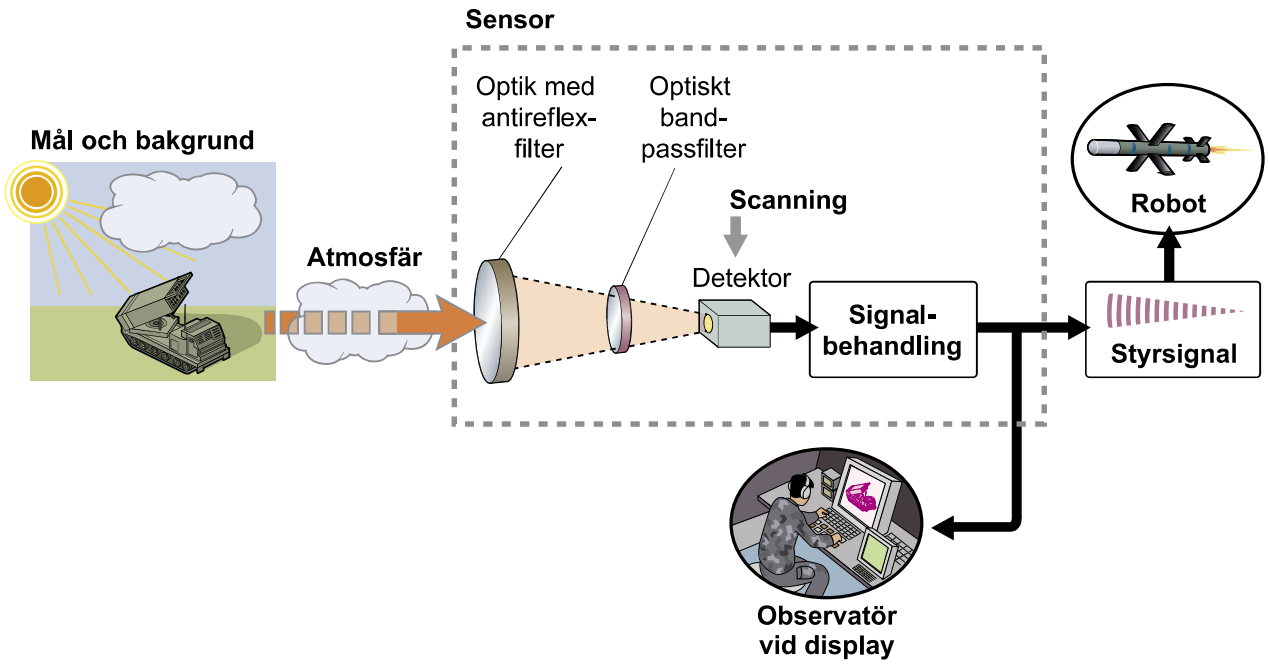
Det elektrooptiska våglängdsområdet

UV, ultravioletta området, (0,1–0,4 µm): Våglängder under 0,2 µm har ingen praktisk användning vid optisk vågutbredning i atmosfären. Molekylspridningen i atmosfären spelar stor roll och medför att belysningen från solen blir mer diffus och skuggbildningen därför mindre markant än i det visuella området. Dämpningen i ozonskiktet gör att bakgrundsnivån minskar vid de kortaste våglängderna, det s.k. solblinda området under ca 0,3 µm. Målföljare och varnare utnyttjar området.

VIS, visuella området, (0,4–0,7 µm): Det mänskliga ögats känslighetsområde är anpassat till solstrålningens spektrala maximum. Bildförstärkare, t.ex. NVGer (Night Vision Goggles), och videoutrustning utnyttjar området.

NIR, nära infrarött, (0,7–2,0 µm): Enkla kiseldetektorer fungerar upp till drygt 1 µm och används mycket inom kommunikation via fiber och vid övervakning med eller utan aktiv belysning. Nd:Yag-laser har våglängden 1,06 µm och används för olika ändamål, t.ex. i avståndsmätare, men strålningen är skadlig för ögat. Våglängden 1,54 µm används i sammanhang där man vill ha ögonsäker laserutrustning.

TIR, termiska IR-området (ca 2–14 µm): Kan delas in enligt SW IR (short wave IR, 2–3 µm), MW IR (medium wave IR, 3–5 µm) och LW IR (long wave IR, 8–14 µm). Avgasstrålning från jetflammor syns tydligt inom MW IR-området Solreflexer kan även uppträda inom detta område. Bakgrunden har sin maximala strålning inom LW IR-området. Strålningsenergin vid ca 300 K (27 °C) har också sitt maximum inom det långvågiga IR-området och medför hög mätnoggrannhet vid de omgivningstemperaturer som är vanliga i naturen.



Figur 49. Ett passivt elektrooptiskt system består av optik, filter, avsökningsmekanik, detektor och signalbehandling. Detta gäller oavsett om det är ett system för att presentera en bild på en monitor eller för att generera styrsignaler för en robot med passiv målsökare.

olika typer av avbildande system, dels skannande system med ett eller flera detektorelement, dels system med stirrande matrisdetektorer. Detektorer för längre våglängder i TIR måste ofta kylas för att minska det termiska bruset.

Passiva EO-sensorer

Med passiva elektrooptiska system avses sensorer som mäter termiskt emitterad strålning eller reflektion av naturlig strålning (solljus). En schematisk skiss av ett passivt elektrooptiskt system visas i figur 49. Beroende på vilka typer av föremål som skall betraktas används sensorer som är känsliga i olika våglängdsområden. Val av vilket våglängdsintervall ett system skall arbeta inom bestäms av de tänkta målobjektens förväntade signaturer, bakgrundens variationer (klotter) och atmosfärens transmission.

Spaningssensorer

Optisk spaning från satelliter har blivit allt mer betydelsefull och pågår kontinuerligt för inhämtning av information.

Flygspaning är delvis detsamma som flygfotografering. Oftast används film som har känslighet inom det visuella området. Vid mörker används NIR-film och NIR-blixt. Denna typ av spaning har långa omloppstider, d.v.s. tiden från fotografering till insats mot ett mål är relativt lång. Denna klass av spaningskameror byts allt mer ut och ersätts med elektrooptiska kameror. Informationen i dessa är från början digital och kan signal- och bildbehandlas. Att informationen är digital innebär också att det finns möjlighet att länka informationen och korta ner omloppstiden.

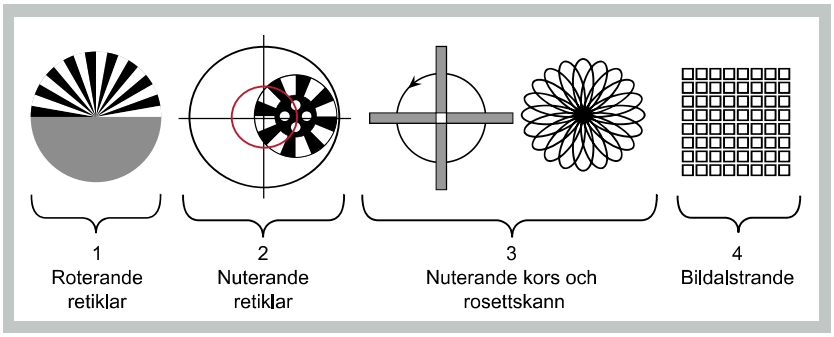
Bildförstärkare förstärker svagt ljus från bl.a. stjärnor och gör det möjligt att verka i mörker. Den teknik som används i bildförstärkare kan även utnyttjas till mörkersikten, periskop för mörkerkörning, mörkerkikare m.m.

Med elektrooptiska sensorer inom TIR-området kan spaning ske även i mörker. Dessa sensorer är inte beroende av någon ljuskälla till skillnad från bildförstärkare. Okylda system kan göras små, men har sämre prestanda än kylda IR-system. Beteckningen FLIR (Forward Looking InfraRed) är en benämning på sensorer för skilda ändamål. En annan benämning är IRV (InfraRed Vision). Upplösningen varierar mellan 0,1 och 1 mrad beroende på synfält. FLIR-sensorer finns i bl.a. helikoptrar, stridsvagnar, fartyg och som sikten i robotsystem.

Målsökare

Inom det elektrooptiska området är det främst värmedetekterande och bildalstrande system som utvecklas. System som till sin natur inte är bildalstrande kan illustreras

med elektrooptiska jaktrobotar och manburna luftvärnsrobotar (s.k. MANPADS, MAN Portable Air Defence Systems). Utvecklingen av dessa inleddes under 1950-talet, och målsökarna kallas för retikelsystem. I första generationens system är principen att låta den infallande strålningen fokuseras på en roterande retikelskiva. När målet var centrerat inom synfältet blev följningen inte bra med denna typ av system. Genom att vinkla ut optiken (från optiska axeln) och låta den rotera kring den optiska axeln erhålls ett nuterande system. Det nuterande systemet har därför ett momentant synfält och ett totalt synfält. Utvecklingen fortsatte sedan med nuterande kors och rosettskannande system. De system som idag utvecklas är i de flesta fall bildalstrande, se figur 50.



Figur 50. Indelning av olika IR-målsökare i generationsklasser.

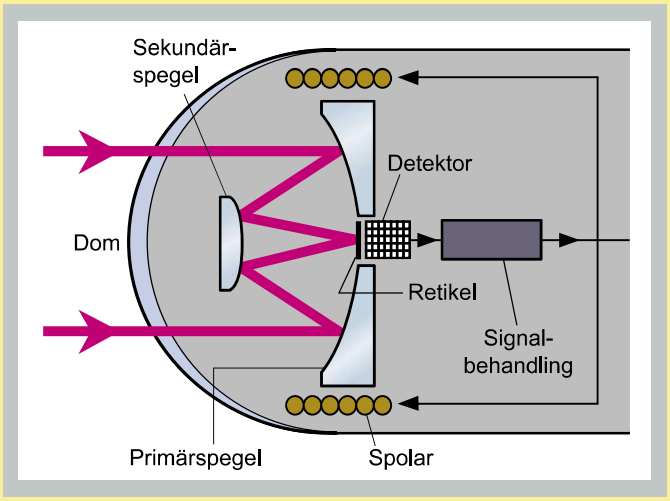
Målföljare där FLIR eller TV utnyttjas som sensor har en operatör som gör målval. Systemet tar sedan genom signal- och/eller bildbehandling över och sköter följningen och styrningen. Bildbehandling i en målsökare innehåller följande delar: förbehandling av bild (brusreducering), segmentering (framtagning av intressanta områden i bilden), egenskapsextraktion (ta fram målkandidaters egenskaper) samt klassificering (avgöra vad som är troliga mål).

Följning kan ske genom att använda någon av ett antal olika principiella metoder för att följa målet. Centroidmålföljare använder sig av kantföljning och s.k. areabalansering. Kantföljning sker genom att detektera målets utsträckning i höjd och sida (vilket kräver att intensitet såväl från bakgrund som från mål har mätts upp). För att kompensera för asymmetrier i målets form görs en areabalansering. Principen för areabalansering är att en rektangel som ges av målets utsträckning i höjd och sida, delas upp i 4 stycken lika stora delrektanglar (2 i höjd och 2 i sida). Därefter jämförs målets area i höjd- och sidled för att ge styrsignaler så att målets area blir jämnt fördelad i höjd respektive sida.

Korrelation bygger på att en referensbild tas (när målet pekas ut) och jämförs med nästa inlästa bild av sensorn. Den punkt som matchar bäst mot referensbilden är följepunkten. Uppdatering av referensbilden sker ett par gånger per sekund.

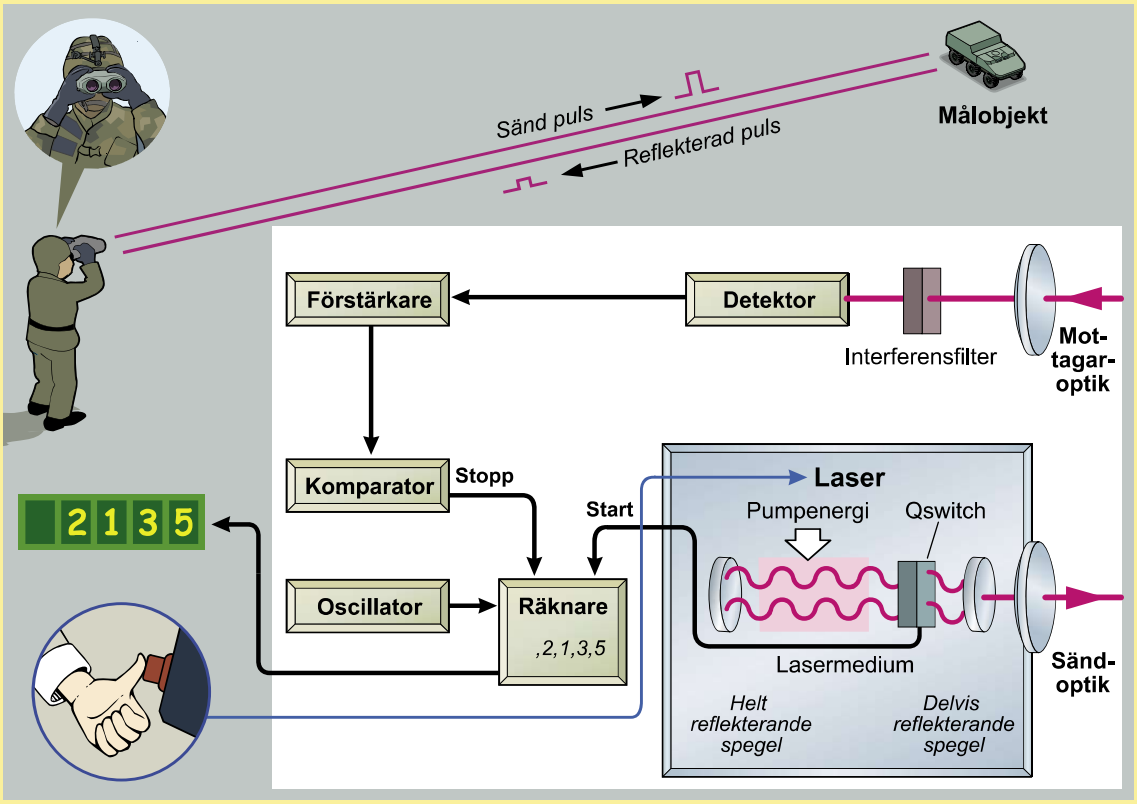
Roterande retikelsystem

Strålning från mål och bakgrund projiceras via ett spegelsystem (primär- och sekundärspegel) på en roterande (ca 100 Hz) retikel (mönstrad skiva), som är placerad framför detektorn. Mönstret och rotationen för retikelskivan ger upphov till en modulerad signal, från vilken målets position kan avgöras. Denna typ av system kallas ibland för punktmålsökare. Genom att luta sekundärspegeln och låta den rotera samtidigt som retikelskivan hålls fix erhålls ett nuterande retikelsystem. Samma optikkonfiguration kan utnyttjas för nuterande kors. Om såväl primär- som sekundärspegeln lutas och ges motsatta rotationer kan ett rosettmönster erhållas.



Figur F12. Principskiss på ett roterande retikelsystem.

Laseravståndsmätare



Figur F13. Principen för laseravståndsmätare.

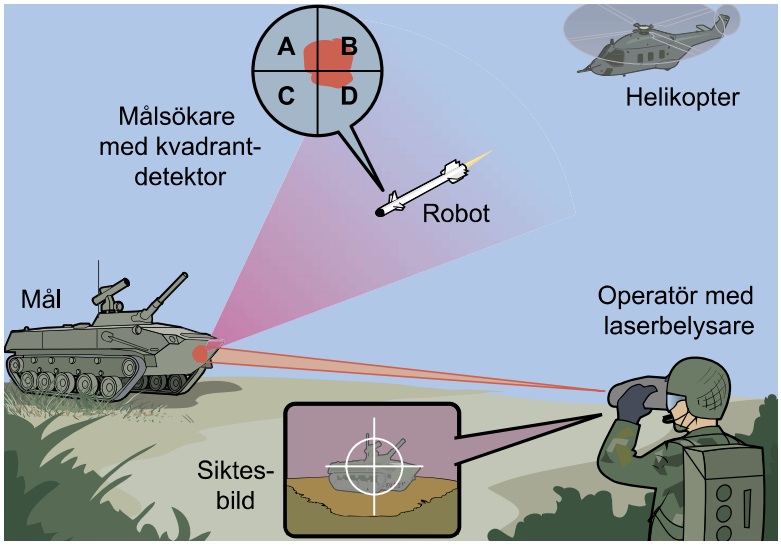
När ett avstånd skall mätas går en signal dels till en Q-switch, vilken släpper igenom en kort laserpuls, dels till ett räkneverk som räknar pulser från en oscillator. Mottagarobjektivet fokuserar den infallande reflekterade laserpulsen mot en fotodetektor. I denna genereras en signalström som, med hjälp av en förstärkare, förvandlas till en spänning som jämförs 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 (ca $3x10^8$ m/s), N antalet klockpulser och f klockfrekvensen. Typisk räckvidd för en laseravståndsmätare är 10–20 km vid god sikt.

Aktiva system

En aktiv EO-sensor är en optisk sensor som mäter reflekterad strålning från en egen belysare. Den första militära tillämpningen var avståndsmätning, följt av målinvisning och ledstrålestyrning av robotar och glidbomber samt zonrörstillämpningar. Avbildande laserradar är en annan tillämpning.

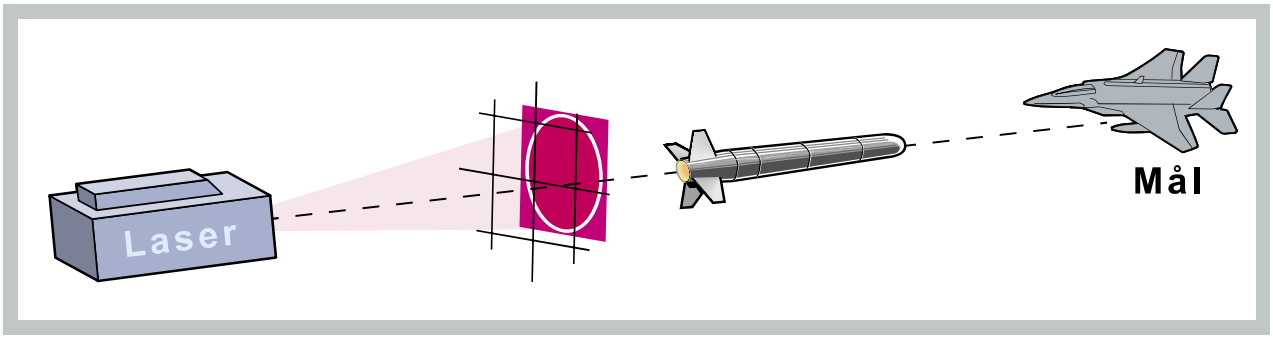
Laserbelysare

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 t.ex. en robot mot den laserfläck som reflekteras från målet. Målsökaren i roboten består av en kvadrantdetektor, fyra detektorer som känner av bilden av laserfläcken, och via roder driver roboten att centrera fläckbilden och därmed styra mot denna (samma princip som areabalansering). 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 ca 1 streck). I belysningssystem på rörliga plattformar, som flygplan och helikoptrar, används lasern tillsammans med FLIR eller TV-kameror. Dessa används för att identifiera och efter pålåsning för att följa mål. Lasern slavas till siktessystemet, d.v.s. riktningen hos lasern är sådan att den hela tiden



Figur 51. Exempel på laserbelysare.

Figur 52. Fältgrupperad luftvärnsrobot 70. Foto: Försvarets Bildbyrå/Lasse Sjögren.



Figur 53. Principen för ett laserledstrålesystem. Lasern ger en rums-tidsmodulerad stråle som medför att roboten som har en laserdetektor baktill vet sitt läge relativt syftlinjen.

riktas mot centrum av synfältet för det siktessystem (FLIR/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 51.

