FOI-R--0691--SE
December 2002
ISSN 1650-1942

Underlagsrapport

Göran Kindvall

Värdering av telekrig

Metoder, verktyg och verksamheter vid FOI Försvarsanalys

Försvarsanalys
172 90 Stockholm

TOTALFÖRSVARETS FORSKNINGSINSTITUT
Försvarsanalys
172 90 Stockholm

FOI-R--0691--SE
December 2002
ISSN 1650-1942
Underlagsrapport

Göran Kindvall

Värdering av telekrig

-

Metoder, verktyg och verksamheter vid FOI Försvarsanalys

Utgivare	Rapportnummer, ISRN	Klassificering
Totalförsvarets Forskningsinstitut - FOI Försvarsanalys 172 90 Stockholm	FOI-R--0691--SE	Underlagsrapport
	Forskningsområde 6. Telekrig	
	Månad, år December 2002	**Projektnummer** E1421
	Verksamhetsgren 5. Uppdragsfinansierad verksamhet	
	Delområde 61 Telekrigföring med EM-vapen och skydd	

Författare/redaktör	Projektledare
Göran Kindvall	Camilla Andersson
	Godkänd av E. Anders Eriksson
	Uppdragsgivare/kundbeteckning Försvarsmakten
	Tekniskt och/eller vetenskapligt ansvarig

Rapportens titel

Värdering av telekrig – Metoder, verktyg och verksamheter vid FOI Försvarsanalys

Sammanfattning (högst 200 ord)

Huvudsyftet med denna rapport är att beskriva metoder och verktyg för värdering av telekrigföring. Rapporten inriktas framförallt på att beskriva verksamhet som genomförts inom projektet Taktisk värdering telekrig vid FOI Försvarsanalys, i huvudsak under perioden 2000-2002. Fokus i framställningen ligger på utnyttjade metoder och framtagna verktyg.

Rapporten innehåller även en allmän beskrivning av telekrigföringens grunder samt en diskussion kring telekrigföring med utgångspunkt i Försvarsmaktens utveckling. Därutöver ingår avsnitt om teknikutvecklingen inom telekrigrelevanta områden samt en allmän beskrivning av värdering.

Rapporten har även som syfte att kunna bidra till förståelse för telekrigföringens möjligheter och begränsningar och kan därigenom förhoppningsvis bl.a. vara till nytta för operationsanalytiker.

.

Nyckelord

Telekrig, värdering, metoder, verktyg, GPS, informationsteori, VMS, avdömningsregler, cross-eye

Övriga bibliografiska uppgifter	Språk Svenska
ISSN 1650-1942	**Antal sidor:** 70 s.
Distribution enligt missiv	**Pris: Enligt prislista**

Issuing organization	Report number, ISRN	Report type
FOI – Swedish Defence Research Agency Defence Analysis SE-172 90 Stockholm	FOI-R--0691--SE	Base data report
	Research area code 6. Electronic Warfare	
	Month year December 2002	**Project no.** E1421
	Customers code 5. Commissioned Research	
	Sub area code 61 Electronic Warfare including Electromagnetic Weapons and Protection	
Author/s (editor/s) Göran Kindvall	**Project manager** Camilla Andersson	
	Approved by E. Anders Eriksson	
	Sponsoring agency Swedish Armed Forces	
	Scientifically and technically responsible	

Report title (In translation)

Assessment of electronic warfare – methods, tools and studies performed by the division of defence analysis

Abstract (not more than 200 words)

The main objective of this report is to describe methods and tools for assessment of electronic warfare. The report is primarily focused at describing activities that have been accomplished within the project Assessment of Electronic Warfare at the Division of Defence Analysis within the Swedish Defence Research Agency, mainly between the years 2000 and 2002. The focus is on methods used and tools developed.

The report also contains a general description of electronic warfare and a discussion concerning electronic warfare in association with the development of the Swedish Armed Forces. In addition to that there are sections about technology development in areas relevant to electronic warfare and a general discussion on assessment.

Another objective of this report is to make a contribution to the understanding of opportunities and limitations offered by electronic warfare and may hence be of use e.g. for operations analysts.

Keywords

Electronic warfare, EW, assessment, methods, tools, GPS, information theory, DAS – defensive aids systems, cross-eye jamming

Further bibliographic information	Language Swedish
ISSN 1650-1942	**Pages** 70 p.
	Price acc. to pricelist

Förord

Projektet Taktisk värdering telekrig (E 1421) vid FOI Försvarsanalys har haft som mål bl.a. att utveckla värderingsmetoder och genomföra värdering av telekrigsåtgärder på taktisk nivå. Ett led i detta är att successivt bygga upp kunskap och förståelse såväl för metoder för värdering som för den växelverkan mellan teknik och taktik som de facto uppstår vid utnyttjande av telekrigföring. Projektet ingår i FoT-område Telekrig.

Ambitionen med denna rapport är att ge en beskrivning av vad telekrig är, hur det kan utnyttjas, vilka möjligheter teknikutvecklingen kan ge, hur värdering av telekrig kan och bör genomföras, vilka verktyg som finns m.m. Dokumentet syftar primärt till att beskriva det arbete inom telekrigområdet som sker vid FOI Försvarsanalys. Det är en utveckling av det dokument som utkom i en första version december 2000 (FOA Memo 00-5672/S, 2000-12-20) och i en delvis reviderad version i december 2001 (FOI Memo 01-4016, 2001-12-19).

Projektet Taktisk värdering telekrig avslutas i december 2002. Ett nytt projekt som bygger vidare på den värderingskompetens inom telekrigområdet som byggts upp startar 2003. Detta nya projekt – Värdering av telekrig i NBF – kommer att ges ett delvis annorlunda fokus.

Denna rapport sammanfattar verksamhet som bedrivits i huvudsak under de tre senaste åren inom projektet Taktisk värdering telekrig. Med förhoppning om att rapporten kan vara av intresse.

Camilla Andersson
Projektledare

Innehållsförteckning

1 Inledning

Huvudsyftet med denna rapport är att beskriva metoder och verktyg för värdering av telekrigföring på stridsteknisk, taktisk och operativ nivå. Rapporten fokuserar härvid på att beskriva olika verksamheter som genomförts inom projektet Taktisk värdering telekrig.

Ett annat syfte är att bidra till att sätta in telekrigföring i ett sammanhang, såväl kopplat till Försvarsmaktens utveckling och teknikutvecklingen som till erfarenheter från de senaste årens konflikter.

Ett tredje syfte är att rapporten skall kunna vara en skrift som kan spridas till dem som behöver en översiktlig beskrivning av telekrigföring ur ett ”FOI Försvarsanalys-perspektiv”. Detta gäller kanske främst operationsanalytiker från FOI verksamma inom Försvarsmakten. Därför är rapporten öppen, vilket också inneburit att tyngdpunkten ligger mer på metoder än på resultat.

Innan framställningen fokuseras på telekrigvärdering ges därför en allmän beskrivning av telekrigföring utifrån det perspektiv som Försvarsmaktens utveckling ger, varpå följer avsnitt om teknikutvecklingen samt värdering i generella termer. Därefter beskrivs verksamhet med betoning på utnyttjade metoder och framtagna verktyg.

Rapporten utgavs i en första utgåva i december 2000 (FOA Memo 00-5672/S, 2000-12-20) och i en andra reviderad utgåva i december 2001 (FOI Memo 01-4016, 2001-12-19). Här föreliggande utgåva är en vidareutveckling av dessa.

2 Definition av telekrigföring

Som inledning är det viktigt att presentera de definitioner som används för telekrigföring och dess komponenter inom Försvarsmakten. [1]

Telekrig
Militär verksamhet som utnyttjar det elektromagnetiska spektrumet för att bekämpa, förvanska eller exploatera motparters inhämtning, bearbetning eller delgivning av information samt skydd mot för oss ogynnsamt utnyttjande av det elektromagnetiska spektrumet. Består av:

Elektronisk Attack (EA)
Utnyttjande av elektromagnetisk energi i syfte att nedsätta eller förstöra motpartens systemfunktioner eller stridsförmåga. Omfattar bl.a.:
- Störning och vilseledning inklusive utnyttjande av elektromagnetiska skenmål.
- Användning av elektromagnetiska pulsvapen (NNEMP) och mikrovågsvapen (HPM).
- Användning av laservapen.
- Logiska attacker mot informationssystem, t.ex. dataintrång.[2]

Elektronisk Stödverksamhet (ES)
Åtgärder för att stödja pågående verksamhet genom att upptäcka, identifiera och lokalisera elektromagnetiska källor. Omfattar bl.a.:
- Signalspaning mot kommunikationsnät inklusive att fysiskt ansluta på dessa (kommunikationssignalspaning, (KOS)).
- Signalspaning mot övriga typer av elektromagnetiska emittrar (teknisk signalspaning (TES)).