Laserledstråle

Principen för ledstrålesystem är att när roboten har skjutits iväg sända en laserstråle mot en detektor i robotens bakre del. Laserstrålen är kodad över tvärsnittet så att roboten kan avgöra var i strålen den befinner sig och därmed styra mot centrum av strålen. Detta gör att roboten hela tiden styr dit laserstrålen pekar. Eftersom detektorn sitter placerad i robotens bakre del och är riktad mot lasern behövs en lägre lasereffekt (ca 10000 ggr) än hos t.ex. laserbelysarsystem, vilka förlitar sig på reflekterad strålning. Detektorplaceringen innebär också att den är riktad från målet, vilket gör systemet svårstört. Det svenska luftvärnsrobotsystemet RBS 70 är ett sådant system, se figur 52.

Laserradar

Till skillnad från passiva bildalstrande sensorer kan en laserradar, i likhet med en traditionell radar på radiofrekvenser, bestämma ett måls avstånd och hastighet. Laserradar bygger på samma princip som laseravståndsmätare med den skillnaden att flera pulser skickas ut för att generera en högupplöst avståndsbild. En laserradar medger hög avståndsupplösning och kan ge en tredimensionell registrering av ett objekt, som underlag för klassificering eller t.o.m. identifiering. En laserradar kan även diskriminera mål mot terrängbakgrund. En vanlig våglängd för laserradartillämpningar är 1,5 µm. Vanligtvis integreras en laserradar med en IR-sensor, typ FLIR.

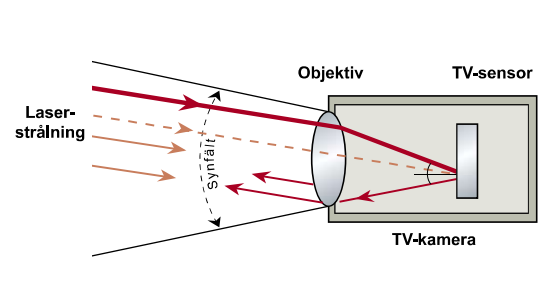
Elektronisk stödverksamhet

Optikspanare

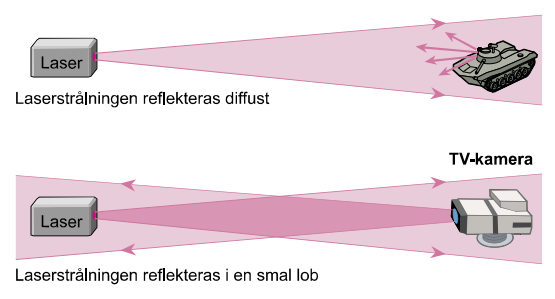
För att upptäcka passiva elektrooptiska system är en metod att använda en s.k. optikspanare. Denna bygger på principen att en laser som belyser en optisk sensor inom dess våglängdsområde ger upphov till en kraftig retroreflex (kattögeeffekt) om lasern befinner sig inom sensorns synfält. Även med lasern strax utanför synfältet kan reflexen vara betydligt starkare än de diffusa reflexer som omgivande bakgrund kan ge. En optikspanare utnyttjar retroreflexen för invisning och följning. Optikspanaren består i grunden av en laser samt spegelsystem som möjliggör snabb avsökning av ett område. Avsökningen sker med en spaltformad laserstråle som avsöker spaningsområdet. Om ett passivt elektrooptiskt system finns inom det avskannade området erhålls en retroreflex som gör det möjligt att med stor noggrannhet göra en lägesbestämning.

Figur 54. NVG-bild av retroreflektion från en fältkikare på två kilometers avstånd.

Retroreflektion



Figur F14. Princip för retroreflektion



Figur F15. Diffus reflektion och retroreflektion.

När en laser belyser ett objekt kommer laserstrålen att reflekteras. Normalt är reflektionen diffus, vilket innebär att endast en liten del av den reflekterade strålningen kommer tillbaka till laserkällan. För elektrooptiska system med detektor uppstår en retroreflex, vilket innebär att i stort sett all strålning som träffar optiken fokuseras och reflekteras tillbaka. Vid retroreflektion är signalen typiskt ca 100000 gånger starkare än vid diffus reflektion.

Varnarsystem inom det elektrooptiska området

Funktionen för ett varnarsystem är att detektera hot som är på väg mot varnarsystemet och varna den plattform som skall skyddas om det inkommande hotet. Ett typiskt varnarscenario innehåller följande delar; en plattform som skall skyddas, ett omedelbart hot och till sist en omgivande miljö innehållande ett varierande antal objekt och händelser som skall särskiljas från hotet.

UV-baserad robotskottvarnare

En varnare som bygger på detektion av strålning inom UV-området kan detektera strålning från en robotflamma så länge roboten har motorn igång. Robotflamman strålar i våglängdsbandet 0,2 till 0,3 µm (det solblinda området där ingen naturlig strålning finns). Varnaren består av en stirrande detektormatris. En varnare har normalt en täckningsgrad på ca 90° x 90°. För att få fullgod täckning behövs därför flera varnare.

IR-baserad robotskottvarnare

IR-baserade robotskottvarnare är uppbyggda enligt motsvarande princip som UV-baserade varnare, men här detekteras den termiska strålningen (3–5 µm) från såväl robotskrov (aerodynamisk uppvärmning) som flamma. En fördel med det valda våglängdsbandet är att bakgrundens inverkan inte blir så stor, vilket minskar falsklarmsrisken. Liksom hos den UV-baserade robottskottvarnaren har den IR-baserade varnaren normalt en täckning på ca 90° x 90°, vilket enligt ovan kräver flera varnare för täckning runt om.

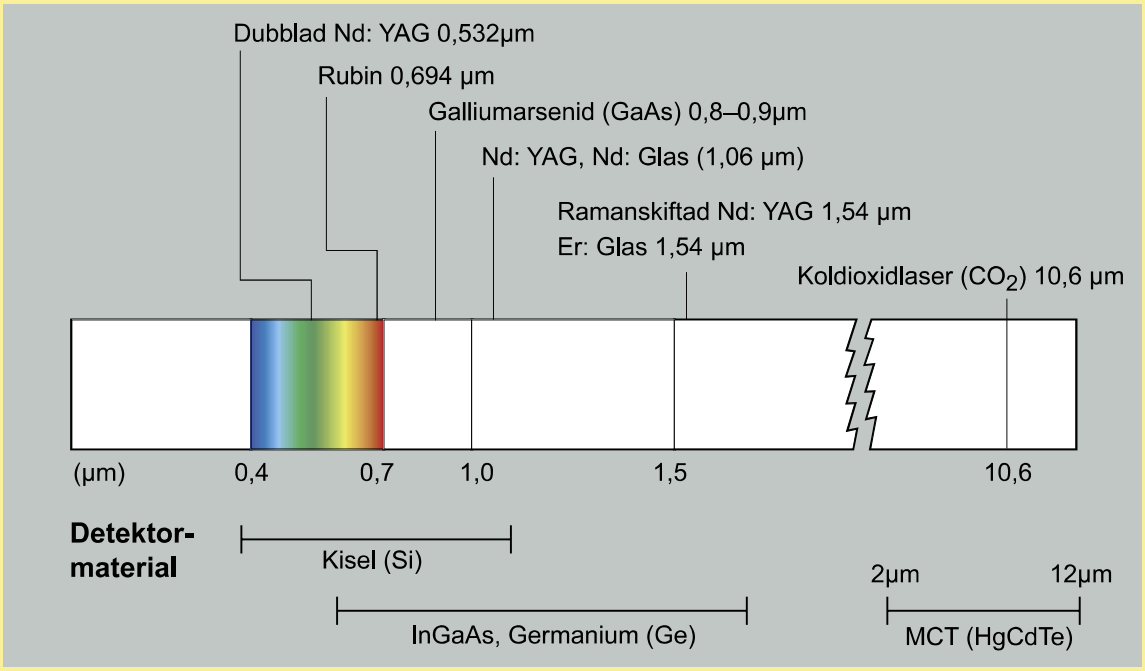
IRST

Ett annat system, vilket bl.a. kan upptäcka inkommande missiler, är IRST (Infrared Search and Track). Systemet avsöker 360° i horisontalplanet och upp till 90° i elevation (med ett eller ett par svep) med frekvensen några Hz och en geometrisk upplösning kring 0,1 mrad. Om ett mål upptäcks kan systemet övergå till snabb avsökning av ett litet område kring målet.

Laservarnare

Laservarnare har som namnet antyder till syfte att detektera laserstrålning. Detta kompliceras bl.a. av det stora våglängdsområde inom vilket hotlasrar kan uppträda, det krav på stor vinkeltäckning som finns för att ge förvarning oberoende av var hotet befinner sig samt det faktum att många lasersystem endast sänder mycket korta pulser. Se även faktaruta.

Laservarnare



Figur F16. Vanligt förekommande hotlasrar samt olika detektormaterial som utnyttjas i laservarnare.

Laservarnare för detektion av pulsade laseravståndsmätare och semiaktivt laserstyrda bomber/robotar började utvecklas på 1970-talet. De första varnarsystemen var enkelt uppbyggda med ett fåtal detektorelement. Hotriktningen angavs i vinkelsektorer om typiskt ±45° och presenterades på displayer med lysdioder eller liknande.

Hotbilden är numera betydligt mer omfattande och ett större antal våglängder utnyttjas. En modern laservarnare skall kunna detektera och klassificera laseravståndsmätare, laserbelysande system och ledstrålelasrar. Nya hot såsom "viskande" laserradar för exempelvis 3D-avbildning i målsökarsystem och olika typer av stör- och bländlasrar kommer ytterligare att öka kraven på framtidens laservarnare. Figur F16 visar våglängder för de vanligast förekommande hotlasrarna samt de detektormaterial som används i laservarnare för att detektera dessa våglängder. I framtiden kommer säkerligen tonbara lasrar, där våglängden kan väljas fritt inom ett stort våglängdsband, att utnyttjas av vissa hotsystem.

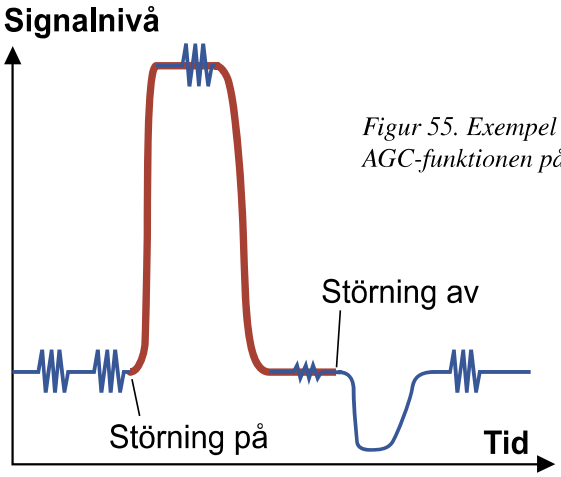
Laservarnare kan skilja på laseravståndsmätare, laserbelysare och ledstrålelasrar genom att mäta pulsrepetitionsfrekvensen (PRF) hos inkommande laserpulser. Mer avancerade system har möjlighet att utnyttja biblioteksfunktioner för identifiering av specifika system, framför allt för ledstrålestyrda robotar. Förutom PRF kan även våglängdsinformation utnyttjas för identifiering. Att noggrant bestämma våglängden hos en hotlaser i en laservarnare är komplicerat och görs vanligtvis inte. En del varnare utnyttjar optiska filter för att bestämma hotlaserns våglängd i ett antal våglängdsband.

Vinkeltäckningen för en laservarnare kan variera beroende på vilken plattform som skall skyddas (fordon, helikopter, fartyg, m.m.). Vanligtvis krävs 360° vinkeltäckning i azimut. Invisningsnoggrannheten varierar från ± 45° för de enklaste systemen ned till ± 1° för de mer avancerade. Avståndsmätar- och belysarlasrar har smal laserlob (typiskt 0,1-1 mrad). Spridning i atmosfären medför dock att en laservarnare kan detektera laserstrålning från avståndsmätare och laserbelysare även om de riktas tiotals meter vid sidan av laservarnarens sensor.

Det finns en rad potentiella falsklarmskällor såsom solreflexer, blixtljus, mynningsflammor, eldsvådor och elektromagnetisk interferens. Falsklarmsfrekvensen är normalt låg (<1 på 24 timmar) trots krav på hög känslighet, stor dynamik, brett synfält och god våglängdstäckning. Undertryckning av falsklarm sker med avancerad signalbehandling. Tekniker som utnyttjas är bland annat tids-, koherens- och våglängdsdiskriminering.

Elektronisk attack

För verkan mot elektrooptiska system finns ett antal olika system och olika tekniker. Det kan vara enkla fysiska skenmål, avskärmande rök eller vattendimma som döljer det skyddade objektet, facklor som genererar en IR-signatur för att vilseleda hot, eller lasersystem som kan störa eller t.o.m. förstöra målsökare.



Figur 55. Exempel på hur signalen från AGC-funktionen påverkas vid störning.

Blinkstörare

Blinkstörare är tänkta att användas mot retikelsystem av generation 1 och 2, se figur 50. Principen är att utnyttja en xenonlampa som blinkar med stark intensitet (ca 2-3 ggr plattformens intensitet). I signalbehandlingslogiken är det blinkstörarens vågform som skall skapa fel avseende fas, amplitud eller frekvens i den modulerade signalen. Detta svarar mot en ändring i följesignalen och således fås styrautomaten i missilen att avvika från rätt kurs. För att lyckas med detta måste blinkstöraren stråla inom det spektralområde som målsökaren använder. Vidare måste pulserna från blinkstöraren ta sig genom målsökarens retikel. Dessutom måste blinkstörarens pulser utnyttja frekvenser som tilllåter att de passerar genom bandpassfilter och förstärkare. Slutligen måste blinkstöraren stråla med tillräcklig energi för att garantera att den överväger signalen från målet i målsökaren.

Blinkstörning kan delas in i AGC-störning och modulationsstörning. AGC (Automatic Gain Control, automatisk förstärkningskontroll) används för att hålla en elektrisk signals spänningsnivåer i ett lämpligt intervall, genom att ändra förstärkningen av signalen. Vid AGC-störning önskas störning nära AGC:ns egenfrekvenser. Störningen drar upp signalnivån, så att då störningen avbryts blir målföljaren tillfälligt blind, se figur 55. Vid modulationsstörning gäller det att störa nära retikelns modulation och rotationsfrekvens. I praktiken finns tre typer av modulerande blinkstörare mot retikelsystem: Bärvågsfrekvensstörare (eng. noise jammer) som genererar en uteffekt med hög energi på kontinuerlig basis; Amplitudmodulerande störare (eng. deception jammer) som är tänkta att utnyttjas mot specifika retikelmålsökare och således kräver djupare kunskaper om hotet; Rotations- och nutationsstörare (eng. reticle-spin jammer) som genererar pulser (ca 10 ggr plattformens intensitet) kring målsökarens rotations-/nutationsfrekvens.

Laserstörare

Avsikten med laser som motmedel mot optiska sensorer är att störa, blända, vilseleda eller förstöra sensorn för att avvärja eller motverka ett hot. Laser som motmedel mot sensorer kallas ibland antisensorlaser. En sådan kan exempelvis användas för skydd av plattformar genom att störa ut ett hotsystems målföljare. För att störningen skall lyckas krävs att lasern utnyttjar en våglängd som ligger i det våglängdsintervall inom vilket sensorn är känslig.

Invisning och inriktning av en antisensorlaser kan ske på olika sätt,

Figur 56 Laserbländning av en IR-kamera inom området 3-5 µm. De tre bilderna åskådliggör, från vänster till höger, det ostörda fallet, laserstörning inom synfältet, samt laserstörning 6 grader utanför synfältet.

alltifrån manuell inriktning (jfr gevär) till information från TV- eller IR-sensorer, robotvarnare, lasermålföljare, laserradar, laservarnare eller radarsystem. Antisensorlasern kan även vara sammonterad med eldrörsvapen eller robotlavett. Den kan då utgöra en tillsatsfunktion när målet är bortom vapnets räckvidd. Laserstörare utnyttjas vanligtvis tillsammans med optikspanare.

2D- och 3D-skenmål

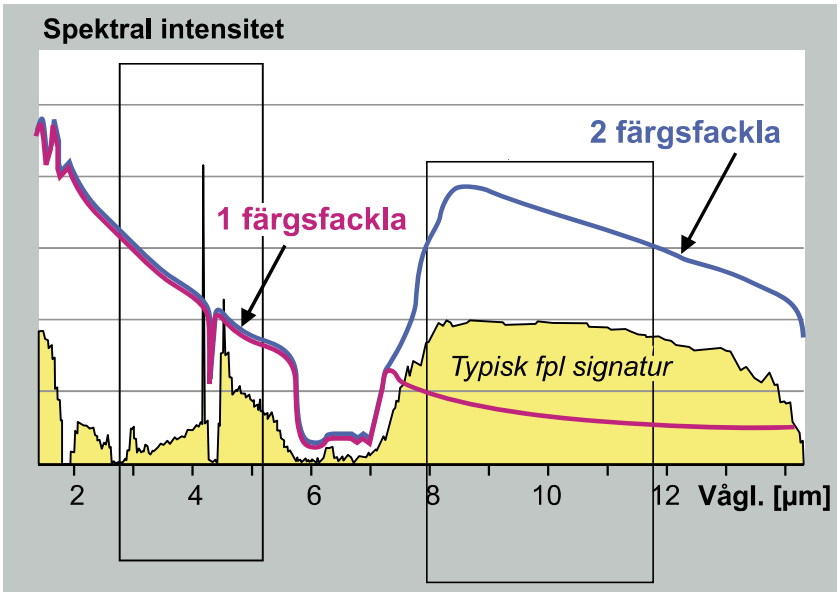
Skenmål kan vara konstruktioner som fysiskt efterliknar skarpa objekt och som är två- eller tredimensionella. Även enkla skenmål kan ha effekt, något som exempelvis visades under kriget i Kosovo. Skenmålens signaturer bör överensstämma med de verkliga objekten både avseende våglängd och signalstyrka. Utöver en visuell signatur krävs främst en relevant signatur inom IR-området. Det är möjligt att med relativt enkla hjälpmedel åstadkomma detta, exempelvis genom att använda enklare värmekällor. Denna typ av skenmål är främst tänkta att användas mot spaningssensorer. Som skenmål mot laser kan prismor som ger retroreflex användas. Dessutom kan man vilja att skenmålet skall simulera aktiv sändning som överensstämmer med vad det verkliga målet skulle ha genererat.

Facklor

En typ av skenmål som huvudsakligen är avsedda för icke bildalstrande elektrooptiska system är facklor. Facklor är pyrotekniska anordningar, vilka emitterar sin energi i målsökarens våglängdsområde (från början avsedda för att skydda flygplan). Syftet är att de skall framstå som mer lockande för en målsökare än det riktiga målet och få roboten att jaga facklan istället för det riktiga målet. För att åstadkomma detta måste facklorna ha en spektral fördelning anpassad till hotsensorn. Facklornas intensitet skall dessutom vara högre än målets. (De tidiga retikelmålsökarna styrde mot tyngdpunkten av målen inom synfältet.) Vidare önskas en snabb uppblomningstid (tid från detonation eller fällning till det att facklan har full intensitet) och en tillräckligt lång brinntid. För att en eller flera facklor skall få effekt krävs dessutom att de separerar från målet så pass mycket att roboten inte kommer nära målet. Därför bör utskjutningsvinkeln vara anpassad till hotriktningen. Utvecklingen av facklor har gått från enfärgsfacklor (anpassade för ett våglängdsintervall) till facklor för att få övervikt i två våglängdsband, se figur 58. Det finns även facklor som består av pyrofort material. När pyrofort material kommer i kontakt med syre antänds det. Facklor används för skydd av flygplan, helikoptrar och fartyg.

Figur 57. Flygplan 37 (Viggen) som fäller fackla.