Elektronisk Protektion (EP)
Åtgärder för att minska effekten av motståndarens telekrigföring samt åtgärder för att undvika elektromagnetiska konflikter. Omfattar bl.a.:
- Åtgärder för att bibehålla systemprestanda.
- Åtgärder för att minska risken för upptäckt, identifiering, lokalisering och avlyssning. EP utgör härvid en viktig del i systemets/objektets totala signaturanpassning.
- Åtgärder för att undvika konflikter i det elektromagnetiska spektrumet.
- Taktisk ledning och kontroll av egna emissioner i det elektromagnetiska spektrumet (EMKON).

[1] Definitionerna är hämtade ur ”Försvarsmaktens funktionsplan för telekrigföring del 1”, HKV 12 860:68453, 1999-08-04.
[2] Att logiska attacker mot informationssystem definieras som ingående i EA är inte helt okontroversiellt och har diskuterats en del. För närvarande gäller dock denna definition.

3 Telekrigföring och Försvarsmaktens utveckling

3.1 Telekrig och Försvarsmaktens långsiktiga inriktning

Försvarsmaktens långsiktiga inriktning ges i huvudsak av perspektivplaneringen. Den rapport (rapport 6) som gavs ut i februari 2002[3] fokuserar på idébildsperspektivet, d.v.s. utvecklingen av Försvarsmakten sedd ur ett 20-årigt perspektiv. Där finns visionen, beskrivning av trolig omvärldsutveckling, teknikutveckling, samhällsutveckling, konsekvenser för det framtida slagfältet, idébilder m.m.

Punkterna nedan är formuleringar ur årsrapporten från perspektivplaneringen 2001-2002 och visar ett antal av de slutsatser som där dras avseende teknikutvecklingen. Det handlar mycket om ledningskrigföring, sensorer, elektromagnetiska vapen och annat som innehåller telekrigföring alternativt är intressant som medel eller mål för telekrigföring.

- Sensor- och nätverksutvecklingen för också med sig en utveckling av motmedel och en ökad betydelse av IT-säkerhet och informationsoperationer. Kravet på skydd måste åtgärdas genom breda samverkanslösningar. Obemannade farkoster och rymdbaserade system utnyttjas alltmer. Konventionell bekämpningsförmåga förbättras genom precisionsvapen. Civil teknikutveckling, inte minst inom IT, är av ökad betydelse även för militära applikationer.
- Kampen om omvärldsuppfattning och ledningsförmåga intensifieras. Möjligheter att under ostörda förhållanden se hela slagfältet i nära realtid öppnas. Det enda område där en motståndare även framgent kan räkna med att förbli dold för upptäckt är under vattnet. Möjligheten att bevaka rörelser ökar betydelsen av ledningskrigföring. Nätverksbaserade system ökar möjligheterna till snabb bekämpning och uppföljning av verkanseffekt efter upptäckt och identifiering av mål. En uppbyggnad av nätverk bedöms bli avgörande för den framtida kvalificerade striden. Civil teknik kommer i framtiden alltmer nyttjas i militära system, men militärt specifika behov kvarstår inom vissa systemområden.
- Det ökande beroendet av IT-baserade system ökar också känsligheten för informationskrigföring inom hela samhället och för ledningskrigföring inom militär verksamhet. Informationskrigföring blir ett nytt fundamentalt strategiskt element.
- Slagfältet utvidgas i samtliga dimensioner. Rörligheten och tempot i den kvalificerade striden ökar. Förutsättningarna för och kraven på att kunna genomföra gemensamma insatser med mark-, sjö- och flygförband ökar. Allt fler sensorer och bekämpningssystem utnyttjar luftrummet och rymden och en utveckling sker mot större andel luftburna förband.

[3] Årsrapport från perspektivplaneringen 2001-2002: Idébilder och fördjupningsområden inför försvarsbeslut 2004 – rapport 6, HKV 23 210:62285, 2002-02-28.

- Vapenplattformarnas betydelse som enbart vapenbärare minskar på lång sikt och får en förändrad betydelse i takt med att tjänstetänkandet ersätter plattformstänkandet. Plattformen blir således en tjänsteleverantör i egenskap av både kunskaps- och kompetensleverantör som levererar olika tjänster. En ökande vikt kommer i framtiden att läggas vid att dessa plattformar fungerar som uppdateringsbara informationsnoder i nätverk och som resurs för att visa närvaro och hävda nationella intressen.
- Användningen av obemannade farkoster ökar främst i luften men även på marken samt under havsytan för spaning, kommunikation och längre fram även offensiva uppgifter. Utvecklingen går på sikt mot kombinerade sensor- och stridsfarkoster.
- Bekämpningsförmågan är inte enbart beroende av antalet plattformar. Trots reduceringar i dessas numerär kan ändå den sammantagna bekämpningsförmågan öka bland annat genom att använda långräckviddiga vapen med hög precision och att på större avstånd bekämpa såväl punktmål som ytmål.
- Hotutvecklingen visar på ett behov av att vidta skyddsåtgärder i ett betydligt bredare spektrum än tidigare. Bland annat det ökade internationella deltagandet innebär på samma sätt förändrade krav på skyddsåtgärder. Denna utveckling visar på behovet av lösningar som omfattar breda samverkanslösningar, såväl inom Försvarsmakten, som med andra aktörer.
- Utvecklingen inom områdena vapen och explosivämnen samt den ökande betydelsen av elektromagnetiska vapen, leder till att verkanskraften i framtida vapensystem ökar väsentligt. Hotet mot infrastruktur och fasta militära mål ökar därmed. Hotet mot rörliga mål varierar med graden av informationsöverläge, inkluderande signaturanpassningsåtgärder.
- De allt kortare tiderna från upptäckt till bekämpning kräver en vidgad syn på överlevnad och motståndskraft. Skydd av förband och funktioner skapas genom en kombination av signaturanpassning, vilseledning, rörlighet samt utnyttjande av sensoraktiverade och ballistiska skydd.

Under 2002/2003 bedrivs arbetet i perspektivplaneringen inriktat mot att ta fram målbildsunderlag, d.v.s. underlag för Försvarsmaktens utveckling i ett 10-årigt perspektiv. För närvarande arbetar man med fyra olika målbilder, med olika betoning på nationellt försvar respektive internationella insatser. Även kraven på anpassningsförmåga varierar mellan målbilderna.

3.2 Telekrig och det nätverksbaserade försvaret

Hur kommer då telekrig in i alla de trender, framtidstankar och nya begrepp som vi ser och hör idag? Det talas inom Försvarsmakten om nätverksbaserat försvar (NBF). Som en viktig del inom detta satsas stora resurser på att utveckla det framtida ledningssystemet.

Utvecklingen mot det nätverksbaserade försvaret skall ske som en kontinuerlig interaktion mellan doktrin/metodik-, organisations-, personal- och teknikutveckling. För att samordna denna utveckling bedrivs fyra samordnade verksamheter inom FM Ledsyst – LedsystM, LedsystT, LedsystO och LedsystP. LedsystM omfattar utveckling av lednings- och stabsarbetsmetoder för ett nätverksbaserat försvar. LedsystT omfattar utveckling av de tekniska delarna i Försvarsmaktens framtida ledningssystem, däribland en gemensam informationsinfrastruktur. LedsystO skall bereda eventuell vidareutveckling av ledningsorganisationen. LedsystP skall möta de förändrade krav på kompetenser i FM som NBF innebär.

Än så länge har arbetet i huvudsak fokuserat på de det framtida ledningssystemets tekniska delar (LedsystT). Inom LedsystT inriktas arbetet mot att utnyttja systemdemonstratorer för att genomföra tester som visar delar i ett tänkbart framtida ledningssystem. Ett delmål för verksamheten är demonstratorverksamhet 2005 (Demo 05) och 2006 (Demo 06). Dessa syftar till att skapa underlag för beslut om hur NBF skall implementeras. Ledningssystemet kan härvid ses som den första implementeringen av tankarna kring det nätverksbaserade försvaret.

Demo 05 inriktas mot att demonstrera hur en gemensam omvärldsuppfattning kan uppnås i ledningssystemet med hjälp av en nätverksbaserad informationsinfrastruktur, Demo 06 mot att demonstrera hur insatsledning kan utföras i ett nätverksbaserat försvar. Demonstratorverksamheten skall vara en kontinuerlig aktivitet för utveckling, prov och kompetensupprätthållande.

Inspirationen till den utveckling som sker idag i Sverige kan i mycket sökas i de framtidsstudier som bedrivits i det amerikanska försvarets regi (bl.a. Joint Vision 2010 och Joint Vision 2020[4]) och det arbete som utförts åt den svenska Försvarsmakten av det amerikanska företaget Science Applications International Corporation (SAIC). En viktig bärande idé i det senare arbetet är uppbyggnad av ett system av sensorer och sensorbärare (i luften, på marken, på och under vattenytan) som kan bidra till en mycket god situationsuppfattning.

I Joint Vision 2020, vilken publicerades under år 2000, bygger man i USA vidare på tankarna i Joint Vision 2010. Som fokus ses att uppnå ”Full Spectrum Dominance”. Detta skall ske genom ett samordnat utnyttjande av de operativa koncepten Dominant Maneuver, Precision Engagement, Focused Logistics och Full Dimensional Protection. Som förutsättningar för att nå detta mål ses informationsöverlägsenhet (Information Superiority) och förnyelse (innovation). Frågeställningar kring ledning och informationsoperationer lyfts också fram i Joint Vision 2020.

Således handlar det i det amerikanska framtidstänkandet om ledning, information, verkan, logistik och skydd. En kontinuerlig forskning och utveckling behövs för att

[4] Se t.ex. http://www.dtic.mil/jv2020.

understödja denna utveckling. Härutöver är det givetvis viktigt att hantera frågeställningar kring integration av människan (operatören) i systemet (MSI, Människa-System-Integration). T.ex. är det tekniskt möjligt att föra över mycket stora mängder information, men hur behöver den presenteras för att en beslutsfattare skall kunna utnyttja den för att fatta beslut.

Arbete med att studera framtida koncept bl.a. inom sensorområdet har utförts inom ramen för den s.k. FoRMA-verksamheten (FoRMA = Forskning om RMA). FoRMA verkar inom FOI som en sammanhållande struktur inom vilken arbete sker med de olika delar som ingår i det framtida försvaret (bl.a. ledning och situationsuppfattning). Samarbete sker härvid också med övriga försvarsmyndigheter och försvarsindustrin.

Efter telekriganalys av den sensorstruktur som utnyttjats i FoRMA drogs bl.a. följande sammanfattande slutsatser[5]:

- ”För en tidig upptäckt av mål i luften och på ytan är vi beroende av både aktiva och passiva sensorer inom ett stort frekvensområde.
- Den bästa kombinationen av sensorer i aerostaten är ur telekrigssynpunkt ESA-radar, EO-sensor samt ESM-sensor både på radar- och kommunikationsområdet.
- FSR Ny bör innehålla radar-ESM för egenskydd.
- Klassificeringsfrågan på stora avstånd i en telestörd miljö är främst beroende av EO-sensorer och ESM, både på kommunikations- och radarområdet. Dessa sensorer är också av avgörande betydelse för identifieringsfrågan.”

Inom ramen för arbetet med den framtida insatsfunktionen blir också telekrigföring intressant att studera då det finns ett antal steg/faser i kedjan från målupptäckt till verkansverifiering där telekrigföring i olika former kan påverka systemförmågan. Bland sådana steg/faser kan nämnas: upptäckt, räckvidd, navigering, identifiering, precision, verkan och verkansverifiering.

3.3 Telekrig och informationsoperationer

Vi lever i ett informationssamhälle, brukar det heta. Och visst har information fått betydelse, såväl i vårt vardagsliv som för militära beslutsfattare verksamma i det allt otydligare kontinuum som formas av fred, kris och krig. Begrepp som informationskrigföring och informationsoperationer har myntats för att sammanfatta kampen om informationsherraväldet. Dessa begrepp har diskuterats fram och tillbaka och fyllts med allehanda innehåll. En rimlig ”definition” skulle kunna vara[6]:

[5] “FoRMA uppsummering 2001 – På tröskeln till ett nätverksförsvar”, FOI Memo 02-349.
[6] Se Kindvall, G., ”Informationsoperationer – Allt, inget eller något?”, FOI Memo 02-260, 2002-09-27.

Informationsoperationer/informationskrigföring handlar om att information är mål för insatsen. Det handlar således om att utnyttja eller påverka en motståndares information samtidigt som egen information skall skyddas. Ytterst är målet att påverka beslutsfattaren.

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, dataintrång i nätverk, attacker mot infrastrukturen m.m. Det är i fallet informationsoperationer svårt att göra en tydlig separation mellan t.ex. militär och civil informationsinfrastruktur.

Informationsoperationer har ibland blivit likställt med IT-krigföring eller ”cyber-war”. Detta är inte sant om vi betraktar de definitionsförslag som tagits fram, även om IT-krigföringen (eller Computer Network Operations, CNO) är en viktig komponent. Informationsoperationer innehåller även andra komponenter – psykologiska operationer, telekrigföring m.fl. – med förmåga att påverka motståndarens vilja eller kapacitet att strida. IT-krigföringen är dock potentiellt ett område där det kan vara möjligt för många nationer/aktörer att uppnå en förmåga som kan utmana även de mest industrialiserade länderna. De stora nationerna bedöms dock vara de flitigaste aktörerna inom området.

Ett förslag kan vara att betrakta informationsoperationer som en verksamhet som kan genomföras med olika metoder och verktyg för att påverka motståndaren och där information är målet för insatsen. Bland metoder och verktyg kan man tänka sig t.ex. psykologiska operationer, CNO, telekrigföring och fysisk bekämpning mot t.ex. nyckelpersoner eller sambandsnät. På det viset sätts fokus på metoderna och verktygen (som kan användas även inom andra operativa verksamheter).

Införandet av nya begrepp har ibland fått konsekvenser för gamla begrepp. I USA har man sett hur telekrigföring från att vara något självständigt först kom att till del omfattas av begreppet ledningskrigföring (Command and Control Warfare, C2W). Genom den definition på C2W som fastställdes kom telekrigföring att i stort uppfattas som en delmängd av C2W.[7] När sedan begreppet informationskrigföring infördes kom det att överlappa såväl C2W som telekrigföring, men inledningsvis inte helt täcka något av dem. Det nya var informationskampanjer, informationssäkerhet, IT-krigföring etc. Därefter blev C2W bara en delmängd av informationskrigföringen, vilken i sig blev en delmängd av något större – informationsoperationen. Det är inte omöjligt att en reaktion kan komma på detta.[8]

---

[7] I Sverige har vi bl.a. för att betona att telekrigföring till stor del ligger utanför ledningskrigföringen i vår definition av ledningskrigföring inte sett telekrigföring som en komponent av ledningskrigföring utan som ett verktyg bland andra som kan användas för att uppnå ledningskrigföringens syften.

[8] I bl.a. USA pågår diskussioner om att renodla begreppen. Med de definitioner som idag är giltiga är det svårt att hitta åtgärder som inte inryms inom begrepp som informationskrigföring och informationsoperationer. Ett förslag som framförts är att låta informationskrigföring omfatta Perception Management (Psyop, militär vilseledning och motpropaganda) och CNO (Computer Network Operations). Det finns dock såvitt känt inget beslutat ännu.

Befintliga definitioner i USA ger en begreppshierarki ungefär enligt fig. 3.1. I Sverige pågår arbete såväl med att definiera begrepp inom området informationsoperationer som med att klara ut ansvarsförhållanden inom området.