För att skydda svenska ytstridsfartyg mot elektrooptiska system har ett motmedelssystem (MASS, Multi Ammunition Softkill System) införskaffats. För att ge effekt i flera våglängdsområden består varje skenmålsgranat av såväl en fackla som en remslast (för verkan inom radarområdet). För att skydda fartygen skjuts ett antal skenmålsgranater för att kunna generera ett tillräckligt stort skenmål i avsikt att kunna lura målsökare. Exempel på detta visas i figur 59.



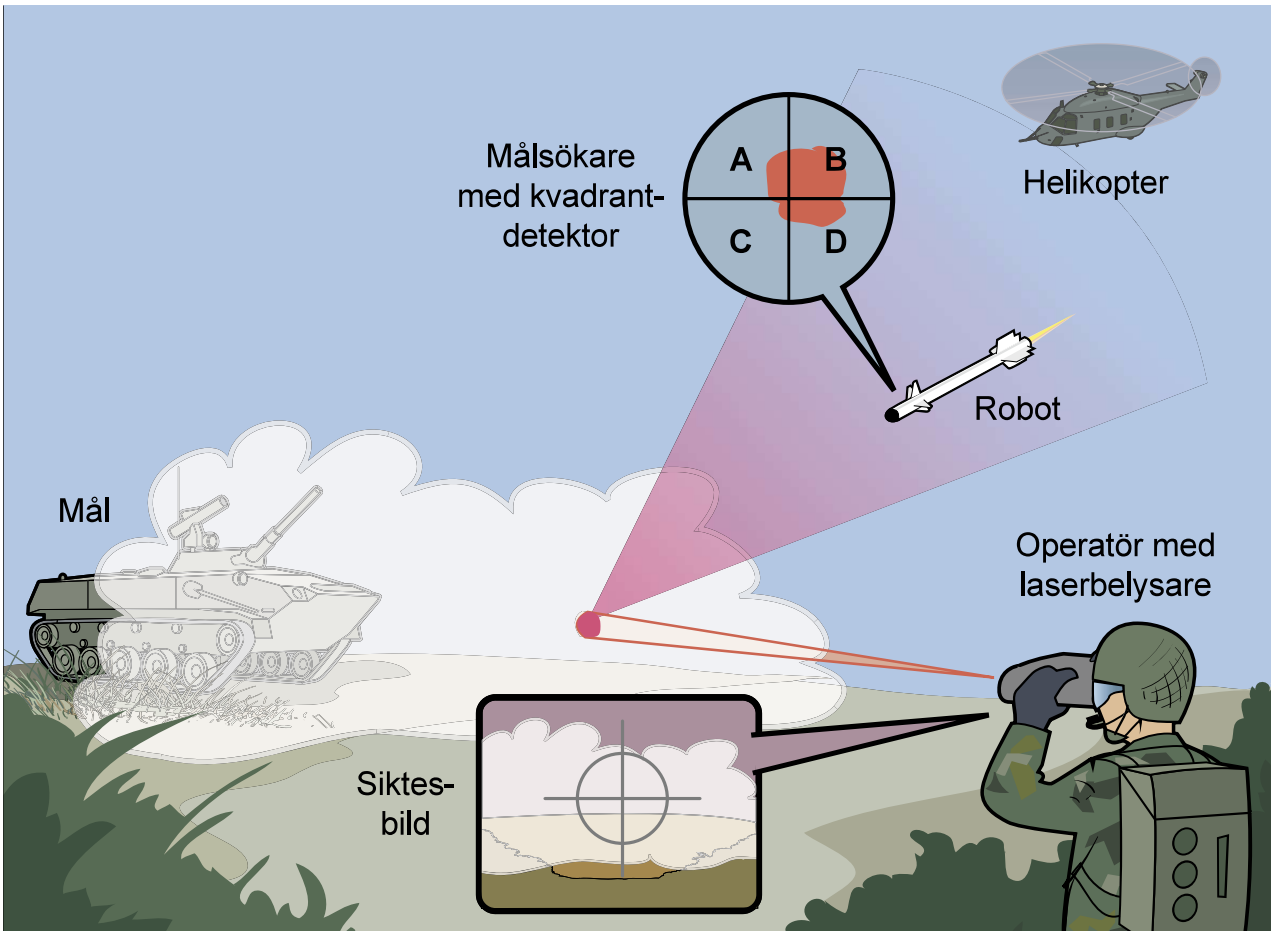
Figur 58. En- och tvåfärgsfackla i jämförelse med typisk flygplanssignatur.

Figur 59. Fartyg som skjuter ut 16 skenmålsgranater. Notera att skenmålet tidvis täcker fartyget. Foto: BUCK Neue Technologien GmbH.

Avskärmning

För att uppnå avskärmning måste siktlinjen mellan målsökare och plattform brytas. Detta kan åstadkommas med rök, facklor eller vattendimma som täcker den plattform som skall skyddas. Av stor vikt är att partikelstorleken hos den avskärmande röken/vattendimman minst motsvarar den våglängd som skall dämpas ut. Önskas en rök som kan dölja inom 8-12 µm bör storleken hos partiklarna i röken ligga kring 10 µm. I stridsfordonsfallet sitter normalt två kastare på tornet, en på vardera sidan om eldröret. En insats består av 6-8 rökgranater och kompletteras med undanmanöver. Om hotet är en laserstyrd robot kan två effekter erhållas med en rökinsats, dels att siktlinjen skyms, vilket ger problem för den operatör som skall följa målet, dels att laserstrålen reflekteras i rökmolnet, vilket ger upphov till en geometrisk felvisning som kan leda till att roboten missar, se figur 60.

Vattendimma åstadkoms genom att vatten trycks ut ur ett antal munstycken anpassade för att skapa vattendroppar av rätt storlek. Exempel på detta visas i figur 61.

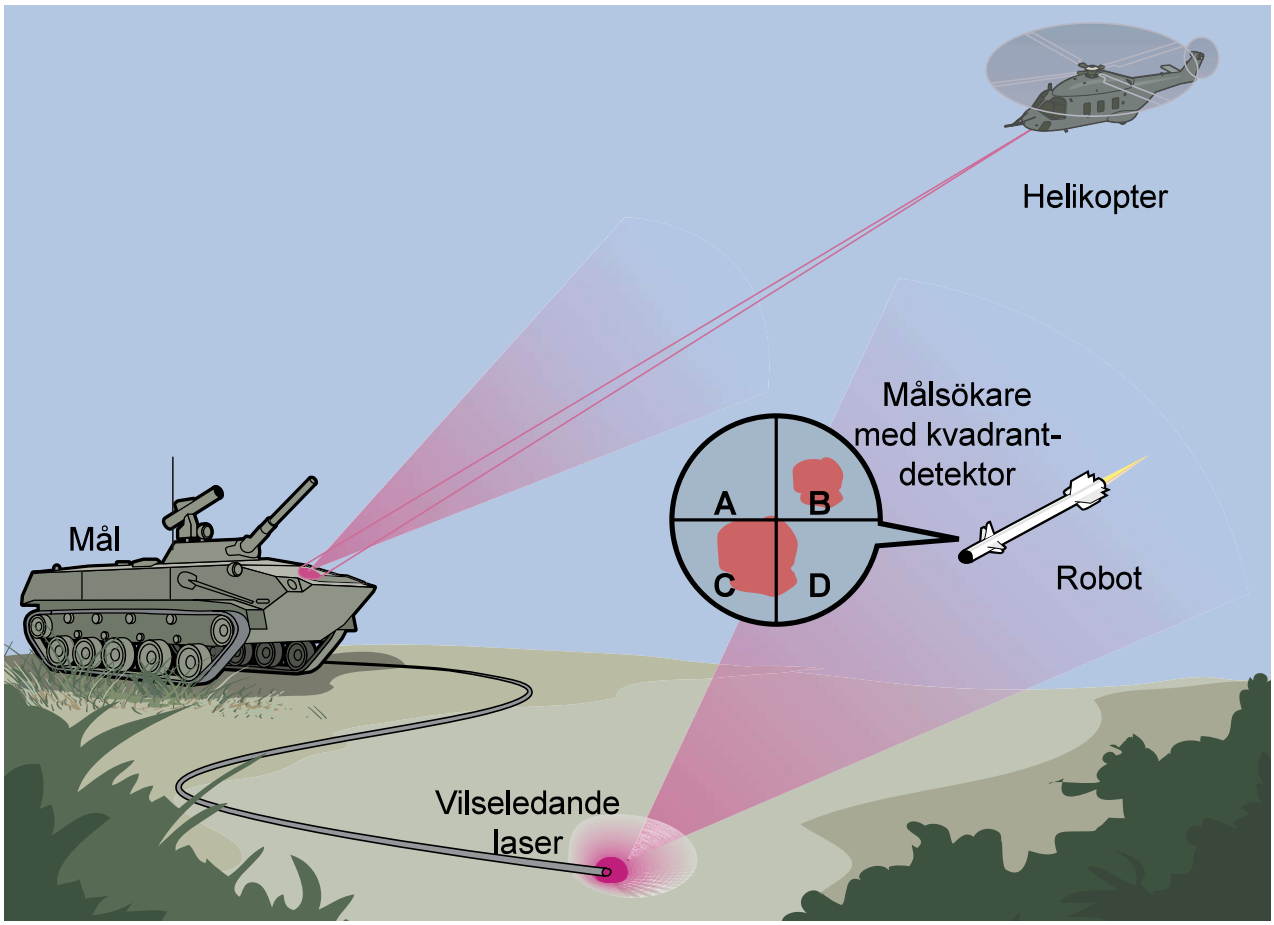


Figur 60. Rök i avskärmande syfte. Här uppnås förflyttning av reflektionspunkt för laserstrålen och skymd siktlinje för siktesbild.

Figur 61. Vattendimma applicerat på stridsfordon 90. Här avskärmas vagnen från hot uppifrån, t.ex. slutfasstyrda granater. Det tar ca tre sekunder innan stridsfordonet är helt täckt av vattendimman (bilden till höger).

Vilseledande laser

Vilseledning av laserbelysare kan åstadkommas genom att utnyttja data från en laservarnare för att med egen laser vilseleda laseravståndsmätare och laserbelysarsystem. När laserpulsen från en avståndsmätare upptäcks kan den egna lasern sända ut en laserpuls som ger laseravståndsmätaren ett extra falskt avståndssvar. En operatör eller ett system kommer på detta sätt att störas. Ett laserbelysarsystem skulle kunna vilseledas genom att skenfläckar skapas för de lasersökande vapnen att styra mot. För att detta skall lyckas krävs en flexibel laser som kan replikera den kod som laserbelysaren har. Kopplas lasern till en optisk fiber som läggs ut (se figur 62) kan ett effektövertag skapas för den falska laserpunkten.



Figur 62. Vilseledning av laserbelysarsystem.

Elektronisk protektion

Det finns ett antal sätt att skydda elektrooptiska system mot den motverkan de kan utsättas för.

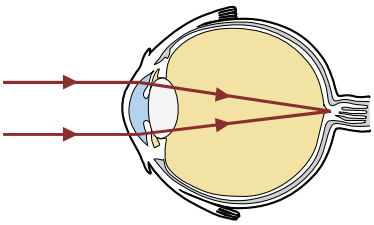
En passiv målsökare kan t.ex. skyddas mot elektrooptiska motmedel genom implementering av störskydd i målsökaren. Gemensamt för alla störskyddsmetoder är att målsökaren först måste detektera att den är utsatt för motverkan. Detta kan åstadkommas på flera sätt, t.ex. genom att detektera snabba ökningar i den inkommande strålningsenergin (intensitetsstegring), att studera energiförhållandet i flera våglängdsområden (multispektral), att detektera följehastighetsändringar (kinematisk), eller att detektera flera mål inom synfältet (spatial).

När målsökaren detekterat att den är utsatt för störning vidtar den sina motåtgärder. Några exempel på sådana åtgärder är blind styrning/minnesgång, ”seeker-push-pull”, ”seeker-push-ahead” och sektordämpning. Blind styrning eller minnesgång betyder att roboten blint (d.v.s. på den senaste kursen) fortsätter sin bana en kort tid i förhoppningen att motmedlet (men inte målet) skall vara borta ur synfältet då styrningen återupptas. Push-pull innebär att målsökaren drivs mot det svagare målet från det starkare. Push-ahead innebär att målsökaren ”i förväg” styrs ut i målets senast bestämda färdriktning då ett motmedel detekterats och att man samtidigt hoppas att motmedlet skall hamna utanför synfältet. Sektordämpning innebär att t.ex. den nedre halvan (det är oftast där motmedlen befinner sig) av detektorns synfält dämpas, vilket får till följd att detektorns utsignal påverkas mindre av motmedlet.

Under senare år har laserhotet ökat allt mer, till följd av det ökande antal lasrar och lasertillämpningar som blivit aktuella i militära sammanhang. Skydd är relevant redan mot det hot som oavsiktlig laserbelysning innebär. Exempel finns t.ex. på att helikopterbesättningar utsatts för belysning med relativt enkla lasrar i samband med internationella insatser. När lasersystem dessutom ges mer avsiktliga vapentillämpningar blir behovet av laserskydd än mer accentuerat.

Laserbelysning riktad mot ögon kan, förutom bländning, medföra synnedsättning eller blindhet. Hornhinnan och linsen kan liknas vid ett brännglas som fokuserar laserstrålningen till en punkt på näthinnan, så att intensiteten där förstärks i storleksordningen 100000 ggr. Detta innebär, trots att näthinnan inte är mer skadekänslig än hud, att den skadas betydligt lättare. Vid användning av förstorande optik, t.ex. kikare eller sikte, ökar skaderisken ytterligare eftersom koncentrationen på näthinnan då blir ännu kraftigare. Motsvarande förhållanden gäller även för elektrooptiska sensorer, men där är det ett objektiv som fokuserar strålningen på en detektor, vilken således motsvarar ögats näthinna.

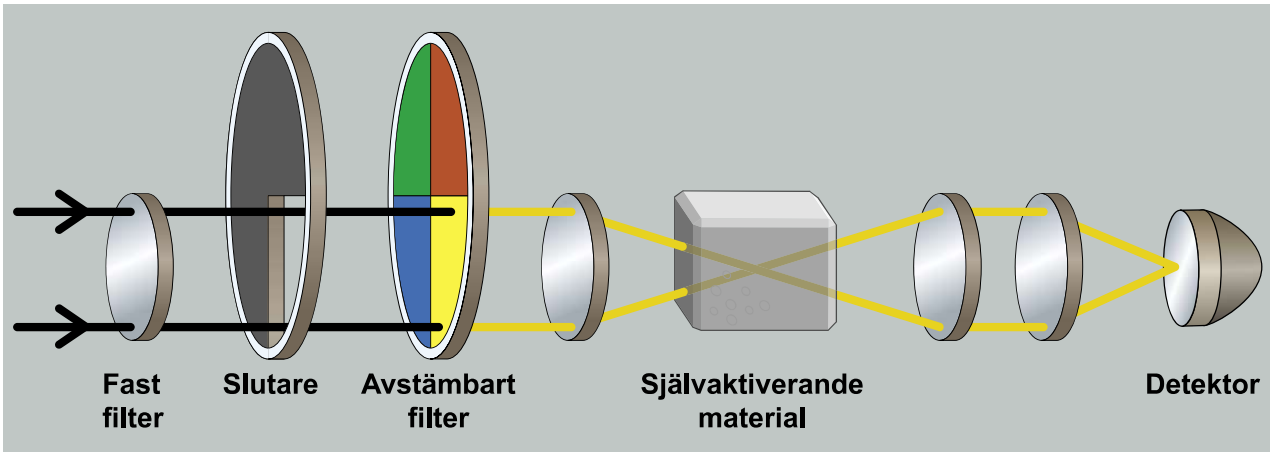
Användning av optisk utrustning ger alltså, på grund av kraftigare



Figur 63. Ögats lins och hornhinna koncentrerar laserstrålningen.

fokusering, en ökad risk för ögonskador. Dessutom ökar risken för att bli upptäckt genom optikspaning, vilket i sin tur ökar risken för laserangrepp och därmed också risken för skada. Taktiska skydd går därför ofta ut på att minska upptäcktsrisken, bl.a. genom att minimera exponeringen av den optiska utrustningen, och att i övrigt begränsa den visuella kontakten med omvärlden. Även vilseledning, exempelvis genom utnyttjande av skenmål, kan ses som ett taktiskt skydd.

De tekniska skydden kan i sin tur delas in i tre kategorier: statiska, styrda och självaktiverande. Statiska skydd förändras inte under ett laserangrepp. Exempel på sådana skydd är fasta spektrala filter och indirekt seende. Fasta filter utgör ett gott skydd under förutsättning att hotvåglängden är känd. De är också användbara för att filtrera bort våglängder utanför det våglängdsområde som utnyttjas av sensorn eller ögat. Därigenom reduceras risken för upptäckt och skada orsakad av strålning som inte kan detekteras. Indirekt seende, via t.ex. videokamera och bildskärm eller bildförstärkare, kan skydda ögon även mot okända våglängder. Indirekt seende ger dock sämre upplösning och mindre synfält än



Figur 64. Figuren illustrerar ett skyddskoncept mot framtida 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 placerat i ett mellanfokus. Om det avstämbara filtret snabbt kan ställa om till att blockera laservåglängden, fås ett skydd mot efterföljande laserpulser, och det blir möjligt att fortsätta informationsinhämtningen. I vissa fall kan det vara önskvärt att utestänga alla våglängder, vilket görs genom att aktivera slutaren.

direkt seende, samt oftast försämrat färgseende. Elektrooptiska sensorer är dessutom ofta mer känsliga för bländning än ögat.

Skydd mot störning av en optisk sensor från laserkällor utanför synfältet kräver att ströljuset i sensorns optik minimeras. Detta åstadkoms genom omsorgsfull konstruktion, t.ex. med bländare och motljusskydd, samt med lågspridande och lågreflekterande ytbeläggningar. När det gäller skydd mot upptäckt måste också detta beaktas då sensorn konstrueras, för att på så sätt åstadkomma en konstruktion med minimal lasermålarea.

Styrda skydd, t.ex. slutare och styrbara filter, kan förändra sina optiska egenskaper på kommando från en yttre styrsignal, t.ex. från en laservarnare. Exempel är slutare och avstämbara filter. 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 avstämbart filter skall i princip ge samma skydd mot laser som slutare men släppa igenom ofarliga våglängder. Då erhålls ett skydd som gör det möjligt att använda optiken trots kontinuerlig belysning.

Självaktiverande material skyddar automatiskt ögat eller sensorn utan påverkan från yttre styrsignaler. Transmissionen för dessa s.k. optiskt ickelinjära material minskar med ökande intensitet hos ljuset. Dessa effekter kan vara såväl reversibla (optiska begränsare, vilka begränsar den transmitterade strålningstätheten till en maximal nivå) som irreversibla (optiska säkringar, vilka bryter strålgången permanent när intensiteten når en viss nivå). För att de självaktiverande skydden skall fungera krävs ofta höga energitätheter, varför de måste placeras i ett mellanfokus. De kan skydda mot skada eftersom de är mycket snabba (<<ns), men ej mot störning och bländning.

Operativt finns idag (2005) statiska filter.

HPM OCH STÖRNING AV NAVIGERINGSYSTEM

I de fyra föregående avsnitten har telekrig mot kommunikationssystem och sensorsystem beskrivits. Det finns dock tillämpningar som inte låter sig klassas enligt denna uppdelning. Ett exempel på detta är HPM (High Power Microwaves), ett annat är störning av navigeringssystem.

HPM beskrivs endast kortfattat här då området finns väl beskrivet i skriften ”FOI orienterar om elektromagnetiska vapen och skydd”.