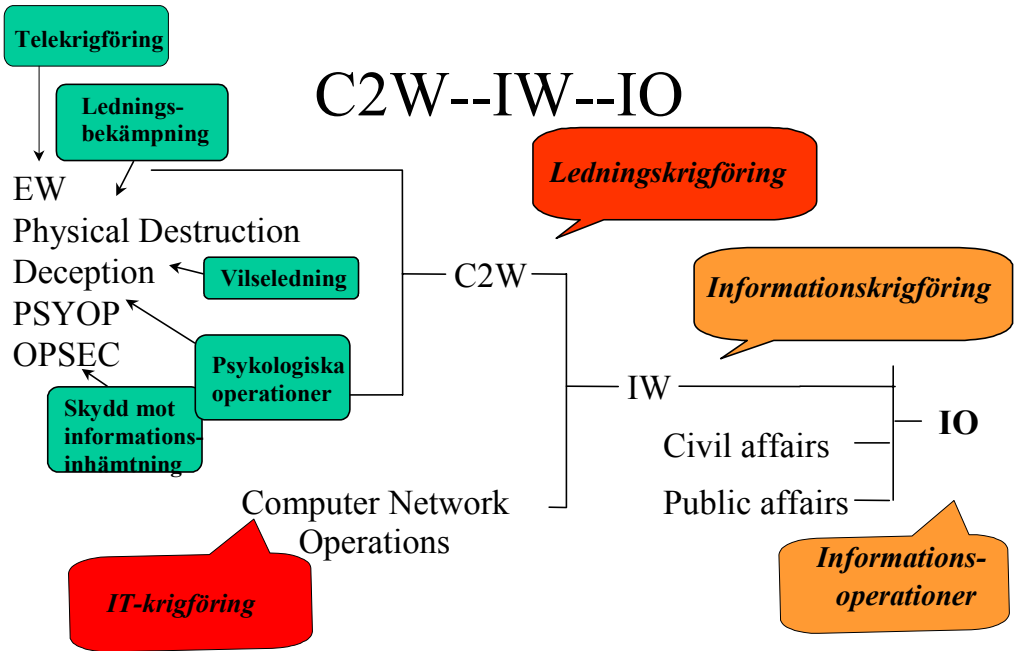

Fig. 3.1. Denna figur visar grovt vad som räknas in inom ramen för informationsoperationer i USA.

Under perioden 2000-2002 har arbete med beskrivning av åtgärder och koncept inom informationskrigföringsområdet bedrivits inom FoRMA-verksamheten. Representanter från FM, FOI, FMV, FRA, FHS och försvarsindustrin har deltagit i detta arbete som bl.a. har inneburit analys av informationskrigföring genom spel samt beskrivning av konceptuella förbandsstrukturer. Inledningsvis behandlades huvudsakligen CNO-komponenten inom informationskrigföring, men arbetet har senare vidgats till att även hantera andra verktyg och metoder – t.ex. telekrigföring och psykologiska operationer. Tanken är att fördjupa arbetet under år 2003 genom att bl.a. ta upp ledning av informationskrigföring.

3.4 Telekrig och navigering

Navigering blir allt viktigare. Hög vapenprecision möjliggörs t.ex. med hjälp av GPS. Det är därför intressant att utröna huruvida störning kan utnyttjas för att minska noggrannheten hos navigeringssystem. Hur stor är störkänsligheten hos

satellitnavigeringssystem (GNSS, Global Navigation Satellite System[9])? Om systemen är sårbara, hur kan de göras störfastare? Går det att bygga in störskydd i systemet, eller är lösningen att kombinera olika navigeringstekniker?

År 1996 deklarerade USA en ny policy för GPS där det bland annat sades att den sämre precision (Selective Availability, S/A) som avsiktligt påförts för den civilt tillgängliga koden skulle stängas av senast år 2006. Framsteg inom störningsmöjligheterna samt att nya militära kanaler planeras i kommande satelliter gjorde denna policyändring möjlig. Ett faktum som hade gjort S/A onödigt var den alltmer utbredda civila användningen av differentiell GPS (DGPS), vilken ger en noggrannhet på ner till 0,5 meter. Detta gjorde att USA istället skaffade sig möjligheten att stänga av (störa ut) GPS lokalt, utan att civila användare utanför störområdet berördes. I och med detta uppkom begreppet navigationskrigföring (NavWar).[10] S/A stängdes av den första maj 2000, men med en årlig revision fram till år 2006.

I fig. 3.2 nedan visas en kommersiellt tillgänglig GNSS-störare från det tyska företaget C. Plath GmbH.

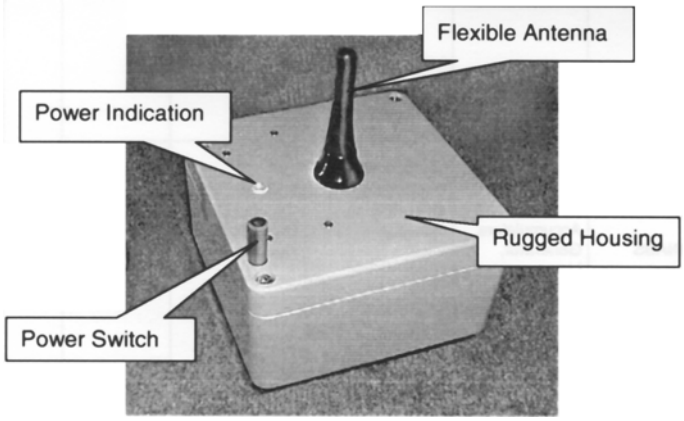

Fig. 3.2. Kommersiell GNSS-störare från C. Plath GmbH. Den finns i effekter från 1 W till 50 W, och uppges ha ett verkansavstånd på 1 km respektive över 10 km mot C/A-mottagare.

[9] Idag finns främst GPS (Global Positioning System), medan det ryska Glonass har begränsad täckning. I Europa planeras också ett eget system, Galileo, vilket inte beräknas vara i full drift förrän ca år 2008.

[10] I Sverige definieras Navigationskrigföring *Åtgärder för att nedsätta prestanda i navigationssystem. Med navigationssystem avses här alla former av navigeringshjälpmedel så som t.ex. satellit-, radio-, positionerings-, terrängföljnings- och tröghetsnavigeringssystem. Prestanda kan nedsättas genom störning, förstöring och vilseledning.* Källa: ”Försvarsmaktens funktionsplan för telekrigföring, del 1”, HKV 12 860:68453, 1999-08-04.

4 Telekrigets grunder

4.1 Det elektromagnetiska spektrumet

Telekrigföringen kan ses som striden om det elektromagnetiska spektrumet. Det elektromagnetiska spektrumet sträcker sig från gammastrålar vid de högsta frekvenserna och ner till det radiofrekventa området, där radar och radio återfinns. Inom telekrigsområdet brukar man ej ta hänsyn till de högsta frekvenserna utan bara använda frekvenser mellan ultraviolett ner till radiofrekvent, se fig. 4.1.

Förhållandet mellan våglängd λ, frekvens f och ljusets hastighet c ($c=3\cdot10^8$ m/s) är följande:

$$c = \lambda f$$

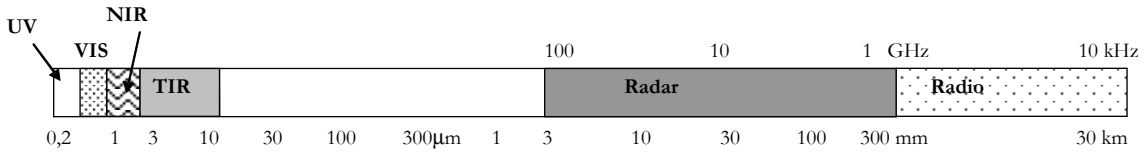

Fig. 4.1. Det elektromagnetiska spektrumet[11].

Optroniksystem arbetar inom området 0,05 –14 µm vilket innefattar det ultravioletta, det visuella och det infraröda (IR) området av spektrumet. IR-området (0,7-14µm) delas upp i det termiskt infraröda (TIR, 2,0-14µ) och nära infraröda (NIR, 0,7-2,0µm). Det senare gränsar till det visuella området (0,4-0,7µm). Mellan IR-området och det radiofrekventa området återfinns mikrovågsområdet.

Det radiofrekventa området brukar uppdelas i åtta områden[12]. Vanliga frekvenser för radar brukar innefatta 1-94 GHz och för radiosamband 10 kHz (VLF) upp till 18 GHz (mikrovågslänkar).

Telekrigområdet omges med en rad begrepp och historia som definierar området. Traditionellt har telekrig varit starkt kopplat till radar och kommunikation. Det finns därför historiskt en ganska stark uppdelning mellan teknikområdena optronik, radar och samband. Systemen använder sig också av ganska olika tekniker varför de kan kännas mer olika än de egentligen är.

---

[11] UV = ultraviolett, VIS = visuellt, NIR = nära infraröd, TIR = termiskt infraröd.

[12] Det radiofrekventa området är uppdelat på följande sätt:
EHF – Extremely high frequency, SHF – Super high, UHF – Ultra high, VHF –Very high, HF – High, MF – Medium, LF – Low, VLF – Very low

Eftersom radarn skickar ut en signal i radiell led och sedan analyserar den, ger systemet avståndsinformation om det studerade objektet. Optroniken däremot fungerar mer som ett avbildande system i x-y-led, där reflekterad eller alstrad strålning (värme) från objektet kan observeras. Detta leder då till att dessa system istället ger positionsinformation för det studerade objektet. Däremot används laser i vissa system på samma sätt som radar, en ljuspuls sänds ut och den returnerade pulsen analyseras. Det är en fråga om både teknik och våglängd/frekvens. Även om teknikerna är olika beskriver systemen olika aspekter av samma studerade objekt och ger tillsammans en mer komplett bild av objektet än vad som skulle erhållas om det bara studerades med ett system.

4.2 Störbegrepp

För att beskriva störning och effekten av störning kan flera olika indelningsgrunder användas. Det vanligaste är att de indelas efter *användningsförfarande, åsyftad verkan* eller *realiseringsmetod*. Dessutom finns olika typer av *förstörande system*. För flera av de nedan uppräknade störformerna är det vidare intressant att diskutera störningens beroende av *bandbredden* hos störsignalen.

Användningsförfarande

Det taktiska/operativa användningsförfarandet kan delas upp efter följande fyra huvudprinciper:

- Bakgrundsstörning "Stand-off-Jamming"
- Medstörning "Escort Jamming"
- Egenstörning "Self-Protection Jamming"
- Närstörning "Close-in Jamming"

Bakgrundsstörning mot radar

Med bakgrundsstörning mot radarstationer menas att störaren befinner sig på ett större avstånd från radarn än skyddsobjektet. Störaren ligger ofta utanför radarns instrumenterade räckvidd. Bakgrundsstöraren strävar också efter att befinna sig utanför motståndarens vapensystemräckvidder.

Bakgrundsstörning syftar primärt till att skydda inkommande objekt mot upptäckt eller att försena upptäckt och därmed insatsbeslut. Störobjekten är framförallt olika långräckviddiga spaningsradarsystem.

För att uppnå störeffekt på långa avstånd inom mikrovågsområdet krävs att störarna ligger ovanför radarhorisonten. Därför är de flesta bakgrundsstörare mot radarsystem flygburna. Genom att koncentrera störningen i vissa riktningar med hjälp

av riktantenner och mycket höga uteffekter kan effektiv störning ske inte bara i huvudlob (d.v.s. i radarns riktning) utan även i sidolob. Se fig. 4.2 nedan.

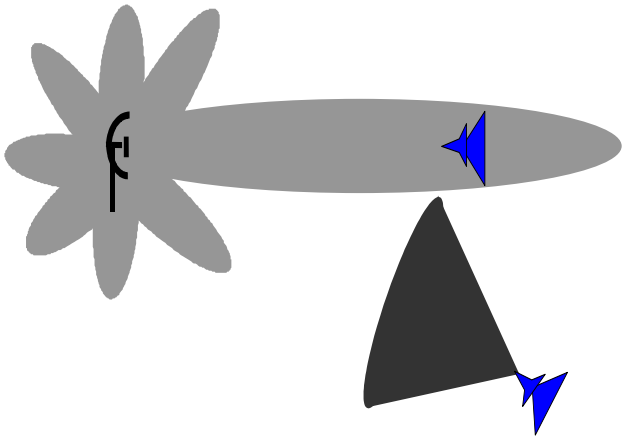

Fig. 4.2. Bakgrundsstörning i sidolob, d.v.s. störeffekten når radarmottagaren via en av sidoloberna. Störaren ligger ofta utanför radarns instrumenterade räckvidd. Störning sätts in mot spaningsradarstationer med medellång eller lång räckvidd.

Medstörning mot radar

Medstörning (ibland kallad eskortstörning) innebär att speciellt utrustade störplattformar, vanligtvis flygplan, eskorterar ett förband i samband med ett anfallsuppdrag. Denna störmetod är aktuell såväl för att skydda de plattformar som inte själva medför störutrustning som för att förstärka effekten av deras eventuella egenskyddsutrustning.

Medstörning har i huvudsak två syften, dels att försvåra eller förhindra upptäckt från radarsystem med lång räckvidd, dels att försvåra och fördröja insatser från olika vapensystem genom att selektivt störa ut deras målinmätningssystem. Störobjekten är primärt lokala spanings- och eldledningsradarsystem som tillhör de hotande vapensystemen. Eftersom medstörarna skall följa sina skyddsföremål krävs det att de har samma tekniska prestanda som flygplanen i övrigt. Medstöraren måste dock i regel vara ett flersitsigt flygplan med störoperatör för att säkerställa att god taktisk effekt uppnås.

På störutrustningen ställs krav på både maskerande brus och vilseledande störformer (avstånds-, vinkel- och hastighetsavhakning).

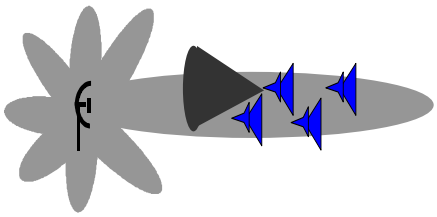

Fig. 4.3. Medstörning. Störare och mål ligger i samma bäring och ungefär på samma avstånd från radarn. Störning sker endast i radarns huvudlob.

Egenstörning

Egenstörningsutrustningar på farkoster syftar primärt till att försvåra målupptäckt, inmätning samt eventuell låsning och följning i sikten och målsökare. Genom olika typer av avhakning och vilseledande störformer förbättras överlevnadsmöjligheterna för plattformen. Störformer som riktar in sig på att bryta en etablerad följning är viktiga.

Egenstörning kan genomföras bl.a. med:
- pyrotekniska störutrustningar (facklor) mot optiska målsökare/sikten
- laser för bländning/störning
- rök/dimma (fartyg, stridsfordon m.m.)
- passiva radarreflektorer (remsor, friflygande/bogserade mål)
- farkostbaserade aktiva störutrustningar ("On-board Jammers")
- aktiva störutrustningar mot radar som släpps eller bogseras ("Off-board Jammers")

Vanliga IR-motmedel är facklor och rök, men det finns många fler. Motmedlen brukar delas upp i grupperna emitterande, spridande, absorberande och störande. Utvecklingen av målsökare går mot högre störfasthet och multispektral teknik, vilket innebär att traditionella facklor ej klarar av att haka av roboten utan det krävs att de bl.a. är spektralt anpassade. Andelen målsökare med bildalstrande tekniker ökar också vilket kräver nya tekniker så som störande laser – DIRCM (Directed IR Countermeasures).

Rök används för olika syften, det kan vara för att avvärja ett uppkommet robothot, men också för att dölja en förflyttning. Därutöver används rök för vilseledning. Röken behöver genereras under hela tiden som skyddet skall fungera, vilket kan göras genom rökgeneratorer eller pyrotekniska störladdningar. I dag finns det en utveckling av multispektral vattendimma som kan ses som en vidareutveckling av IR-röktekniken.

Remsor används ofta som fysiska radarskenmål. På cm-våglängder ger varje remsa mycket liten radarmålarea varför de packas tillsammans i buntar som sprids ut med hjälp av fartvinden (i flygfallet) eller en liten sprängladdning (i fartygsfallet). Remsorna genererar skenekon. Remsor bör ha längd motsvarande en halv våglängd. Remsornas nackdel är att de bromsas upp och får samma hastighet som den omgivande luften. För skydd av flygplan är de därför i huvudsak effektiva mot äldre system utan effektiv dopplerfiltrering.