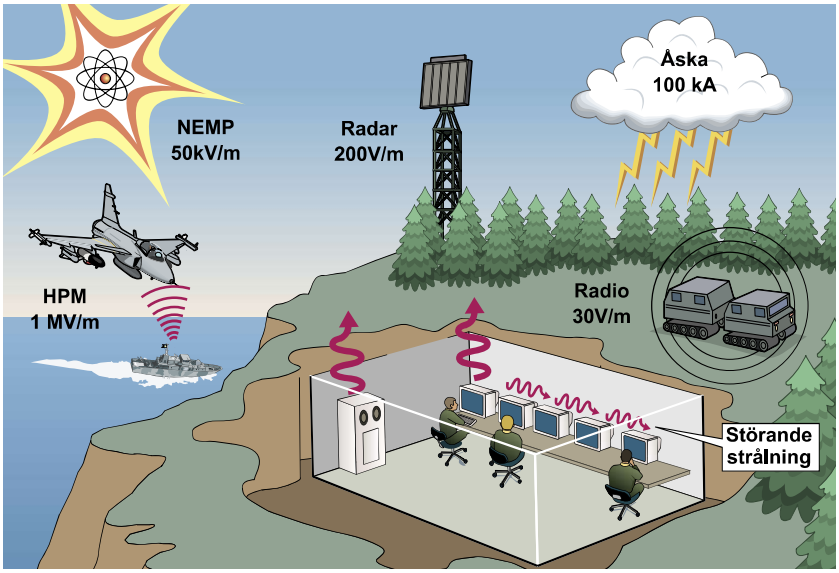
För störning av navigeringssystem avgränsas beskrivningen till att omfatta störning av satellitbaserade navigeringssystem, då dessa dels bedöms vara de som ges flest tillämpningar, dels är de som torde vara lättast att störa. Störning av navigeringssystem delar många likheter med störning av radiokommunikation, då det är radiosignaler det handlar om. Funktionen är dock en annan än ren kommunikation, och då många, såväl civila som militära, system utnyttjar navigeringssystem förtjänar området ett eget avsnitt.

HPM

HPM, utgör en delmängd av den totala elektromagnetiska miljön, se figur 65. Eftersom konventionella mikrovågskällor, såsom radarkällor, har pulseffekter på högst 100 MW anges detta ibland som en undre gräns för vad som avses med ett HPM-vapen. Följande typiska parameterrymd kan uppställas:

- Frekvens: 0,3 – 300 GHz.
- Utstrålad effekt: upp till 10 GW.
- Pulslängd: upp till 1 µs.

HPM-vapen delas ofta in i kategorierna smal- respektive bredbandiga (Ultra Wide Band, UWB). Bredbandiga källor, som generellt har en enklare konstruktion än de smalbandiga, har korta pulslängder, typiskt 0,1 – 1 ns, och korta verkansavstånd, typiskt 100 meter. Smalbandiga källor har pulslängder på typiskt 0,1 – 1 µs, och kan ha verkansavstånd på flera mil. Båda typerna av HPM-källor drivs med

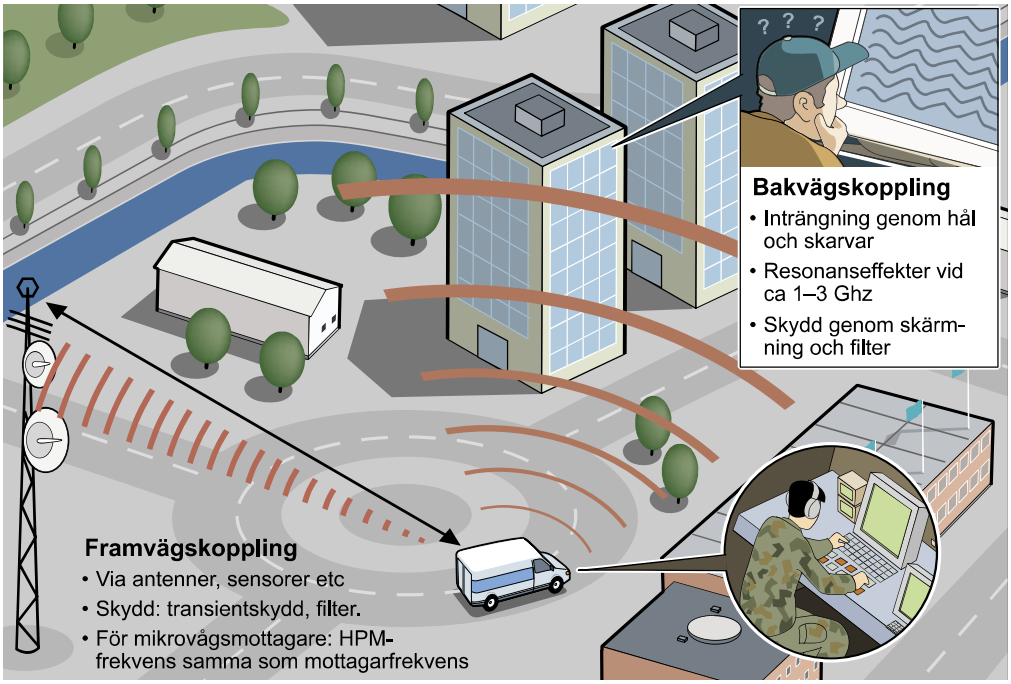


Figur 65. Den elektromagnetiska miljön för militära system.

korta högspänningspulser från ett pulsgenererande system som är integrerat med strålkällan.

Huvudsyftet med HPM-vapen är att störa eller förstöra funktionen hos elektronikberoende system. Även en kortvarig störning, t.ex. av ett flygplans styrsystem, kan leda till katastrofala konsekvenser. HPM-strålningens inträngning i målet kan ske på två sätt, via bakvägskoppling eller via framvägskoppling, se figur 66.

Sedan de första insikterna under det tidiga 70-talet att HPM kan störa och förstöra elektronik har



Figur 66. De två typerna av inträngning i målet för HPM – framvägs- respektive bakvägskoppling.

stora resurser satsats på forskning avseende såväl på HPM-vapen som skydd mot HPM. Rykten om att HPM-vapen har testats vid internationella konflikter, t.ex. under Gulfkriget 1991 och på Balkan 1999, har cirkulerat under flera år. USA och dess allierade bedöms ha operativa HPM-vapen till 2010. I Tyskland finns redan bredbandiga HPM-källor. Som exempel på tillämpningar anges att stoppa fordon eller att störa ut all informationsinhämtning i en terroristcentral.

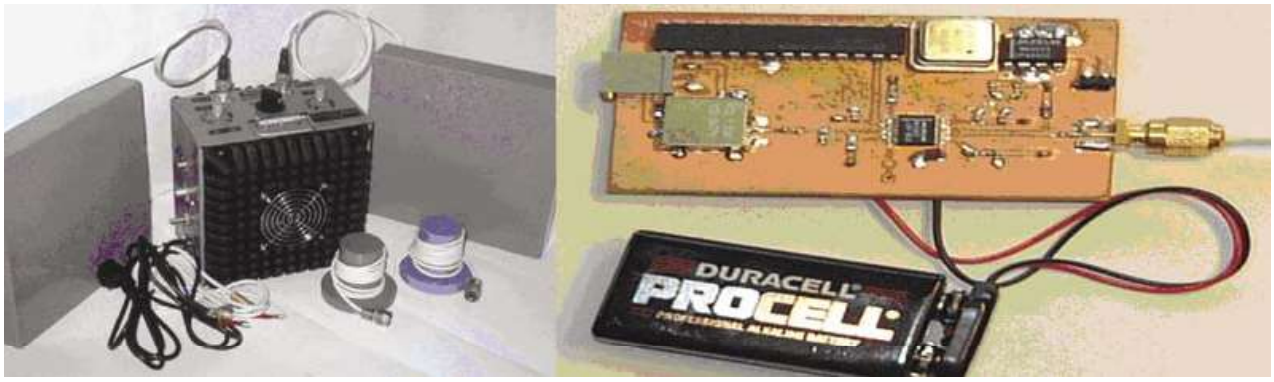
Beträffande aktuellt skyddsläge kan sägas att det i allmänhet, militärt såväl som civilt, saknas krav på skydd mot HPM. Det finns dock vissa viktiga undantag för moderna militära system. Flygplan och helikoptrar, även civila, är skyddade mot intensiv radarstrålning och har därmed också ett gott grundskydd mot HPM. Det skall också påpekas att oskyddad utrustning, t.ex. i civila sammanhang, kan vara hyggligt skyddad p.g.a. att den är placerad på ett stort avstånd från en tänkbar förövare.

Lite tillspetsat kan man säga att skyddsmetoder för bakvägskoppling finns kommersiellt tillgängliga medan kydd mot framvägskoppling kräver skräddarsydda lösningar, om sådana alls existerar. I det senare fallet innebär applicering av skydd oftast att nyttofunktionen försämras. Särskilt för bakvägskoppling är problematiken att verifiera ett systems tålighet mot HPM svårhanterlig. Orsaken är HPM-hotets stora parameterrymd och systemens vanligtvis höga komplexitet.

Störning av navigeringssystem

Genom att använda ett satellitnavigeringssystem (GNSS – Global Navigation Satellite System) fås på ett enkelt sätt position, hastighet och tid med hög noggrannhet och tillgänglighet. Tre sådana system kommer inom en snar framtid att finnas verksamma – GPS, Galileo och GLONASS. Systemen har många fördelar jämfört med mer traditionella navigeringssystem och metoder, t.ex. kommer användarna att ha täckning i princip var de än befinner sig på jorden. Användning och utveckling av nya tjänster baserade på GNSS ökar kontinuerligt, vilket leder till ett ökat beroende av GNSS såväl militärt som civilt. En viktig tillämpning är synkronisering och tidhållning i t.ex. mobila kommunikationssystem och finansiella system.

Idag är GPS, som drivs av USAs Department of Defense (DoD),



Figur 67. Två GPS-störare. Den vänstra bilden visar en rysk militär störare från Aviaconversiya med 20 W uteffekt och störavstånd på över 200 km. Kostnaden för störsändaren har uppgivits till 40000 USD. Den högra bilden visar en enkel GPS-störsändare framtagen av FOI, med uteffekt 100 mW och ett störavstånd på någon kilometer.

det enda satellitnavigeringssystem som är fullt operativt. GPS är uppbyggt kring passiva mottagare som tar emot signaler utsända av 24 satelliter. Satelliternas banor kontrolleras och korrigeras från markstationer utspridda över jordytan. Systemet genomgår en modernisering, vilket kommer att medföra fler civila signaler med förbättrad prestanda och även nya militära signaler med större störskydd. Det europeiska systemet Galileo beräknas vara operativt runt 2008 och erbjuda både öppna samt reglerade positionstjänster med motsvarande prestanda som för det moderniserade GPS. GLONASS är den ryska motsvarigheten till GPS, vilken idag inte är fullt operativ. Det har emellertid aviserats att systemet skall bli operativt igen.

De civila och militära positionstjänsterna (signalerna) är mycket lätta att störa ut och därmed blir system som använder GPS eller annat GNSS mycket sårbara. En GPS-mottagare kan påverkas av avsiktliga och oavsiktliga störningar. De oavsiktliga störningarna är främst övertoner från sändare såsom radio, radar, TV etc., vars frekvenser ligger i närheten av GPS-frekvenserna. En annan källa till degradering av precisionen är jonosfärstörningar, vilka ökar vid solfläcksmaximum.

En enkel störare med en uteffekt på 20 Watt kan slå ut en civil GPS-mottagare på avstånd över 200 km. Troligen är militära GPS-mottagare avsevärt svårare att störa ut, bl.a. på grund av att de är bättre konstruerade. Det finns militärt utvecklade GPS/GLONASS-störare att köpa, eventuellt även för privatpersoner. Det är också relativt enkelt att konstruera en GPS-störare. De komponenter som behövs kan köpas från elektronikfirmor. Från Internet kan ett flertal utförliga beskrivningar på störsändare, med tillhörande kopplingsscheman, laddas ner. På vissa hemsidor beskrivs var, när och hur GPS skall störas för att ge största effekt. Slutsatsen är att tillgängligheten på GPS-störare är stor.

Oavsiktlig störning (interferenser) har inträffat, vilket visar på systemets känslighet. Ett hot som på senare tid har identifierats är terroristhot mot den civila användningen av GPS och då riktad mot t.ex. civilt flyg. Konsekvenserna av en sådan attack kan vara allt ifrån svåra med dödlig utgång till incidenter med liten påverkan, beroende på situationen i vilken störningen inträffar.

När det gäller störning av militär användning av GPS har USAs försvarsdepartement bekräftat förekomsten av störattacker under det senaste Irakkriget (OIF, Operation Iraqi Freedom). I ett försök att skydda Bagdad mot attacker av GPS-styrda vapen placerades störare på höga torn runt staden. Enligt USAs försvarsdepartement misslyckades störningen och GPS-styrda vapen kunde användas för att bekämpa störsändarna. Störstrategin som användes för att skydda Bagdad utformades på ett felaktigt sätt. Vapnen som användes för att slå ut störarna använde i de flesta fall någon typ av störskyddssystem. En stark utveckling av störskydd för GPS-mottagare har skett och pågår. Det finns ett antal tekniker som kan användas för att skydda en GPS-mottagare. Ett taktiskt skydd är att utnyttja flera navigeringstekniker, t.ex. satellitnavigering i kombination med markbunden radionavigering, trögnetsnavigering och/eller terrängnavigering. Detta förbättrar dessutom precisionen.

Även om telekrigföring i mycket handlar om växelverkan mellan tekniska system (en duell mellan medel och motmedel) är det viktigaste ändå hur denna växelverkan fortgår i en taktisk eller operativ kontext. Ett sätt att sätta in tekniken i dess sammanhang är att diskutera telekrig på förbandsnivå. Därigenom kommer fokus att läggas på förbandsresurser för genomförande av telekrig och hur dessa växelverkar med resten av försvarsmaktens resurser.

En annan viktig tillämpning är telekrig för egenskydd. Detta kan handla såväl om skydd av enstaka plattformar som om egenskydd av förband. I egenskyddsfallet talas det i allmänhet om varnar- och motverkanssystem (VMS), d.v.s. integrerade lösningar för att såväl upptäcka hot (varna) som verkställa olika motåtgärder mot dessa hot (motverkan). Motverkan kan handla om störning, vapeninsats eller rena taktiska åtgärder (t.ex. undanmanöver). Här kommer dock fokus att läggas på telekrigåtgärder.

Telekrigförmåga är en nödvändighet vid nationella och internationella operationer och en förutsättning för framgång i väpnad strid. Telekrig är ett vapen bland andra.

I samband med diskussionen av förbandstillämpningar av telekrig och egenskydd är det också centralt att beskriva hur telekrigsystem kan bidra till successivt förbättrat underlag avseende hotet. En viktig roll i detta sammanhang har de resurser som ansvarar för uppdatering av telekrigbibliotek.

Telekrigföring måste enligt ovan ses i ett sammanhang. I detta ingår också att diskutera angränsande verksamheter, speciellt sådana där avgränsningen inte är helt entydig. Ett exempel på en sådan verksamhet är signalunderrättelsetjänst, vilken i mycket utnyttjar samma teknik och metoder som elektronisk stödverksamhet (ES), men där syfte, avnämare och tidsförhållanden skiljer sig åt. Ett annat sådant område är informationsoperationer, vilket snarast är en vidsträckt kostym i vilken bl.a. telekrig kan inrymmas. Detta diskuterades i inledningen. Ett tredje är signaturanpassningsteknik (SAT), vilket kan handla om allt från traditionella kamouflagenät till färger som anpassar sig till omgivningen.

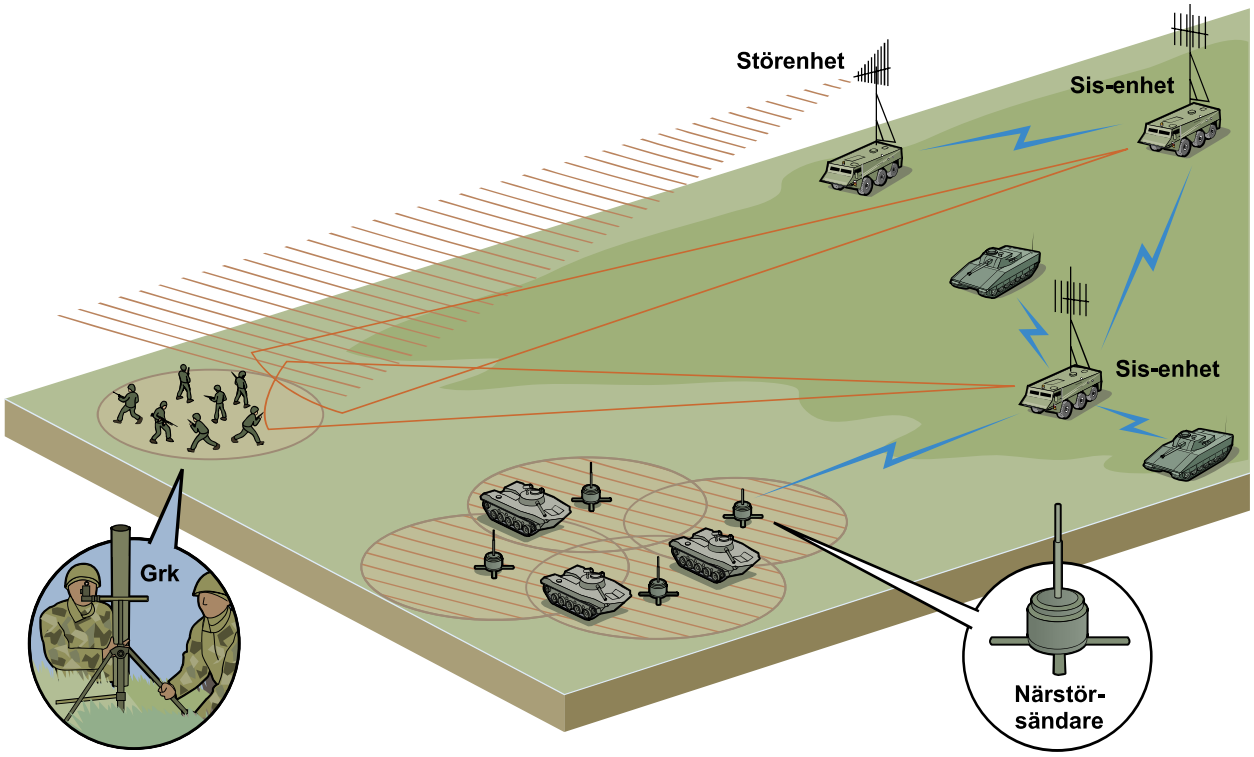
Tillämpningar

Telekrig på förbandsnivå

Telekrig har en roll i alla sammanhang för alla förband. Att inte röja sig i onödan, d.v.s. genomförande av elektronisk protektion, ingår i normalt taktiskt uppträdande. Därutöver finns speciella förband – telekrigförband – som har telekrigföring som huvuduppgift. Genom telekrigförband kan motståndarens positioner, rörelser och aktiviteter identifieras och störas.

Exempel på telekrigföring är avlyssning av en aktörs radiotrafik. Härigenom är det möjligt att dels bearbeta avlyssnade meddelanden, antingen direkt eller efter dekryptering, dels genom analys av annan information som ingår i de emitterdata man samlat in – t.ex. vem som sänder till vem, hur ofta sändningarna skett eller var i geografin emittern lokaliserats – möjliggöra identifiering av förbandstyp, förbandsstorlek, pågående verksamhet m.m.

Telekrigförband kan genomföra elektronisk attack mot motståndarens kommunikations-, radar-, navigations- eller andra typer av system, vilket kan reducera motståndarens ledningsförmåga. Störningen kan ha olika syften, som att försvåra eller förhindra motståndarens kommunikation, vilseleda honom genom falsk signalering, nedsätta hans kapacitet, störa ut signaler för radarsystem som används för invisning av robotar, eller undertrycka spaningsradarstationers täckningsområden för att dölja egna förbands rörelser och verksamhet.