Den aktiva störformen mot radar är främst vilseledande störning. Radarsignalerna förvanskas genom fördröjning av pulser (avståndsvilseledning), amplitudmodulering, fasfronts- eller polarisationsvridning av pulser (vinkelvilseledning) samt dopplerförskjutning av signalen (hastighetsvilseledning).

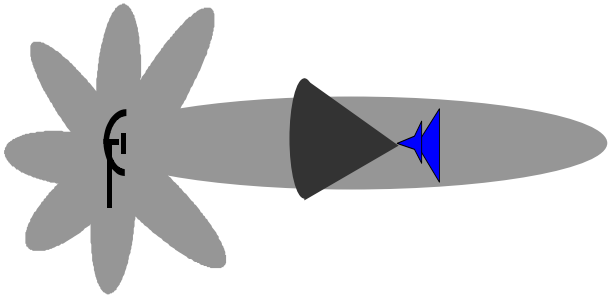

Fig. 4.4. Egenstörning mot radar. Mål och störare är samma enhet. Egenstörning används huvudsakligen som egenskydd.

Närstörning

Närstörare är störsystem som är placerade mycket nära radar- eller radiomottagaren. När störning sker på nära håll reduceras behovet av störeffekt mycket kraftigt, ofta ner till några watt. Detta betyder att störsändaren kan göras heltransistoriserad, enkel och billig. Den kan t.ex. föras fram av en UAV. Fällda eller utskjutna engångsstörsändare kan verka mot såväl radarsystem som radiosamband.

Närstörning mot radarstationer kan oftast ske inom radarantennens närfält där antennloben inte är fullt utbildad och sidolobsundertryckningen därför är dålig. En principiell fördel med närstörning är att opredikterbara byten av frekvens i radarn inte duger som störskydd eftersom störaren kan mäta in och störa de nya radarpulserna innan dessa har träffat målet.

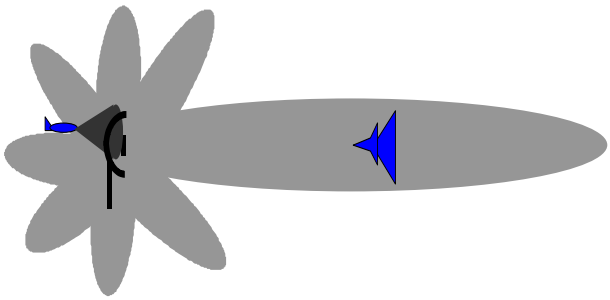

Fig. 4.5. Närstörning mot radar. Störarna befinner sig alldeles i närheten av radarn. Störarna kan i detta fall vara fällda eller utskjutna engångsstörsändare eller bäras av UAV.

Åsyftad verkan

Åsyftad verkan bygger på vilken tänkt verkan störningen skall få. Man skiljer här på huvudgrupperna:

- Maskerande störning "Noise-Jamming" (ngt oegentligt)
- Vilseledande störning "Deception Jamming"
- Mättande störning "Saturation Jamming"

Maskerande störning

I radarfallet utnyttjas den maskerande störformen mest för bakgrunds- och medstörning och då i form av maskerande brusstörning eller remsor.

Vilseledande störning

Vilseledande störformer utnyttjas främst för egenskydd av farkoster, men någon absolut koppling mellan indelningarna finns ej.

Mättande störning

Mättande (informationsöversvämmande) störning kan förväntas bli allt mer vanlig. Speciellt kommer digitala radiofrekvensminnen i störsystem att kraftigt förbättra möjligheterna att såväl mätta en radarmottagare med ett otal falska mål, som att möjliggöra mer avancerade vilseledningss- och avhakningsförlopp. Även måldataöverföringen och beslutsfattandet på högre nivå kan bli utsatt för mättning.

Realiseringsmetod

Ytterligare en indelningsgrund är realiseringsmetoden för störningen, där huvudgrupperna är:

- Aktiv störning "Active Jamming"
- Passiv störning "Passive Jamming"

Aktiv störning mot radar realiseras med störsändare (mark-, sjö- och flygbaserade). Passiv störning sker genom reflektorer, ofta i form av remsor men också från fjärrstyrda signaturförstärkta farkoster.

Förstörande system

Exempel på förstörande system är:

- Signalsökande robotar "Anti Radiation Missiles", ARM
- Elektromagnetiska vapen "High Power Microwaves" (HPM) och laservapen

Signalsökande robotar mot radar

Signalsökande robotar (ssrb) är de viktigaste och mest frekvent förekommande förstörande vapnen inom telekrigsområdet. De är avsedda att sättas in mot elektromagnetiska strålningskällor, främst spanings- och eldledningsradarstationer.

Avfyrning sker ofta på hög höjd med en brant slutfas ner mot målet. Detta bl.a. för att utnyttja den begränsade täckning som radarn oftast har rakt uppåt.

En ssrb har en passiv mottagare, som inom ett snävt frekvensområde känner igen vissa i förväg definierade radarsystemparametrar ur ett signalbibliotek.

De flesta typer av ssrb låser på strålningskällan före avfyrning men det finns även sådana som kan låsa autonomt efter fällning. Moderna ssrb har minneshållning och kan fortsätta att styra in mot målet även om sändaren skulle stängas av. Som komplement kan de också ha en IR- eller millimetervågssensor för slutfasstyrning. En typ av ssrb (ALARM) kan ligga i väntläge hängande i fallskärm, för att sedan gå mot ett radarmål när det tänder sin radar.

Ett problem för signalsökande robotar är att kunna utskilja målsignalen i den ofta mycket täta signalmiljön, samt att signalen varierar mycket kraftigt i styrka beroende på radarns antennrörelser. Utvecklingen av ssrb väntas ge bättre signaldiskriminering, bättre intelligens, mindre storlek och mindre radarmålyta. Dessutom kommer på sikt avancerade signalsökande jaktrobotar att tas fram för bekämpning av nosradar och flygande spanings- och stridsledningsradar.

Elektromagnetiska vapen

Huvudsyftet med *HPM-vapen* är att störa eller förstöra funktionen hos elektronikberoende system. Även en kortvarig störning kan innebära att ett kvardröjande fel uppstår, t.ex. att en bil eller dator måste startas om. För ett flygplan eller en robot kan ett sådant fel vara förödande. Inträngningen i målet kan ske antingen via dess egen antenn (framvägskoppling) eller via plåtskarvar och liknande (bakvägskoppling). Den elektriska skärmningen i målet är helt avgörande för sårbarheten. En modern tålighetsspecifikation för flygplan och robotar är 10 kV/m. En HPM-sändare med antennstorleken 1 m och 8 GW uteffekt får en räckvidd av c:a 5 km mot ett sådant mål, d.v.s. samma storleksordning som för luftvärnsartilleri.

Med *laservapen* menas lasrar som i första hand är konstruerade för att verka mot andra sensorer, antisensorlasrar, men även sådana med kapacitet att bränna sönder konstruktionsmaterial, s.k. strukturförstörande lasrar. Den stora fördelen med ett laservapensystem är den snabbhet med vilken den kan lokalisera, mäta in och verka mot ett hot. Några nackdelar är att systemen kräver fri sikt till målet och att verkansverifiering inte är lätt.

Bandbredd hos störsignalen

Störning kan vara smalbandig eller bredbandig.

Smalbandig störning

Vid smalbandig störning är bandbredden hos störaren av samma storleksordning som det störda systemets bandbredd. Fördelar vid smalbandsstörning är möjligheterna att koncentrera störeffekten till rätt frekvenskanaler. För att få god störverkan vid smalbandig störning krävs en noggrann frekvensinmätning av de system som skall störas. Ett speciellt problem är att mätning måste göras fortlöpande under ett störförlopp eftersom systemet annars enkelt kan undandra sig störningen genom att byta frekvens. Beroende på mottagar- och sändarenhetens placering på störaren kan det ibland vara möjligt att "lyssna" under pågående störning, men oftast måste korta uppehåll i störningen göras för att medge "lyssning" (look-through). I bägge fallen krävs snabba och noggranna mottagare för signalbehandlingen.

Användning av digitala minnen ger goda möjligheter att optimera den smalbandiga brusstörsignalen.

Bredbandig störning

Bredbandigt brus, där störarens frekvenstäckning sträcker sig över ett stort frekvensintervall har fördelen att:

- i stort vara oberoende av det störda systemets eventuella frekvensväxling.
- ingen look-through behövs

Den stora nackdelen med bredbandsstörning är att störeffekten blir utspridd över stor bandbredd och med liten effektiv störverkan i målet. En annan nackdel är att det är lätt att med s.k. automatisk sidolobsundertryckning i radarantennen kraftfullt dämpa sådan störning.

4.3 Telekrigets roller

Sett ur ett överordnat perspektiv kan telekrig fylla framförallt tre roller: underrättelseinhämtning, ledningskrigföring och duell.

4.3.1 Underrättelseinhämtning

Telekrig i underrättelsesammanhang kan bl.a. exemplifieras med den telekrigtropp som finns i Kosovo. Denna telekrigtropp bemannas med personal från Försvarsmakten och FRA och bedriver signalspaning. Troppen består av en KOS- (Kommunikationssignalspaning) och en analysenhet.

4.3.2 Ledningskrigföring

Ledningskrigföring är ett begrepp som bl.a. innefattar delar av telekrigföringen och som har aktualiserats under det senaste decenniets konflikter.

Den definition av ledningskrigföring vi har i Sverige avviker från den internationella såtillvida att vi valt att bara ta med de offensiva delarna, medan vi hänför skydd av eget ledningssystem till funktionen ledning.[13]

Det övergripande operativa syftet med ledningskrigföring är att bidra till att skapa ledningsöverläge för våra stridskrafter. Detta sker genom att påverka motståndarens omvärldsuppfattning och nedsätta hans ledningsförmåga. Han hindras därigenom från att utnyttja sina stridskrafters potential på grund av begränsningar i omvärldsuppfattningen och ledningsförmågan. Ledningskrigföring kan härigenom vara av avgörande betydelse för resultatet av operationen. Ledningskrigföringens roll illustreras i fig. 4.6. Det är viktigt att peka på det stora behov av underrättelseinformation som finns för att det skall vara möjligt att genomföra en effektiv ledningskrigföring.

[13] Huvudstudie ledningskrigföring – slutrapport (öppen version). HKV 21 120:60831, 1999-01-27; Huvudstudie ledningskrigföring – slutrapport. HKV H21 120:8462, 1998-12-03.

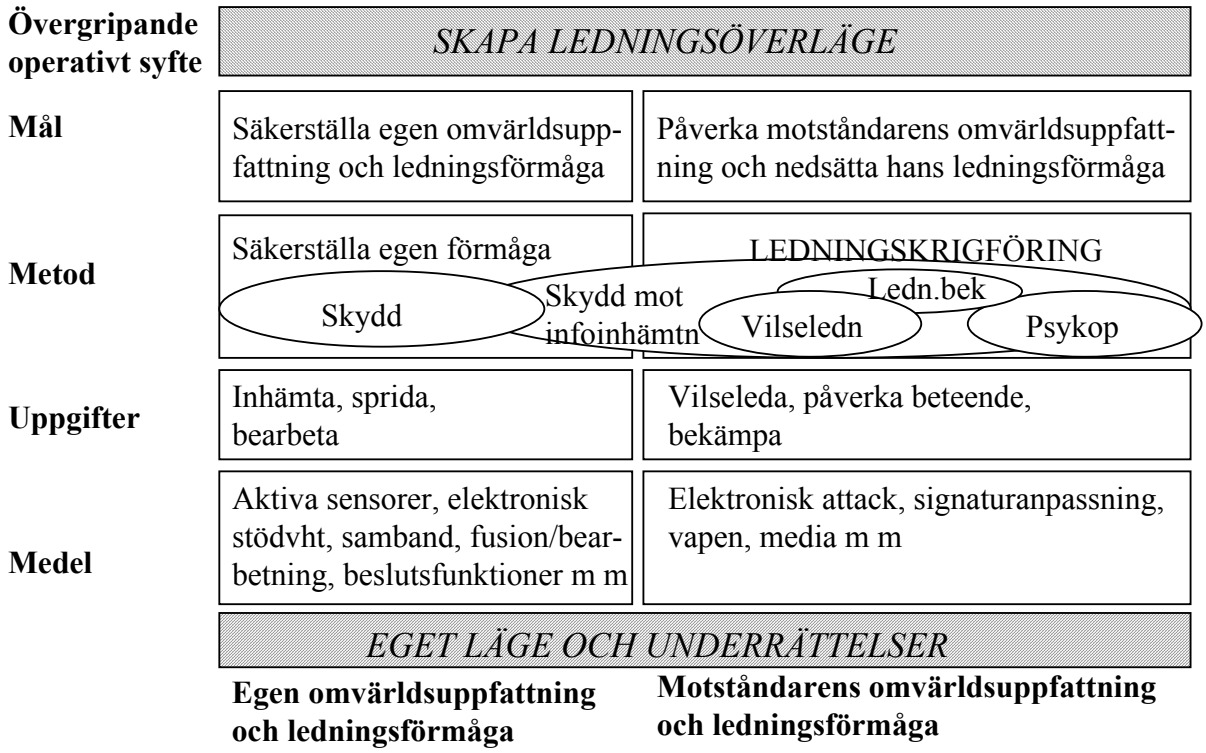

Fig. 4.6. Illustration av ledningskrigföringens stöd till det operativa syftet att uppnå ledningsöverläge genom att påverka motståndarens omvärldsuppfattning och nedsätta hans ledningsförmåga, samt förhållandet mellan ledningskrigföringen och säkerställandet av egen ledning. Som grund för ledningsöverläge krävs dels en god uppfattning om eget läge, dels ett mycket gott underrättelseläge. Skydd mot informationsinhämtning bidrar både till att skydda egen ledning och till att möjliggöra ledningskrigföring.

Ledningskrigföringen har till syfte att slå mot ledande personer och ledningssystemet. Mål kan t.ex. vara politiska eller militära ledare, noder i kommunikations- och informationssystem, enskilda ledningsplatser eller strategiska underrättelseresurser.

4.3.3 Duell

För att kunna sända ut förband i internationella insatser krävs i många fall egenskydd (ibland kan det även vara ett krav för att få deltaga). Detta gäller bl.a. VMS (varnings- och motverkanssystem) till flygplan, något som bl.a. uppmärksammades när Hercules-flygplan skulle utnyttjas för transporter ner till Bosnien. Även laserskyddsåtgärder för personal har diskuterats, bl.a. mot bakgrund av att amerikanska helikopterbesättningar har blivit belysta med laser i Bosnien.[14]

De krav som ställs i samband med internationella insatser, bl.a. avseende varnings- och motverkanssystem som medger duellförmåga mot eventuella motparters system, aktualiseras också i och med att Sverige anmält ett antal förband för

[14] Det är möjligt att det i de åtminstone två fall som rapporterats från Bosnien rört sig om ganska enkla lasrar, av karaktären pekare eller motsvarande.

deltagande i multinationella internationella insatser. Detta omfattar förband från samtliga försvarsgrenar.

I de internationella insatser som genomförts under senare år har det ibland hänt att förband ej tillåtits deltaga p.g.a. bristande egenskydd på plattformar. Det gällde t.ex. mekaniserade förband utan laservarnare på stridsfordon under KFOR inledande fas. Kravet på laservarnare fick bl.a. till följd att amerikanska stridsfordonsförband och attackhelikopterförband inte tilläts deltaga. Det är viktigt att här påpeka att kraven på egenskydd för plattformar varierar p.g.a. uppdrag och miljö och bestäms av den operative chefen (Force Commander). På samma sätt har krav på robot-skottvarnare på flygplan och helikoptrar som insatts på Balkan inneburit att vissa nationers flygplan ej tillåtits deltaga.