Figur 68. Televapenförband signalspanar och stör. Närstörsändare kan placeras ut i förväg. Närstörsändare kan antingen arbeta i automatmod eller fjärrstyras. Framtagen lägesinformation från televapenförbandet ges till andra förband.

Under pågående insats kan telekrigförband bidra med såväl ES, bl.a. lägesbestämning, avlyssning, klassificering och dokumentation som EA, t. ex. störning av en aktörs ledningsnät. Markbaserade telekrigförbands förmåga att under lång tid kunna övervaka stora ytor är viktig för uppbyggnad av den gemensamma lägesbilden. ES över hav (mot fartyg) och i luft (mot flyg) medger ännu större lägesbestämningsområden. Flygburna och sjögående telekrigplattformar övervakar mycket stora täckningsområden varifrån telekriginformation kan inhämtas och delges på motsvarande sätt.

Figur 68 och 69 visar exempel på utnyttjande av telekrigförmåga.

Kontroll av utnyttjandet av det elektromagnetiska spektrumet

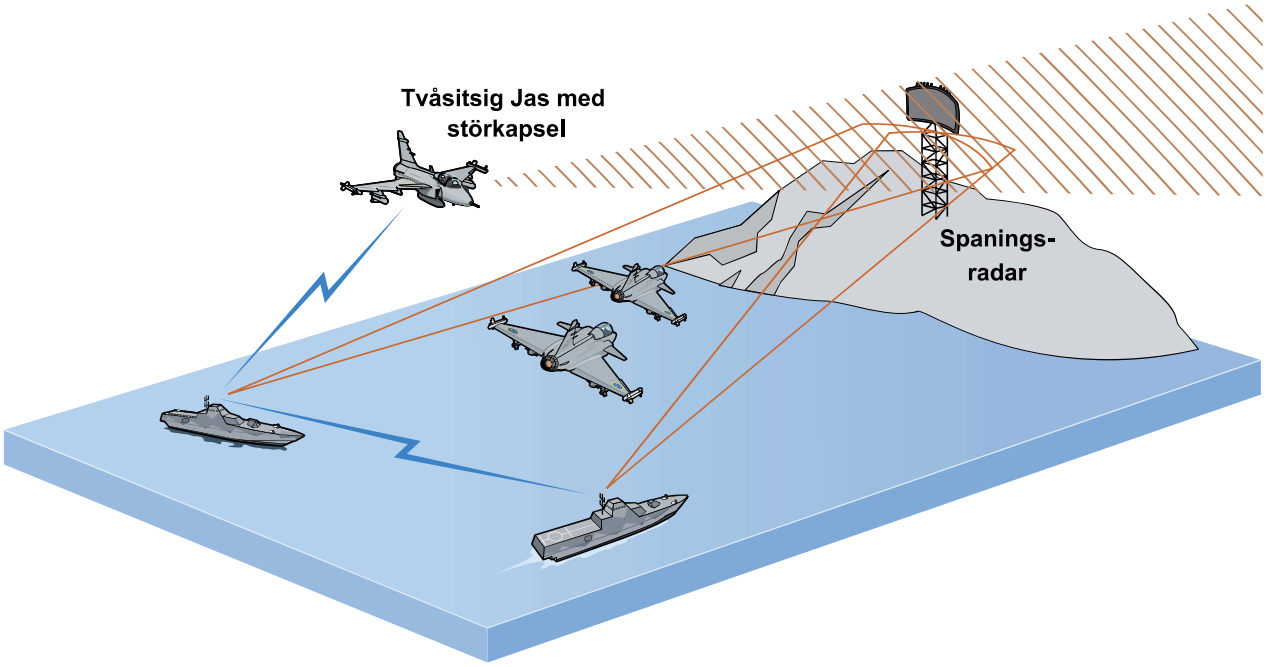
Telekrigföring har också en viktig roll när det gäller att kontrollera utnyttjandet av det elektromagnetiska spektrumet, t.ex. för att undvika elektromagnetiska konflikter (mellan egna system eller mellan egna och eventuella koalitionspartners system). Det handlar här om att tillse att olika system inte på ett ogynnsamt sätt påverkar varandra, genom att t.ex. oavsiktligt störa varandra. Om sådan påverkan kan undvikas kommer systemens samlade effekt att kunna utnyttjas effektivare. Det innebär också att vi kan styra vilken information vi vill att motparten skall uppfatta, 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, i takt med att antalet militära och civila system som utnyttjar det elektromagnetiska spektrumet ökar och i takt med att vi allt mer samverkar med andra nationer inom ramen för fredsfrämjande insatser.

För att kunna kontrollera den elektromagnetiska emissionen krävs mycket god kunskap om egna och koalitionspartners system samt även motsvarande kunskap om civila system inom operationsområdet. För att klara det krävs det dessutom att vi har utvecklade metoder för snabbt utbyte av telekrigdata. För att samordna förbands och systems emissioner över tiden behöver vi också utvecklade metoder för att snabbt styra dessa emissioner, kontrollerad emission (EMKON).

Egenskydd

För att kunna sända ut förband i internationella insatser krävs i allmänhet egenskydd (det är ofta ett krav för att överhuvudtaget få deltaga). Detta gäller bl.a. VMS



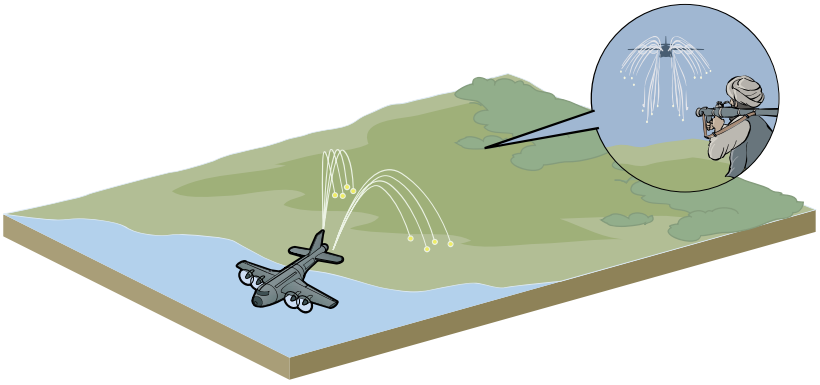
Figur 69. Två korvetter genomför taktisk signalspaning mot radarstationer. Läget rapporteras vidare så att medstörning kan genomföras i syfte att öppna fönster för SEAD.

till fartyg, flygplan och stridsfordon, något som bl.a. uppmärksammades när svenska Hercules-flygplan (TP 84) skulle utnyttjas för transporter ner till Bosnien. Även laserskyddsåtgärder för personal har diskuterats, bl.a. mot bakgrund av att amerikanska helikopterbesättningar blev belysta med laser i Bosnien. Dessa krav aktualiseras för Försvarsmakten i och med Sveriges vilja att delta med resurser i multinationella fredsfrämjande insatser.

Ibland används termen varnar- och motmedelssystem istället för varnar- och motverkanssystem. Skillnaden mellan dessa består egentligen i att medan motmedelssystem i huvudsak omfattar telekrigsystem för att motverka hotet avser motverkanssystem alla tänkbara system (även t.ex. automatkanoner) som kan bidra till denna motverkan. I princip skulle man kunna vidga detta ytterligare och tala om sensor- och motverkanssystem, då även andra sensorer än varnare kan bidra till att ett hot upptäcks och mäts in.

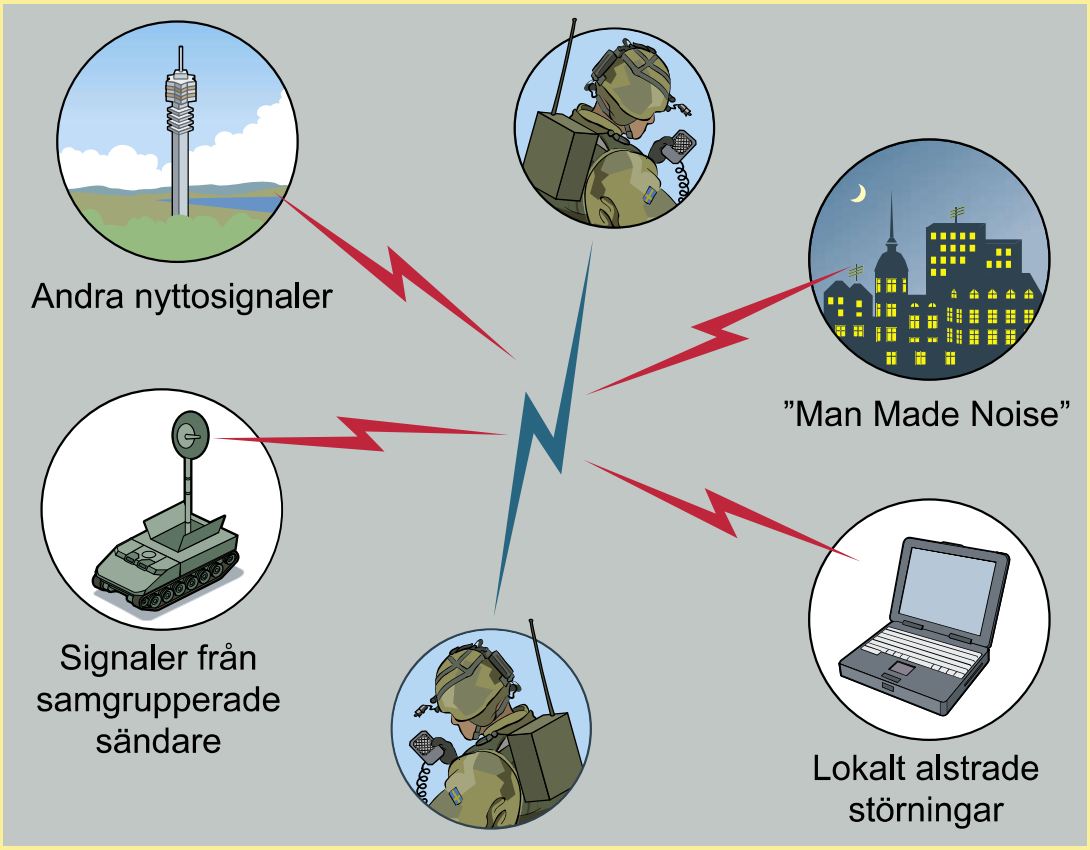
Generellt ställs allt högre krav på förmåga att hantera allt mer kvalificerade hot från den egna plattformen. Detta ställer stora krav på telekrigföring och angränsande verksamheter, bl.a. signaturanpassning och underrättelseinhämtning. Moderna plattformar utrustas med olika typer av varnare (radarvarnare, UV- eller IR-baserade robotskottvarnare, laservarnare) och motverkanssystem (inom telekrigområdet bl.a. antisensorlasrar, radarstörare, facklor och remsor) för att kunna utföra sina uppgifter i en kvalificerad hotmiljö. I vissa fall ges också understöd med speciella telekrigresurser, t.ex. speciellt utrustade störflygplan som skall släcka ut motpartens luftvärnsradar under en insats.

Ett fungerande varnar- och motverkanssystem bygger på att hotet upptäcks, klassificeras och identi-



Figur 70. TP 84 Hercules som detekterat en inkommande robot och släpper facklor.

Telekonflikter

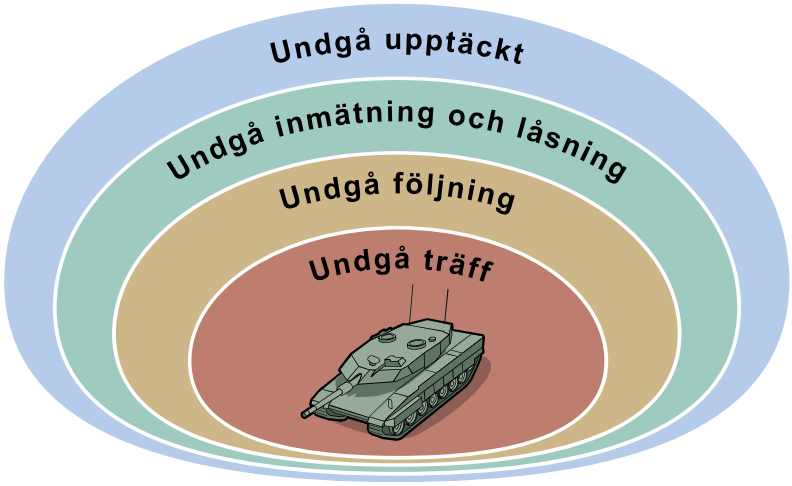


Figur F17. Telekonflikter är störningar kopplade via antennsystemet.

Telekonflikter uppstår när egna system genererar störningssignaler som kopplas via antenner till samlokaliserade system, se figur F17. Telekonflikter har varit ett känt problem inom främst flyg- och sjöstridskrafter under 30-40 års tid. En mängd telekonflikter finns rapporterade från olika militära operationer. Typiskt uppstår telekonflikter när enheter från olika vapenslag eller olika nationer genomför gemensamma insatser. Exempelvis har telekonflikter förekommit vid landning med arméflyg på hangarfartyg. Andra typiska problem är när marinens vapen använts på flygvapnets flygplan och vice versa. Inför operation Uphold Democracy i Haiti 1994 använde USA arméhelikopter av typ UH-60 Black Hawk på hangarfartyget USS Eisenhower. Den vapenlast som användes inom armén var inte testad för signalmiljön runt hangarfartyg, varför fartygets radar inte kunde användas. Detta innebar operativa begränsningar. Black Hawk har dessutom råkat ut för ett antal haverier (ett 20-tal omkomna totalt) där elektromagnetiska störningar misstänks vara orsaken. I samband med internationella insatser i forna Jugoslavien har telekonflikter förekommit mellan flygburna störningssändare och artilleriradar. Vid testflygning i sydvästra USA med den obemannade Global Hawk uppstod en telekonflikt med en markstation på samma frekvens som signalerna för fjärrmanövreringen. Detta resulterade i att självförstörelsemekanismen utlöstes på farkosten, vilken således sprängdes. Allmänt kan sägas att de system som kan vara svårast att få telekonfliktfria i militära plattformar är varnar- och motverkanssystem (VMS). Detta beror på att man i dessa system både vill kunna lyssna och störa i samma frekvensband. Typiska exempel på telekonflikter är mellan radarvarnare och radarstörare/spaningsradar på flygplan och fartyg. En praktisk erfarenhet är att telekonfliktarbete på komplexa militära plattformar oftast är omgärdat av hög sekretess då hemliga data om många system är nödvändiga att känna till. En medvetenhet om detta samt tillgång till kvalificerade experter ökar möjligheten att identifiera och eliminera telekonfliktrisker redan i konstruktionsskedet.

fieras i så pass god tid att motverkan i olika former kan initieras och påverka hotet. I vissa situationer krävs det dock att man genomför preventiva åtgärder, m.a.o. innan möjlighet till identifiering eller klassificering av hotet funnits.

Skyddet av en plattform kan illustreras med hjälp av en ”lökmodell”, se figur 71. Den beskriver i detta fall på ett schematiskt sätt de olika faserna i bekämpning av ett objekt där ett VMS kan ha betydelse. För att undgå bekämpning är första steget att undvika att bli upptäckt. I denna fas är framför allt en riktigt utformad signaturanpassning (SAT) av stor betydelse. Under förutsättning att varning om att spaning sker kan erhållas kan ett VMS i detta skede, i form av till exempel utlagd rök eller vattendimma, eller inom radarområdet maskerande radarstörning, komplettera signaturanpassningsåtgärder. Å andra sidan kan t.ex. rök också vara röjande och leda in spaning, d.v.s. röken indikerar 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. Här har VMS i kombination med signaturanpassning stor betydelse. Likaledes kan ett VMS med hjälp av olika former av störande eller vilseledande motverkansåtgärder bidra till att i nästa steg förhindra följningen. I det sista skedet, då det handlar om att undgå att bli träffad, är motverkansåtgärder nödvändiga för att bekämpa eller lura målet. (Till motverkan räknas här även åtgärder som inte ingår i telekrigföring, t.ex. att hotet bekämpas med robot, automatkanon eller artilleri.) Motverkansåtgärderna kan också kombineras med taktiska åtgärder, vilket t.ex. för ett flygplan kan innebära att rems- eller fackelfällning kombineras med undanmanöver.



Figur 71. Schematisk bild över ett tänkt skalskydd för stridsfordon. Varnar- och motverkanssystemets viktigaste uppgift är att förhindra inmätning, pålåsning och följning av sikten och målsökare för att därmed undvika träff. För att undgå upptäckt utnyttjas i första hand signaturanpassning, eventuellt i kombination med VMS.

I alla dessa steg kommer alltså varnare att kunna ge information om hotet, medan motverkanssystemen är möjliga verktyg för att bryta de olika länkarna i kedjan från upptäckt till träff.

Det finns en stark koppling mellan signaturanpassning och motmedel. Är plattformen väl signaturanpassad krävs mindre insatser av motmedel för att dessa skall få övervikt. Av stor betydelse är att känna till egna signaturer, dels för att veta vilka krav som skall ställas på motmedel, dels för att kunna optimera den uppvisade signaturen mot ett hot.

Signaturanpassning

Syftet med signaturanpassning är att hindra sensorerna att göra sitt jobb, d.v.s. att upptäcka, klassificera och identifiera. Detta kan ske genom att minimera kontrasten mellan ett objekt och dess bakgrund. Metoden för att göra detta benämns signaturanpassningsteknik (SAT). I naturen är kameleonten känd för att kunna anpassa sig efter sin omgivning, den används därför ofta som symbol för teknikområdet. Signaturanpassning är inget självändamål, utan är tillsammans med alla andra skyddsåtgärder en del i överlevnadskonceptet. Med SAT avses förutom konstruktionsåtgärder och grundåtgärder i form av ytbeläggningar, även tilläggsmaskering och tillfälliga åtgärder för kontrastreduktion.

Figur F18. Kameleont. Bild: Midjourney 2023

Den optiska signaturen beror av den yttersta ytans egenskaper och vinkel i förhållande till ljus och omgivning. Den termiska signaturen beror dessutom av objektets temperatur. Radarsignaturen beror främst av objektets form samt utformningen och integrationen av alla yttre komponenter som luckor, vapen, utblickar och sensorer. Eftersom formen är så viktig är det uppenbart att robusta och kostnadseffektiva signaturreducerande åtgärder måste beaktas tidigt i utvecklingsarbetet. Till objektsignatur räknas också strålningsbidrag från avgasmoln och spårbildning.

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. Objektets funktion sätter dock gränser för formgivningen.

Figur F19. Fartyg av Visbyklass. Foto: Försvarets Bildbyrå/ Peter Nilsson.

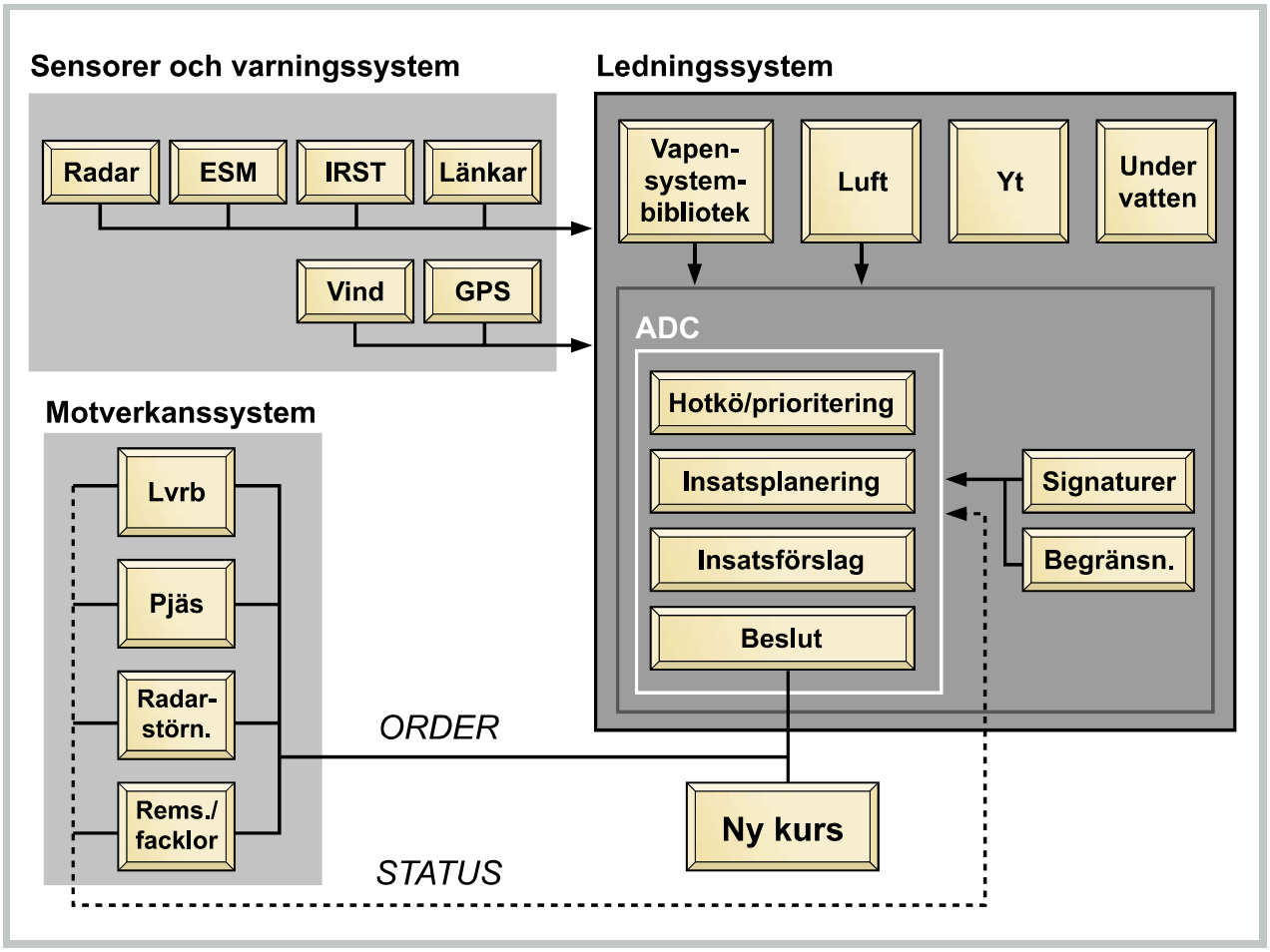
Inom optikområdet är det ytbeläggningens reflektionsegenskaper och objektets form som bestämmer signaturen. Valet av maskeringsbeläggning påverkar indirekt såväl den termiska som radarsignaturen. För att signaturanpassningen skall bli bra i det termiska området måste man kontrollera värmen från interna källor, t.ex. motorer. Detta kan göras genom isolering, skärmning eller ventilation. Man kan också arbeta med s.k. lågemissiv ytbeläggning. En termisk sensor "ser" då en kallare yta. Heta avgaser kan kylas eller skärmas. Inom radarområdet väljer man att reflektera bort strålningen eller att absorbera den i RAM (radarabsorberande material). Håligheter kan ge direktreflexer varför de ägnas särskild omsorg. De kan täckas med galler som skall ligga i samma plan som ytterytan eller invändigt kläs med RAM.

Kända objekt där SAT har utnyttjas för att nå taktiska fördelar är bl.a. det amerikanska stealthflygplanet F117 samt den svenska fartygsklassen VISBY.

Ett VMS kan principiellt sägas bestå av varnare, motverkanssystem samt bibliotek. I många fall är ett VMS integrerat i plattformens ledningssystem. Ett exempel från fartyg visas i figur 72.

Ett exempel på en plattform med ett kvalificerat varnar- och motverkanssystem är den amerikanska attackhelikoptern AH-64 Apache Longbow. Exempel på system som kan ingå i detta VMS framgår av figur 73.

Attackhelikoptrar är genom att de uppträder på låg höjd i en miljö med många hot och att de även har ett relativt svagt skalskydd (d.v.s. det är potentiellt möjligt att bekämpa dem med relativt många vapensystem) i hög grad beroende av ett effektivt egenskydd i form av ett VMS. Ett ytterligare system som diskuteras för helikoptrar är DIRCM (Directed InfraRed CounterMeasures), se faktaruta DIRCM.



Figur 72. Koordinering mellan ADC (Air Defence Controller), ledningssystem och motverkanssystem. Sensor- och varnarinformation går via vapenbibliotek till ADC där inkommande hot prioriteras (vanligtvis närmast först). Insatsplanering innebär att de olika motverkanssystemen ger förslag på insats samt tillhörande överlevnadssannolikhet. I samband med detta utnyttjas kännedom om egen signatur och begränsningar/prestanda (om det finns några) samt aktuella vindförhållanden. De framtagna överlevnadssannolikheterna för respektive motverkanssystem jämförs och det mest optimala alternativet väljs. Systembeskrivningen i figuren är ett exempel hämtat från Kkv Visby.

DIRCM

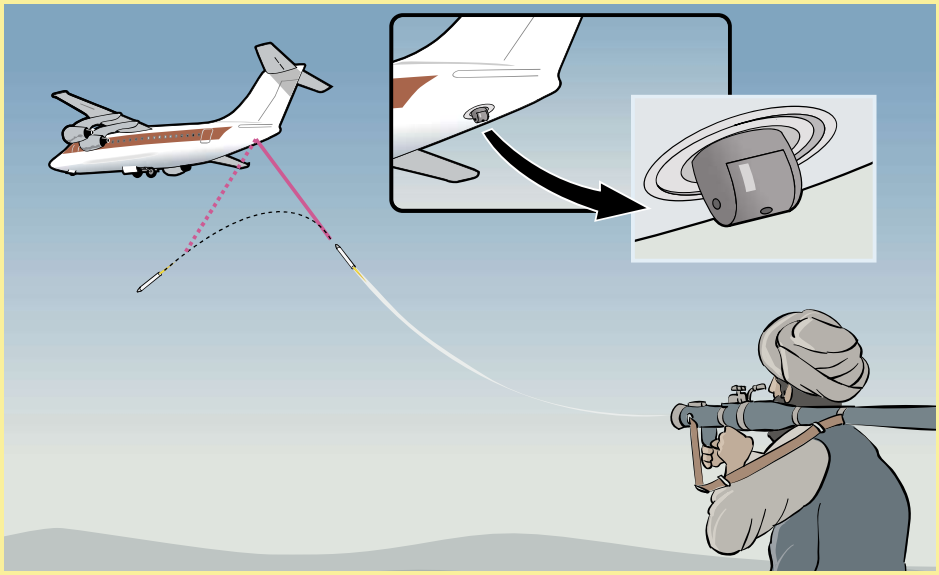
Ett av de största hoten i olika typer av konflikter är manburna robotar med IR-målföljare (s.k. MANPADS, MAN Portable Air Defence Systems). Exempelvis är de ett hot i samband med start och landning av transportflygplan samt vid övervakning på låg höjd som utförs med helikopter. Internationellt (i främst USA, Tyskland, Storbritannien, Frankrike och Ryssland) pågår stora forsknings- och utvecklingsinsatser för att skydda flygplan och helikoptrar mot detta hot. De motverkanssystem som tas fram kallas för DIRCM (Directed InfraRed CounterMeasures). Dessa innefattar en robotvarnare (MAWS - Missile Approach Warning System) tillsammans med någon form av motmedelsinsats, t.ex. riktad IR-bestrålning från s.k. blinkstörare eller laser. Robotvarnaren kan detektera robotflamman. Denna detektion kan ske med antingen en UV-baserad varnare, vilken kan detektera roboten under den inledande delen av dess bana (boostfasen), eller en IR-baserad varnare, vilken kan detektera den förhöjda skaltemperatur som uppstår p.g.a. luftens friktion mot robotskalet. Varnaren ger en grovinriktning. Invisning av störsändaren inom någon grad kan ske på bråkdelen av en sekund med hjälp av en IR-kamera. Traditionella facklor används fortfarande och är verksamma mot äldre generationers målsökare med enklare retiklar. Utvecklingen går dock mot målsökare som använder flera våglängder eller är bildalstrande, vilket innebär att facklor inte fungerar. Detta motiverar användning av laser mot robothotet.

Dagens DIRCM-system arbetar med öppen loop, d.v.s. det finns ingen laseråterkoppling från den belysta roboten. Framtida system kommer troligen att arbeta med sluten loop. Med detta uppnås flera förbättringar, från möjlighet till direkt målidentifiering via retroreflexmodulation till aktiv följning, vilket kan ske med hög följenoggrannhet (storleksordningen 10-tals mikroradianer). Dessutom ges möjlighet att korrigera atmosfärsutbredningens inverkan via adaptiv optik.

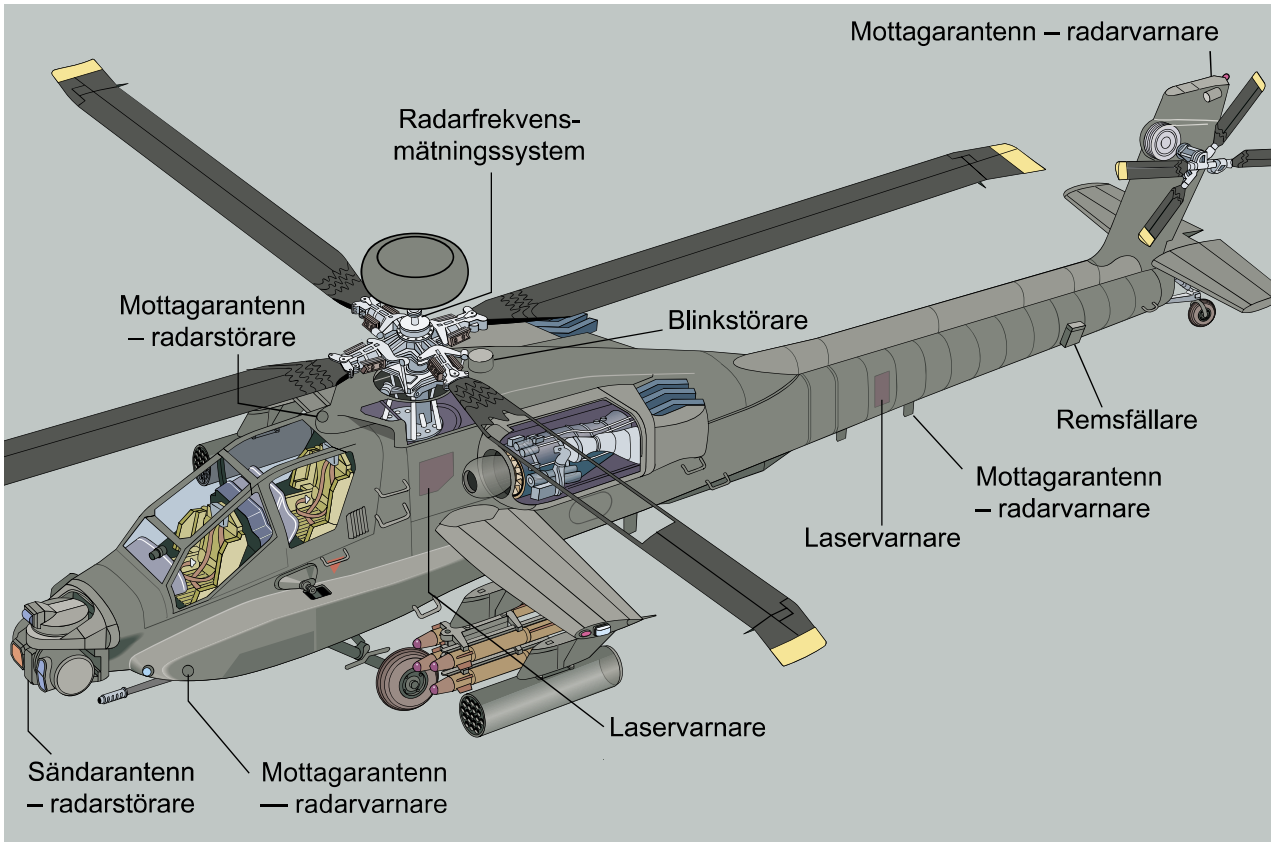
DIRCM-system installeras nu på helikoptrar och transportflygplan. Ett flertal system är under utveckling för snabba flygplan med höga krav på kompakthet.

Hotet mot civila flygplan har aktualiserat möjligheten att förse civila trafikflygplan med DIRCM-system. För civila DIRCM-system studeras även andra alternativ som eskortstörare eller högenergilaservapen som ställs upp nära flygplatser.

Det finns mycket som tyder på att framtida DIRCM-system kommer att vidga sin verkansenvelopp till att lokalisera och störa optiska siktes- och följesystem för att tidigt kunna klippa av hotkedjan. Mycket tyder också på att spaning och igenkänning kan ske med andra sensorer, t.ex. IRST och grindad (2D eller 3D)-avbildning. Ett optiskt hot kan bekräftas genom att detta ger reflexer som indikerar optisk följning av den egna plattformen.



Figur F20. En illustration av MANPADS-hotet. Bilden visar också hur ett DIRCM-system kan tänkas vara installerat på ett civilt trafikflygplan. Hotet är störst vid start och landning.



Figur 73. Exempel på plattforms-VMS för attackhelikoptern AH-64 Apache Longbow.

Dataförsörjning

Deltagande i internationella insatser ställer också krav på utbyte av information om frekvenser och moder hos egna system och även uppdatering av systemens telekrigbibliotek för att hantera nya hot.

Försvarsmaktens telekrigstödenhet, FM TK SE, är den enhet inom Försvarsmakten som idag svarar för systemanpassning av telekrigsystem och telekrigfunktioner i andra system. Det innebär bl.a att tillverka ”bibliotek” till radarvarnare, störsändare och annan telekrigutrustning. Verksamheten vid FM TK SE omfattar alla led i biblioteks- tillverkningen, d.v.s. dataåtkomst, datalagring, produktion, verifiering, validering, distribution, utbildning, analys/ utvärdering och feedback. De främsta leverantörerna av data är, förutom egna förband, FRA, FOI och FMV.

Det är viktigt att framhålla kopplingen till taktik, stridsteknik och soldaten som skall nyttja telekrigsystemet. Det som produceras är kunskap som ger effekt i våra telekrigsystem och därmed möjliggör att insatsförband kan verka på den internationella arenan.

Framtiden pekar på ett ökat behov av telekrigstöd. Nya system inom nya våglängdsområden med behov av dataförsörjning tillkommer. Försvarsmaktens upgifter på den internationella arenan ställer krav på ett snabbt och uthålligt telekrigstöd.

Telekrigbibliotek

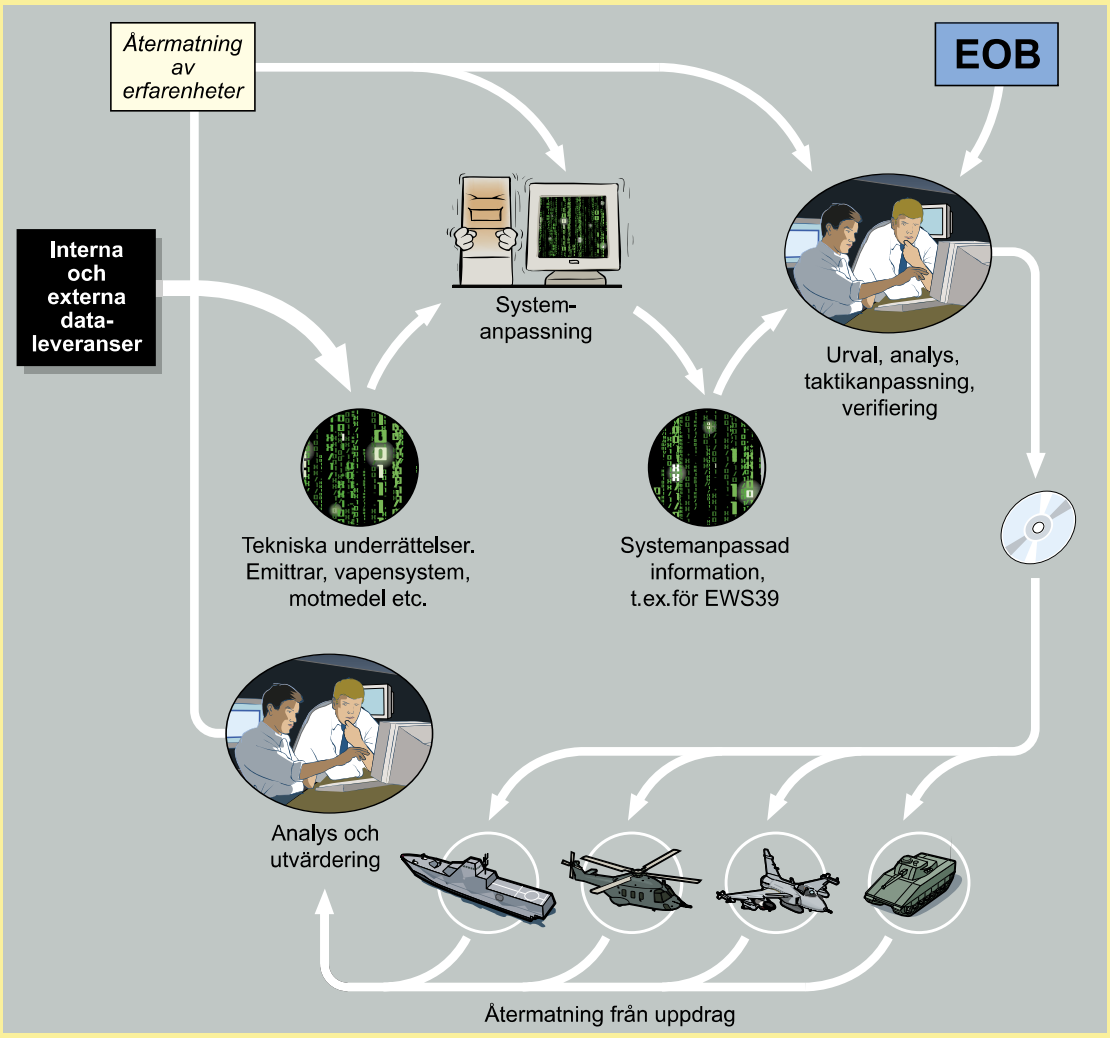
För att moderna varnar- och motverkanssystem skall ha avsedd verkan krävs att de laddas med omvärldsinformation, s.k. telekrigbibliotek. Dessa bibliotek innehåller information dels om emittrar och vapensystem för identifiering, dels om olika motmedelsåtgärder för egenskydd.

Grunden för att tillverka telekrigbibliotek är kunskap inom följande områden:

- Information om vilka vapensystem och emittrar som kan uppträda i den fysiska arenan. Detta omfattar fientliga, egna, neutrala och civila system. Detta kallas med en engelsk term för EOB, Electronic Order of Battle.
- Goda tekniska underrättelser om ovan nämnda vapensystem och emittrar.
- God kännedom om de egna telekrigsystemens funktion och kapacitet.
- Goda taktiska kunskaper.

Telekrigbiblioteken skräddarsys för respektive plattform och uppdragstyp. Det är t.ex. stor skillnad på innehållet i ett bibliotek avsett för ett marint system, där det oftast finns en operatör som tolkar informationen från systemen, och ett bibliotek avsett för ett flygande system, där piloten inte har tid att tolka informationen i samma utsträckning. Det ställs också olika krav på bibliotekens innehåll beroende på uppdragstypen.

Figur F21 visar grovt processen för framtagning av telekrigbibliotek.



Figur F21. En schematisk beskrivning av processen för framtagning av telekrigbibliotek.

Närliggande verksamheter

Telekrigföring är inte något som försiggår isolerat. Förutom att telekrigföring givetvis i alla sammanhang måste koordineras med andra typer av insatser för att undvika att motverka dessa, finns det områden gentemot vilka avgränsningen inte är helt knivskarp. Några sådana områden diskuteras nedan. För informationsoperationer, vilket är ett sådant område, hänvisas till inledningen.

Övrig signalkrigföring

Telekrigföring har kommit att hänföras till det elektromagnetiska spektrumet snarare än till en viss typ av taktisk verksamhet. T.ex. förekommer verksamhet som i sin realisering med medel och motmedel har stora taktiska likheter med telekrig bl.a. i det hydroakustiska området. Generellt brukar de sensortyper som inte hanteras inom telekrigområdet – främst akustik, hydroakustik, seismik och magnetik – samlas under benämningen övrig signalkrigföring.

Ju mer kraven på egenskydd och signaturanpassning drivs på, desto viktigare blir det att hantera även dessa områden samlat med de områden som normalt karakteriseras som telekrigföring. T.ex. kan ett system som signaturanpassats inom IR- och radarområdena 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. Det sagt behandlas de områden som ingår i övrig signalkrigföring inte i denna skrift.

Figur 74. Underrättelseplattform HMS Orion. Foto: Försvarets bildbyrå/ Håkan Nyström.

Signalunderrättelsetjänst

Med signalunderrättelsetjänst (SIGUND, jfr engelska SIGINT) avses strategisk och operativ underrättelseinhämtning genom signalspaning med syfte att fastställa motståndarens eller annan parts läge, verksamhet och tekniska prestanda. Signalunderrättelsetjänst tillhör funktionen underrättelsetjänst.

Inom den strategiska signalspaningen har arbetssättet vid signalspaning mot kommunikation och signalspaning mot radar ofta skilt sig åt väsentligt. Detta har föranletts av att radiokommunikationen har ett informationsinnehåll som kan ge ett stort mervärde om det kan utvinnas. I radarfallet finns inget sådant informationsinnehåll utan de slutsatser som kan dras är beroende av de tekniska parametrar som kan mätas i signalen, till exempel pulsbredd och pulsrepetitionsfrekvens, tillsammans med den förkunskap om olika radarsystem 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 74 och 75.

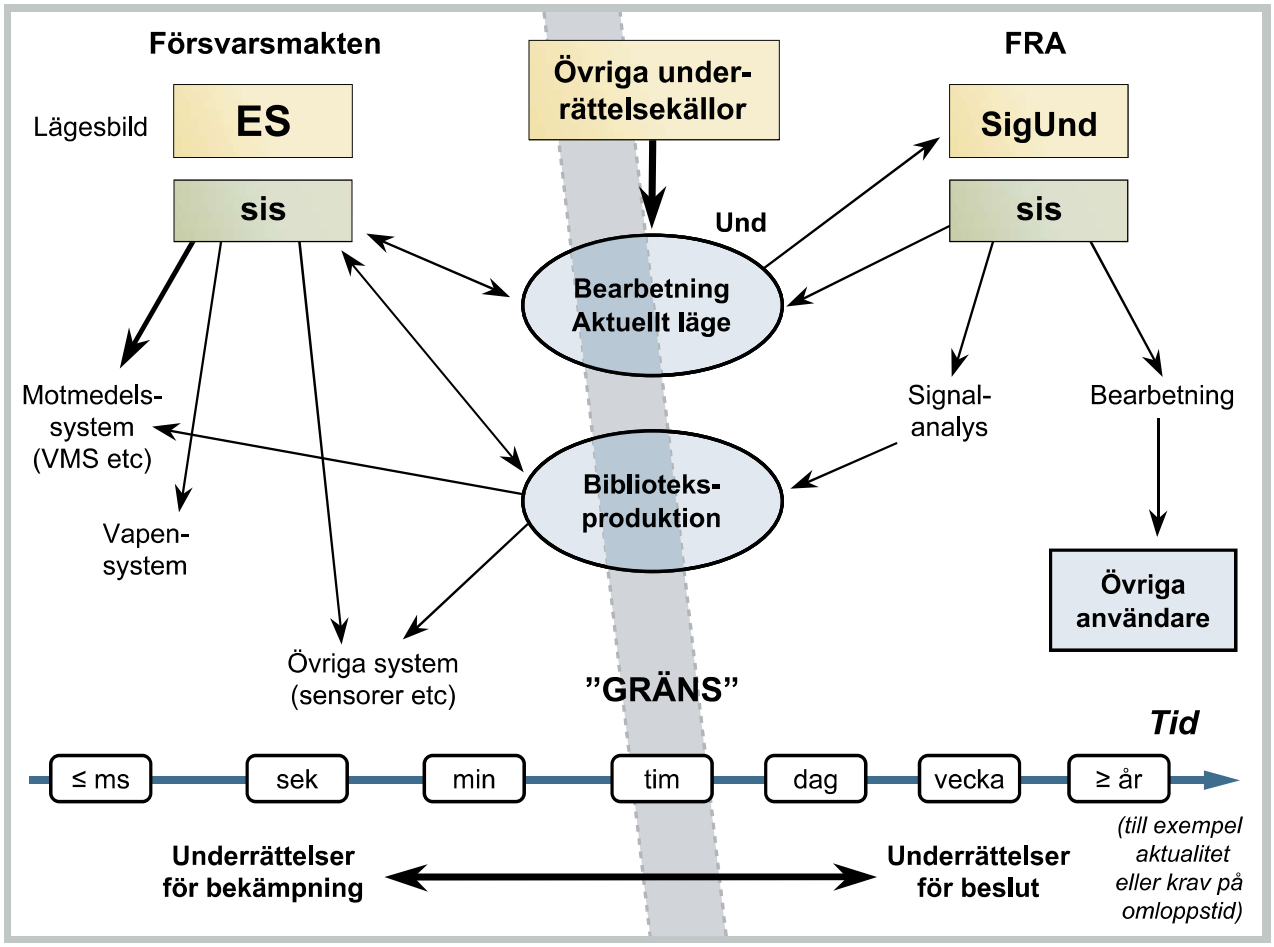
Det finns stora likheter mellan taktisk signalspaning (ES) och SIGUND med avseende på teknik. De skiljer sig dock åt vad gäller syfte och användare. Syftet med operationen är basen för att bestämma om det handlar om en ES- eller en SIGUND-operation. Allmänt kan sägas att ES stödjer telekrig- och taktiska aktiviteter med information.

SIGUND stödjer med underrättelser för användare på alla nivåer, d.v.s. från den nationella regeringsnivån ner till taktiska chefer, och med syften alltifrån långtidsplanering till att i nära realtid stödja operationer, inklusive telekrigoperationer. SIGUND förser också telekrigfunktionen med nöd-

Figur 75. S102 B Korpen som används för teknisk signalspaning. Foto: Försvarets bildbyrå/Peter Liander.

vändiga tekniska data och underrättelser för att kunna utveckla utrustning och procedurer. Detta sker bl.a. genom omfattande prov- och försöksverksamhet där system provas i både simulerad och verklig miljö under längre perioder.

Nära samarbete måste säker ställas mellan ES och SIGUND när separata enheter eller utrustningar används. SIGUND och ES skiljer sig även oftast åt med avseende på tidsförhållanden. SIGUND arbetar med längre tidsperspektiv, timmar till år, medan ES arbetar mot bekämpningsperspektivet, sekunder till timmar. Det är givetvis svårt att sätta en specifik tidsmässig gräns mellan ”underrättelseperspektivet” och ”bekämpningsperspektivet”. Se även figur 76.



Figur 76. En illustration av de olika tidsperspektiven för ES och SIGUND.

En förutsättning för att kunna få effekt av telekrigåtgärder 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 att utnyttja telekrig som en integrerad del vid lösande av uppgifter, d.v.s. det måste bli naturligt att ”tänka telekrig”.

För att klara detta krävs utbildning av både enskilda individer och förband. Det är också nödvändigt att telekrig finns med som en naturlig del vid övningar. För att säkerställa att olika materielsystem fungerar i telekrigmiljö vid en insats är det viktigt att prov och försök genomförs.

Kunskap om telekrigföring bör ingå i alla utbildningssteg med målet att officeren i sin befattning rätt kan bedöma de möjligheter och hot som telekrigföring medför för eget förband och egna materielsystem.

För att tillgodose de behov som finns tillhandahåller Försvarsmakten årligen en orienterande kurs avseende telekrig för försvarsanställd personal. Inom ramen för chefsprogrammet vid Försvarshögskolan finns en särskild inriktning för ledning och telekrig. Utbildningen innehåller kurser med telekriginriktning inom områdena sambandsteknik, radar och optronik.

Soldater måste också ges vana att hantera en miljö där telekrigföring ingår som en naturlig del såväl i grundutbildningen som i samband med övningar. Det är viktigt att inse att telekrigföringen är en realitet så fort man rör sig, sänder med radio etc.

Figur 77. Specialutbildningstecken m/02 för telekrig.

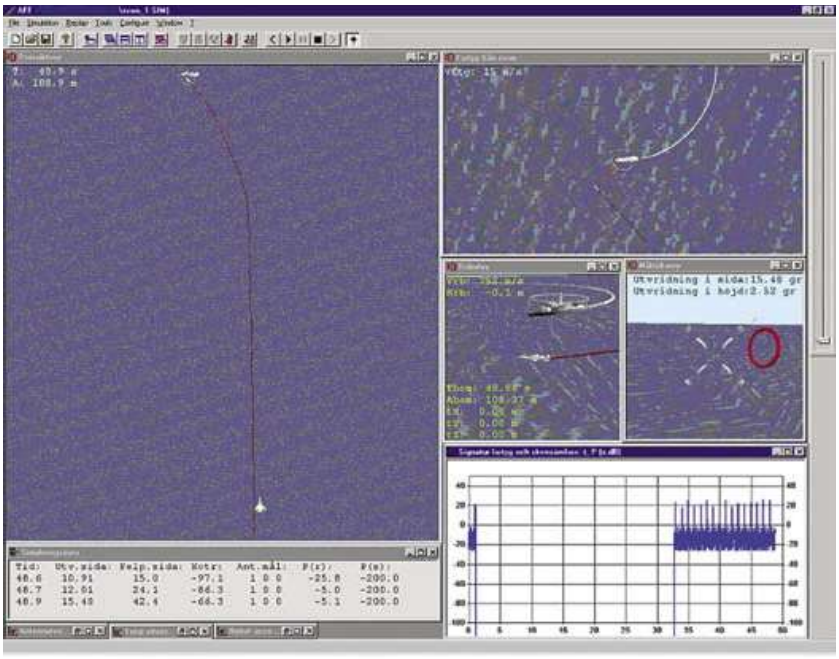
Ett ökat internationellt engagemang med svenska förband kräver utbildning i de procedurer och stabsarbetsmetoder för samordning av underrättelsetjänst, telekrigföring och ledningssystem som används inom NATO. NATO-kurser inom telekrigområdet är dock endast öppna för medlemsländer. PFP-länder är här hänvisade till en särskild kurs som genomförs i Storbritannien och som omfattar procedurer, policy och stabsarbetsmetoder inom NATO. Denna kurs är godkänd av NATO. För att öka mängden utbildad personal genomförs även en motsvarande utbildning i svensk regi. Det svenska genomförandet omfattar i stort samma områden som kursen i Storbritannien men med medvetet fokus på svenska förband och utveckling av egna metoder.

Personal inom Försvarsmakten som har genomgått telekrigutbildning och tjänstgjort i telekrigbefattning kan få rätten att bära specialutbildningstecknet för telekrig, se figur 77.

En viktig väg till ökad kunskap är att öva telekrig, både nationellt och internationellt. Under åren 2003 till 2005 har Telekrigviggen 37E från F 21 samt RBS 90 från Lv 6 med gott resultat deltagit i ELITE (Electronic Warfare LIve Training and Exercise) som är en årlig tysk nationell övning med tyngdpunkt på telekrigföring. I övningen deltar både flyg- och luftvärnsförband från flera nationer. Övningen utvecklar koncept för en europeisk SEAD-förmåga samt utvecklar deltagande förbands förmåga att verka i telekrigmiljö och förmåga att samarbeta i multinationella förband.

Prov och försök utnyttjas för att kontrollera att materielsystem fungerar på avsett sätt samt för att generera kunskap och data för forskning och studier. För ett motmedelsystem kontrolleras exempelvis att det klarar av att hantera de dimensionerande hotsystem som identifierats. Resultaten från försöken används som underlag för att skapa och uppdatera de bibliotek som motmedelssystemet använder. Data från prov och försök är även en viktig grund för att genomföra modellering och simulering (M&S) av materielsystem samt validering och verifiering av befintliga modeller. På motsvarande sätt bör resultat från simuleringar utnyttjas för planering av prov och försök. Genom att använda modellering och simulering som komplement till praktiska prov är det möjligt att göra mängdförsök på ett kostnadseffektivt sätt.

För att utveckla, utbilda samt planera telekrigföring krävs kvalificerade simuleringar av såväl enskilda systems prestanda som av operativa och taktiska effekter av telekrigföringen. Det är därför nödvändigt att simulatorer både på operativ och taktisk nivå korrekt och åskådligt kan visa effekterna av egna och fientliga telekrigföringsåtgärder. Simuleringarna skall kunna understödja såväl studier och planläggning av det framtida försvaret som utbildning och genomförande i direkt anslutning till striden. Simuleringarna behöver ske på olika nivåer, från enskilda system till operativ nivå samt kunna ta



Figur 78. Ett exempel på ett anfall med en signalsökande robot mot ett fartyg. Olika vyer presenteras. T.v. översiktsvy för scenariot. Nere till höger visas den av den signalsökande roboten detekterade radarsignalen från fartyget. Tack vare eller på grund av att radarn på fartyget stängs av kombinerat med gir missar roboten.

hänsyn till förutsättningar såsom terräng och aktuell vågutbredning (särskilt viktigt vid missioner i länder med annorlunda klimat och topografi).

Ett bra exempel på kombinationen mellan utveckling, utbildning och träning är utvecklingen av Marinens telekrigutbildningsverktyg ”DSim”, se figur 78. DSim är ett utbildningsverktyg där Marinens luftvärnsoperatörer efter utbildning får prova olika typer av motmedel mot flera olika sjöhotrobotsystem. Verktyget är en vidareutveckling av forsknings- och analysverktyg som kompletterats med utbildning i telekriginsatser mot sjörobothotsystem. Sammantaget ger utbildningspaketet goda möjligheter till träning och ökad förståelse för aktuella dueller samt indirekt möjligheter till utveckling av stridsteknik och taktik, inom ett område där det ofta är svårt att öva med realistiska hot och insatser.

Utbildning inom telekrigområdet kan bedrivas mycket effektivt om eleverna har tillgång till kursmaterial där de interaktivt kan prova olika problemlösningar 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 att ta fram detta utbildningsmaterial, men det krävs ofta en arbetsinsats för att anpassa forskningsmodellerna och framför allt för att ta fram relevanta och pedagogiska scenarier.

Som allting annat förändras även telekrigets roll avseende syfte, medel och mål. Traditionellt har ansvaret legat på Försvarsmakten och målen har främst varit militära. Åtskillnaden mellan militär och polisiär verksamhet har varit – och är ännu – skarp och tydlig.

I och med den tekniska utvecklingen där kapaciteten i befintliga telekrigsystem förbättrats samtidigt som nya system tillkommit omformas telekrigets funktion. Nya möjligheter uppstår såväl för användning av telekrig som för skydd från verkningar av dessa. Introduktionen av ett nätverksbaserat försvar i kombination med att telekrig är ett av flera verktyg för genomförande av informationsoperationer är några drivkrafter till förändring, om än i huvudsak inom det militära systemet. De nya hot mot det öppna samhället i form av t.ex. terrorism och gränsöverskridande kriminalitet som är en realitet idag kan komma att leda till att gränsen mellan militära och polisiära funktioner och ansvarsområden luckras upp. Sveriges ökande internationella engagemang i fredsfrämjande insatser kan också innebära nya situationer där ett effektivt användande av telekrig kan vara ett medel att reducera risker och hot mot svenska insatser.

Målen för attacker som Sverige potentiellt kan drabbas av kan vara av såväl militär som civil art, t.ex. elsystem, mobil infrastruktur, finansiella sektorer etc. Utförarna, de potentiella antagonisterna, förändras. De behöver inte vara stater utan kan vara individer eller grupper som kan bedriva telekrig med relativt små medel och andra motiv än de gängse. De kan också agera på ett annat sätt, i nya konstellationer och med nya beteenden. Den breddade hotbilden kan sägas vara en konsekvens av uppkomsten av nya sårbarheter, teknisk utveckling och doktrinär förändring i kombination med nya slag av antagonister.

En viktig roll för telekrig har traditionellt varit att skydda plattformar, t.ex. fartyg, flygplan och stridsfordon. En tanke med det nätverksbaserade försvaret är att knyta samman plattformar, system, sensorer och komponenter till nätverk. I och med detta blir det viktigt att skydda hela ”nätet” snarare än de enskilda delarna. Vid en eventuell attack mot ett system skall trafiken kunna ”routas” om och gå andra vägar. Trots påverkan skall nätet kunna synkronisera sig så att uppgifter/operationer fortfarande skall kunna utföras. Åtminstone i teorin. Även i framtiden kommer plattformsskyddet självklart att ha stor betydelse.

Genom att använda nätet som enhetlig resurs för att koordinera och kraftsamla telekrigåtgärder kan den totala effekten av en enskild handling öka. Själva nätet byggs upp av både militära och civila komponenter, där exempelvis informations- och kommunikationsstrukturen kan baseras på Internet och GSM/3G. De civila systemen använder sig ofta av en öppen arkitektur med standardiserade gränssnitt. Säkerhetsnivån är således inte lika utvecklad som för de militära varianterna. Det gör att möjligheterna att slå ut eller påverka den information och det trafikflöde som genereras blir stor. Vill man reducera kapaciteten i de militära näten kan man slå mot de civila.

En bedömning är att den framtida striden i högre grad kommer att föras på informationsarenan, på bekostnad av den klassiska striden på de fysiska arenorna (mark-, sjö- och luftarenorna). Utvecklingen går från plattformsskydd till att reducera en potentiell antagonists ledningsförmåga genom att påverka dennes nät av vitala noder, länkar, ledningssystem etc. För telekrigets del kan detta innebära dels att telekrig lyfts upp till en högre nivå, dels att telekrig knyts fastare samman med dator- och nätverksoperationer (Computer Network Operations, CNO) och informationsoperationer. På liknande sätt som civil och militär teknologi konvergerar länkas telekrigföringen samman med informationskrigföring.

Allt detta leder till att telekrig kan ges nya roller, dels som ett hot mot det svenska samhället och svenska militära förband, dels som en möjlighet t.ex. för skydd av svenska förband som sätts in i internationella insatser. Att telekrig även kan karakteriseras som ett s.k. icke-dödligt vapen är i detta sammanhang väsentligt för dess utnyttjande och potential.

Telekrig i urban miljö

Figur 79. Patrullering i urban miljö. Foto Försvarets bildbyrå / Adam Folcker

Vid internationella insatser kommer svenska enheter att till stor del ha sin verksamhet inne i städer. De flesta sensor- och varnarsystem som idag används är till för att upptäcka hot på så långt håll som möjligt. Inne i städer skulle man dock hellre önska sig vidvinkliga än långräckviddiga system. Ett stort problem med den urbana miljön är att civila kommer att vara kvar, varför krav kommer att finnas på att minimera skador på civil materiel. Dessutom kan det vara så att man i vissa fall endast temporärt vill slå ut en funktion som motståndaren använder (t.ex. en TV- eller radiostation) för att senare själv kunna utnyttja den. Ett sätt att temporärt slå ut utrustning kan vara med hjälp av telekrig. Ett hot och ett problem är fjärrutlösta IED (Improvised Explosive Devices). Störsändare skulle kunna användas för att störa utlösningssignalen och därigenom förhindra verkan av dessa system. Även i övrigt finns många potentiella tillämpningar för telekrig vid operationer i urban miljö.

Telekrig mot kommersiella (radio)system

Även om civil teknik är utvecklad för civila förhållanden används den civila infrastrukturen i hög utsträckning redan idag såväl militärt som av de hot som ingår i den nya hotbilden.

Uppbyggnaden av stora system som t.ex. mobiltelefonisystemet GSM bygger på öppna standarder. Ofta är informationsinnehållet i signalen genom kryptering tämligen välskyddat mot avlyssning. Signalen i sig går däremot på kända frekvenser och ligger öppen för utstörning.

Till kommersiella system kan räknas mobiltelefonisystem (t.ex. GSM och UMTS), satellittelefonisystem (t.ex. Iridium och Inmarsat), PMR (Professional Mobile Radio, t.ex. TETRA, MOBITEX och DECT), jaktradio, samt olika typer av datorkommunikationsnät (t.ex. W-LAN och bluetooth). Hit räknas också satellitnavigeringssystem (GNSS, Global Navigation Satellite System).

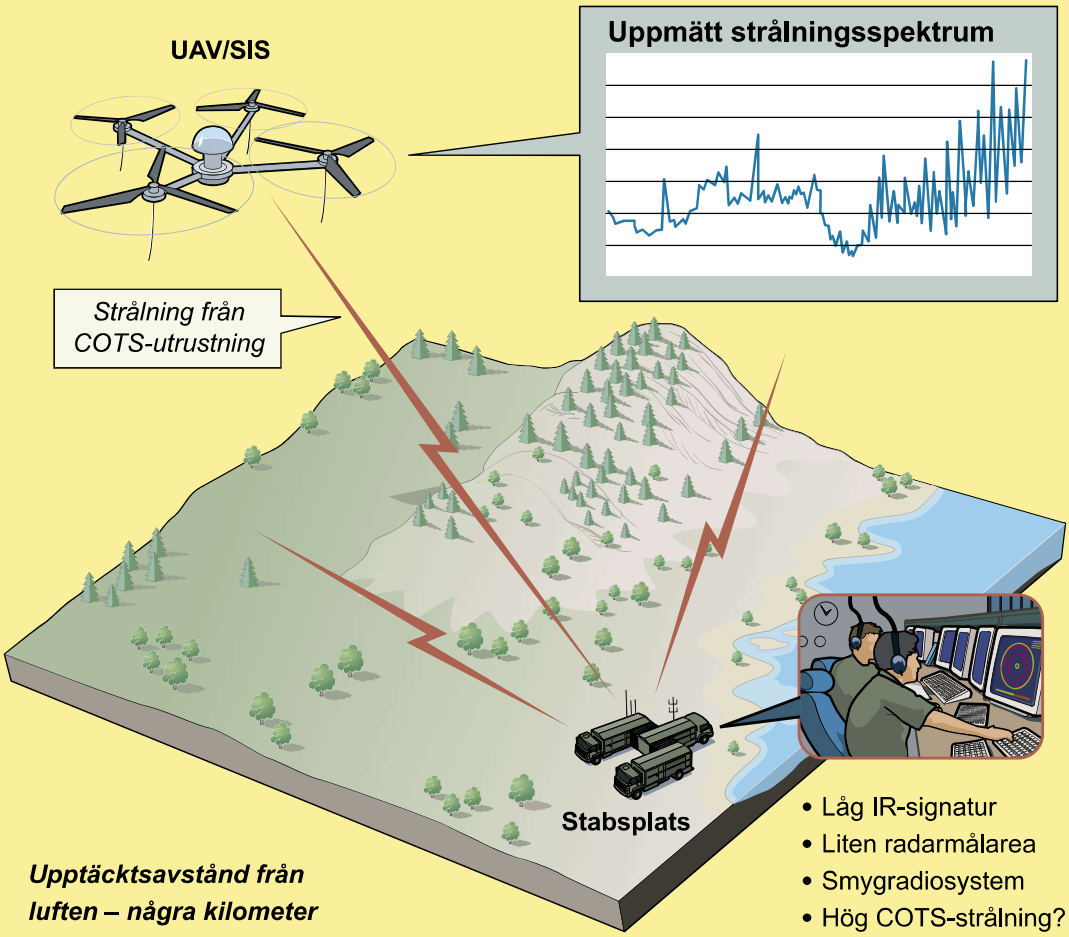
Den mest spridda kommersiella radiosändaren är mobiltelefonen, den yttersta noden i ett komplext nätverk av basstationer, växelsystem och olika abonnent- och telefonregister. Samtal eller annan trafik går aldrig direkt mellan två telefoner utan alltid via nätverket. Den yttersta länken mellan mobiltelefonen och basstationen kan enkelt störas ut med kommersiellt tillgänglig utrustning. Sådan utrustning annonseras öppet på Internet. (Kriminella grupper i Sverige har bevisligen införskaffat störsändare mot GSM som avsetts användas vid planerad kriminell verksamhet). Denna yttersta länk är normalt väl skyddad mot avlyssning. Där tar skyddet slut, såvida man inte har ett utanpåliggande end-to-end-krypto. Med end-to-end-krypto menas att meddelandet är krypterat hela vägen från sändare till mottagare. Det gäller generellt att den operatör som administrerar ett nät också har möjlighet att följa, logga och avlyssna all trafik i nätet. För den som har operatörens medgivande eller på annat sätt lyckats erhålla operatörsprivilegier ligger således nätet öppet.

Det nya systemet RAKEL för ”blåljusmyndigheter” bygger på TETRA-standard (TETRA = TErrestrial Trunked RAdio). Det är uppbyggt som ett mobiltefonisystem med basstationer och växelsystem.

Dessutom finns möjlighet att kommunicera direkt mellan två telefoner, utan att gå via nätet. Skyddet mot avlyssning är väsentligt bättre än i tidigare radiosystem och det finns möjlighet till end-to-end-kryptering. Frekvenstilldelningen är dock öppen och systemet kan utan större svårighet störas ut för den som så önskar. En värdefull förstärkning av systemet skulle vara förmåga att detektera störsändning och förmåga att bestämma riktningen till störkällan.

Sammanfattningsvis kan sägas att en förutsättning för säker informationsöverföring via ett kommersiellt system är att tillgång finns till end-to-end-krypto. Informationen måste vara krypterad hela vägen från sändare till mottagare.

COTS



Figur F22. Civil elektronik avger oönskad strålning som kan vara möjlig att signalspana mot.

COTS står för commercial off the shelf och avser civil teknik som används i militära tillämpningar. Under det kalla kriget var militär teknik teknikledande inom så gott som alla områden. Under 1990-talet blev dock den civila industrin teknikledande inom telekommunikation och informationsteknik. När samtidigt de flesta länders försvarsbudgetar drogs ned föddes tanken att börja utnyttja billig men avancerad civil teknik även i militära tillämpningar. Detta blev speciellt intressant för ledningssystem där telekommunikation och informationsteknik utgör de fundamentala byggstenarna. En nackdel med COTS är att all civil elektronik tillåts att emittera betydligt högre nivåer av oavsiktlig elektromagnetisk strålning jämfört med motsvarande militärspecificerad utrustning. Detta är en av huvudorsakerna till att civil elektronik är betydligt billigare än militär. Att strålningen från civil elektronik allvarligt kan störa taktiska trådlösa kommunikationssystem har varit känt en tid. En fråga som däremot inte är tillräckligt utredd ännu är om denna strålning även går att utnyttja för att med taktisk signalspaning identifiera exempelvis en ledningsplats som i övrigt har låga signaturegenskaper. Enkla uppskattningar visar att upptäcktsavståndet vid en sådan signalspaning kan vara upp till flera kilometer vid signalspaning från luften (till exempel med hjälp av UAV), se figur F22. Utan kännedom om denna egenskap hos civil elektronik kan man alltså få en plattform som har låga signaturegenskaper i exempelvis IR- och radarområdet men som har hög emission i andra frekvensområden. Den oavsiktliga strålningen från COTS ligger typiskt i frekvensområdet 100 MHZ - 1 GHz.

FÖRKORTNINGAR

ADC	Air Defence Controller
AGC	Automatic Gain Control
AM	Amplitudmodulation
ARTHUR	ARTillery HUnting Radar
ASLU	Adaptiv sidolobsundertryckning
AWACS	Airborne Warning And Control System
BER	Bit Error Rate
CCD	Charge-Coupled Device
CNO	Computer Network Operations
COTS	Commercial off the shelf
DAB	Digital Audio Broadcasting
DDOA	Doppler Difference of Arrival
DECT	Digital Enhanced Cordless Telecommunications
DIRCM	Directional Infrared Counter Measures
DRFM	Digitala Radio-Frekventa Minnen
DRM	Digital Radio Mondiale
DS	Direct Sequence, direktsekvens
EA	Elektronisk attack
ECCM	Electronic Counter Counter Measures
ECM	Electronic Counter Measures
ELITE	Electronic warfare LIve Training and Exercise
EMKON	Kontrollerad emission (eng. Emission Control, EMCON)
EO	Elektrooptik, elektrooptisk
EOB	Electronic Order of Battle
EP	Elektronisk protektion
ES	Elektronisk stödverksamhet
ESM	Electronic Support Measures
FH	Frequency Hopping, frekvenshopp
FLIR	Forward Looking InfraRed
FM	Frekvensmodulation
FM TK SE	Försvarsmaktens telekrig stödenhet

GLONASS	Global'naya Navigatsionnaya Sputnikovaya Sistema (Global Navigation Satellite System)
GMTI	Ground Moving Target Indication
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM	Global System for Mobile communications
HARM	High speed Anti-Radiation Missile
HF	High Frequency
HPM	High Power Microwaves
IED	Improvised Explosive Devices
IK	Igenkänning
IR	Infrared, infrarött
IRST	Infrared Search and Track
IRV	Infrared Vision
ISR	Intelligence, Surveillance and Reconnaissance
JSR	Störövervikt (Jammer-to-Signal Ratio)
KOS	Kommunikationssignalspaning
LBI	Long Baseline Interferometry, långbasinterferometri
LBM	Lokal BrytningsindexModell
LWIR	Long Wave IR
MANPADS	MAN Portable Air Defence Systems
MASS	Multi Ammunition Softkill System
MAWS	Missile Approach Warning System
MTI	Moving Target Indication
MWIR	Medium Wave IR
NEMP	Nuclear Electro-Magnetic Pulse
NIR	Near IR, nära IR
NVG	Night Vision Goggles (bildförstärkare)
OFDM	Orthogonal Frequency Division Multiplex
OIF	Operation Iraqi Freedom
OOK	On-Off-keying
OTH	Over the Horizon (Radar)
PMR	Professional/Private Mobile Radio
PPI	Plan Position Indicator
PRF	Pulsrepetitionsfrekvens

PSYOP	Psykologiska operationer
RADAR	Radio Detection and Ranging
RAKEL	Radiokommunikation för effektiv ledning
RAM	Radarabsorberande material
RL	Radiolänk
RSR	Relativ störräckvidd
SAR	Syntetisk AperturRadar
SAT	Signaturanpassningsteknik
SEAD	Suppression of Enemy Air Defence
SEI	Specific Emitter Identification
SIGINT	Signals Intelligence, jfr SIGUND
SIGUND	Signalunderrättelsetjänst, jfr SIGINT
SIS	Signalspaning
SNR	Signal/brusförhållande (Signal-to-Noise Ratio)
STRIL	Stridsledning och Luftbevakning
SWIR	Short Wave IR
TDOA	Time Difference of Arrival
TES	Teknisk signalspaning
TETRA	TErrestial Trunked RAdio
TIR	Termisk IR
UAV	Unmanned Aerial Vehicle
UCK	Kosovos befrielsearmé (Ushtria Clirimtare E Kosoves)
UHF	Ultra High Frequency
UMTS	Universal Mobile Telecommunications System
UV	Ultraviolett
UWB	Ultra Wide-Band
VHF	Very High Frequency
VIS	Visuellt
VMS	Varnar- och motverkanssystem
WCDMA	Wideband Code Division Multiple Access
WLAN	Wireless Local Area Network

LITTERATURLISTA

Allmänt

Berglund L., et. al., **Förstudie Telekrig i urban miljö,** FOI-R--1386--SE, 2004.

Heickerö R, et al.., **Telekrig i en breddad hotbild,** FOI-R--1370--SE, 2004.

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.

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

FOI orienterar om: Sensorer, FOI, 2004.

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

Utkast, Försvarsmaktens Grundsyn informationsoperationer (IO), Försvarsmakten, 01 600:78657, 2003.

Vågutbredning

Börje A., **Vågutbredning över mark och hav – kurskompendium,** FOI-R—0038—SE, 2001.

Hopfgarten A., et al. **Ett stöd för bedömning av radarräckvidd hos marinens fartyg: programmet LBM : en användarhandledning.** FOI-R--1236--SE, 2004.

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., **Antennas and Propagation for Wireless Communication Systems** ISBN: 0-471-98609-7, september 1999.

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

Kommunikation

Ahlin L, Zander J., **Principles of Wireless Communications,** Studentlitteratur.

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

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

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 — Arcitechture and Protocols,** Perentice-Hall.

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

Sklar B. , **Digital Communications — Fundamentals and Applications,** Prentic-Hall.

Radar

Andersson, B. et al., **Precisionslägesbestämning med flygburna radarsis-sensorer,** FOI-R--0719--SE, FOI, 2002.

Andersson B., et al., **Flygburen passiv lägesbestämning baserad på noggrann frekvensmätning,** FOI-R--0329--SE, 2001.

Andersson B., et al., **Sensorsamverkan för radarvarning och taktisk radarsignal-spaning,** FOI-R--1335--SE, 2004.

Bergdal, H. et al., **Signalspaningsteknik del 2, Radarsignalspaning,** FOI, 2002.

Curland, J. & McDonough, R., **Syntethetic Apertur Radar — System and Signal Processing,** John Wiley & Sons, 1991.

Hyberg P., **Kompendium i Radarmotmedelsteknik,** R A 10052-1.1, 1993.

Kingsley, S. & Quegan, S., **Understanding Radar Systems,** SciTech Publishing, 1999.

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, Försvarsmakten, 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.

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.

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

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

Angränsande områden

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

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

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

SAT-handbok Mark, FOI, 2003.

Decibelbegreppet

För fysikaliska storheter vars mätetal vanligen varierar inom ett stort område, åtskilliga tiopotenser, finns det ett behov av att göra värdeskalan 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 = Bel = $\log_{10}(P_1/P_2)$, d.v.s.

dB = decibel = $10 \cdot \log_{10}(P1/P2)$

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 då avståndet ökar observatören uppfattar en lägre frekvens än den utsända.

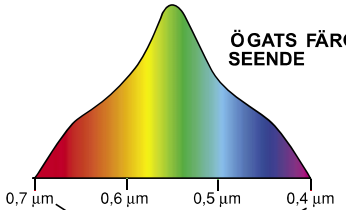
För fallet aktiv sensor med sändare och mottagare (observatör) på samma plattform (och således med samma rörelse) kan frekvensförskjutningen skrivas

$$\Delta f = \frac{2v}{c} f = \frac{2v}{\lambda}$$

där f är den utsända frekvensen, λ våglängden, v målets rörelse relativt sensorn längs siktlinjen och c vågens utbredningshastighet. Beroende på om målet närmar eller fjärmar 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.

DET ELEKTROMAGNETISKA SPEKTRUMET



OMRÄKNINGSTABELL

Ljushastigheten
$c \approx 3 \times 10^8$ meter/sekund

Våglängd i meter
$\lambda = \frac{c}{f}$

Frekvensen i hertz
$f = \frac{c}{\lambda}$

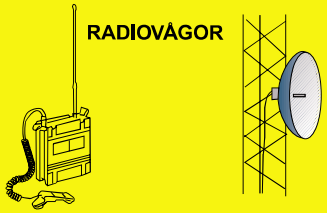
Energi i elektronvolt (eV)
$E = h \times f$

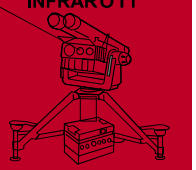
$h = 4{,}1 \times 10^{-15}$ eV × sekund
(Plancks konstant)

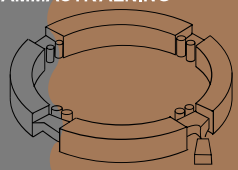
BETECKNING	FÖR-KORTN	10-POTENS	MULTIPLAR OCH DELAR
tera-	T	10^{12}	En biljon
giga-	G	10^{9}	En miljard
mega-	M	10^{6}	En miljon
kilo-	k	10^{3}	Ett tusen
hekto-	h	10^{2}	Etthundra
deka-	da	10^{1}	Tio
deci-	d	10^{-1}	En tiondel
centi-	c	10^{-2}	En hundradel
milli-	m	10^{-3}	En tusendel
mikro-	µ	10^{-6}	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	1A	1×10^{-10}m	En tiomiljarddels meter

TALFREKVENS | LÅNGVÅG | KORTVÅG | ULTRAKORTVÅG | MIKROVÅG | LÅNGVÅGIG IR | TERMISK IR (TIR) | NÄRA IR (NIR) | SYNLIGT LJUS | ULTRAVIOLETT | EXTREMT KORTVÅGIG UV | MJUKA RÖNTGENSTRÅLAR | HÅRDA RÖNTGENSTRÅLAR | MJUK GAMMASTRÅLNING | HÅRD GAMMASTRÅLNING | SEKUNDÄR GAMMASTRÅLNING | GAMMASTRÅLNING UPPKOMMEN UR KOSMISK STRÅLNING

ELKRAFT & TELEFON | RADIOVÅGOR | MIKROVÅGOR | INFRARÖTT | ULTRA-VIOLETT | RÖNTGEN-STRÅLNING | GAMMASTRÅLNING







NUKLEÄR EMP

ICKE-NUKLEÄR EMP
RADIO OCH TELEVISION
ELEKTRONRÖR
INTEGRERADE KRETSAR

RADAR
HPM
MAGNETRONER
KLYSTRONER
GYROTRONER

LASRAR OCH LEDSTRÅLESTYRDA ROBOTAR
AVSTÅNDSMÄTARE OCH LASERSIKTEN
VÄRMEKÄNSLIGA SIKTEN
SYNLIGT OCH FLUORISERANDE LJUS

RÖNTGENRÖR

PARTIKELSTRÅLEENERGI
LINJÄRA ACCELERATORER
BETATRONER
SYNKROTRONER

HERTZ: 1 3 10 30 100 300
KILOHERTZ: 1 3 10 30 100 300
MEGAHERTZ: 1 3 10 30 100 300
GIGAHERTZ: 1 3 10 30 100 300
TERAHERTZ: 1 3 10 30

PARTIKELENERGI I ELEKTRONVOLT (eV)
1 10 eV 100
1 keV 10 100
1 MeV 10 100
1 GeV 10

1 10^1 10^2 10^3 10^4 10^5 10^6 10^7 10^8 10^9 10^{10} 10^{11} 10^{12} 10^{13} 10^{14} 10^{15} 10^{16} 10^{17} 10^{18} 10^{19} 10^{20} 10^{21} 10^{22} 10^{23} 10^{24} 10^{25}

FREKVENS I HERTZ (PERIODER PER SEKUND)

100 Mm | 10 Mm | 1 Mm | 100 km | 10 km | 1 km | 100 m | 10 m | 1 m | 10 cm | 1 cm | 1 mm | 100 µm | 10 µm | 1 µm | 100 nm | 10 nm | 1 nm | 1 Å | 10 pm | 1 pm | 100 fm | 10 fm | 1 fm | 100 am

10^8 10^7 10^6 10^5 10^4 10^3 10^2 10^1 1 10^{-1} 10^{-2} 10^{-3} 10^{-4} 10^{-5} 10^{-6} 10^{-7} 10^{-8} 10^{-9} 10^{-10} 10^{-11} 10^{-12} 10^{-13} 10^{-14} 10^{-15} 10^{-16}

VÅGLÄNGD I METER