5 Utnyttjande av telekrigföring i konflikter

Nedan ges några exempel på hur telekrigföring utnyttjats under några av de senaste decenniernas konflikter. Bekaadalen 1982 brukar ofta framhållas i samband med att telekrigföringens möjligheter diskuteras. Den israeliska sidan utnyttjade då skenmål för att lura luftvärnsradar att ”stråla”, signalspaning mot radar, störning av radar m.m. Denna konflikt var dock i detta avseende ganska asymmetrisk, d.v.s. israelerna var överlägsna avseende telekrig.

De konflikter som var aktuella under 1990-talet var bl.a.:
- Desert Storm
- Kosovokriget

Dessa hade ganska olika karaktär.

5.1 Desert Storm

Desert Storm innebar ett genombrott för rymdbaserade system (för övervakning och navigering), kryssningsrobotar, stealth som medel mot luftförsvaret och avancerad radar i kritiska roller (JSTARS[15], SEAD[16]). Styrda vapen (laserstyrda, elektrooptiska, signalsökande) kom också att få stort genomslag.

Desert Storm gav sensorer möjlighet att verka fullt ut, medgav 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 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. D.v.s. de amerikanska stridskrafterna släpper inte in stealthflygplan över motståndarterritorium utan kraftigt telekrigunderstöd. 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.

---

[15] JSTARS (Joint Surveillance Target Attack Radar System) är ett flygburet system för markövervakning. Det testades som prototyp under Desert Storm och Bosnieninsatserna. Den första serieleveransen skedde 1996. Se även Kindvall, G., ”Reserapport från Air Power Conference 1997-02-27--28, London”, FOA-R--97-00554-201--SE, november 1997.

[16] SEAD (Suppression of Enemy Air Defence) innebär utnyttjande av olika metoder – störning, signalsökande robotar etc. – för att nedhålla och bekämpa framförallt motståndarens luftvärn.

Signalsökande robotar kom att får stor effekt. Mer än 1000 st. HARM (High speed Anti-Radiation Missile) avfyrades och ledde på 6 dagar till att endast 5% av de irakiska radarsystemen var på (inledningsvis var 100% av systemen på).

Saddam var en ”perfekt fiende” för kvalificerade stridskrafter. Det är knappast troligt att det blir så igen.

5.2 Kosovokriget

Kosovo blev något annorlunda, eftersom vädret kraftigt kom att försvåra utnyttjandet av elektrooptiska sensorer. Det var dåligt väder och regnade också mycket. 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 (radarsystemen var 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 utnyttjandet av skenmål och avstängda radarsystem. 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, ställde krav på kontinuerlig bekämpning av luftförsvaret och krävde ISR (Intelligence, Surveillance and Reconnaissance) och SEAD hela tiden. Nato-flygplan fick ej flyga under 15.000 fot (4.500 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. Serberna gömde sig tidigare.

I en analys av kriget står[17]:

”NATO's air defense suppression forces were committed heavily to this campaign. U.S. systems such as RC-135 Rivet Joint electronic intelligence aircraft and EA-6B tactical airborne electronic warfare aircraft were employed in numbers roughly equivalent to those anticipated for a major theater war, and even then were heavily tasked. We need to find innovative and affordable ways to exploit our technological skills in electronic combat to bring greater pressure to bear on a future enemy's air defense system.”

[17] Ur JOINT STATEMENT ON THE KOSOVO AFTER ACTION REVIEW (presented by Secretary of Defense William S. Cohen and Gen. Henry H. Shelton, Chairman of the Joint Chiefs of Staff, before the Senate Armed Services Committee, October 14, 1999)

Här betonas behovet av s.k. ”low density/high demand assets”. Detta syftar bl.a. på EA-6B. Dessa telekrigflygplan anses mycket viktiga för skydd.

Kosovo var ett speciellt krig, med mycket speciella förutsättningar. Bl.a. kan det tyckas att man från amerikansk sida satte sig i en ogynnsam situation från början genom att president Clinton sade att ”we won´t deploy ground forces”. USA:s utrikesminister Madeleine Albright sade också att hon trodde att kriget skulle vara slut på 4-5 dagar. Dessa uttalanden kunde lätt få den jugoslaviska sidan att tro att det bara var att härda ut en kortare tids flygattacker. En klassisk ”undeception act”!

Här är vi inne på förmågan att genomföra informationsoperationer. Serberna använde civila som skydd, lät dem marschera med de militära styrkorna och befinna sig vid militära mål. Eftersom Nato-sidan inte ville skada civila kunde man inte agera. Utifrån ett Public Affairs-perspektiv skapades en situation där serberna medvetet dödade civila, men ingen såg det, medan Nato av misstag dödade civila och världen såg det. Det är således inte alltid det som händer som är det viktiga utan hur det upplevs i media.

6 Teknikutveckling

När det gäller teknikutvecklingen är det viktigt att se på de möjligheter som finns, vilka hot och möjligheter detta kan innebära och hur realiserbar tekniken är.

I avsnitt 3.1 presenterades ett antal ur ett telekrigperspektiv intressanta tankar kring teknikutveckling som finns i årsrapporten från perspektivplaneringen 2001-2002. Här är avsikten att diskutera områden med relevans för telekrigets medel och motmedel.

Inledningsvis är det viktigt att förstå att de konflikter vi talar om i framtiden kan försiggå mellan parter med mycket olika teknikniv å, att det kan handla om konflikter där en invasion inte är möjlig eller önskvärd (jfr. Kosovo), att det kan komma att förekomma nya typer av hot, att gränsen mellan civilt och militärt kan komma att bli allt otydligare, att mycket kan komma att handla om att behärska informationsflödet (den som ”ser allt” kan genomföra striden på sina villkor), att de traditionella plattformarnas betydelse som vapenbärare kan komma att minska till förmån för rollen som ”informationsknutpunkt”, att striden alltmer kan komma att handla om att behärska luftrummet och rymden, att allt fler obemannade plattformar kan komma att få fler roller m.m.

För att bara nämna ett exempel uppges Kina ta fram HPM-vapen som skall kunna neutralisera t.ex. ett hangarfartyg, d.v.s. göra hangarfartyget sårbart för andra angrepp.

Nedan presenteras översiktligt utvecklingen inom ett antal ”telekrigrelaterade” teknikområden.[18]

6.1 Samband och kommunikation

Det pågår en snabb utveckling mot större bandspridning, bl.a. genom direktsekvenskoder och frekvenshopp, där signalerna kan döljas i det allmänna bruset eller på annat sätt göras svårupptäckta. Utvecklingen drivs snabbt framåt av civila krav. Civila kommunikationsnät används allt mer även för militär information. Militära system blir därigenom sårbara genom den civila infrastrukturen.

Teknikutvecklingen ställer nya krav på signalspaningssystem för detektering och positionering, samtidigt som det blir mycket svårt att förutse vilken teknik motparten har att tillgå. Störning av dessa nya sambandsmetoder kräver nya störmetoder

[18] Underlag till texten har hämtats från ett antal källor. Två viktiga källor har varit ”Försvarsmaktens funktionsplan för telekrigföring, del 1”, HKV 12 860:68453, 1999-08-04, samt ”FOI orienterar om Elektromagnetiska vapen och skydd”.

samtidigt som risken för oavsiktlig störning ökar då den nya tekniken medger samtidigt utnyttjande av samma frekvensområde.

Användningen av kommunikationssystem vid våglängder som ger hög absorption i luft (t.ex. 60 GHz, där syre absorberar) kan förväntas öka. Sådana system kan användas för korthållskommunikation, t.ex. för intern kommunikation inom företag.

6.2 Signalspaning

Metoder baserade på digital signalbehandling kommer att medge bättre precision och framförallt bättre identifiering av emittrar, även snabbsändande och frekvensspridda sådana. Viktiga teknikområden är här digitala radiofrekvensminnen (DRFM), mottagning av direktsekvensspridda signaler och avancerad databashantering. Flygburna farkoster, företrädesvis UAV:er och satelliter, kommer att utnyttjas i allt större utsträckning för signalspaningsinsatser, där våglängdsområdet kommer att sträcka sig från kommunikationsbanden via radarbanden upp till mmvåg.

Genom att låta signalspaningsinformation korreleras med övrig information från aktiva och passiva sensorer kan den utnyttjas i nära realtid som måldata i informationssystem.

6.3 Radar

Inom radarområdet sker idag en mycket snabb utveckling inom signal- och databehandlingsområdena. Den syntetiska aperturradarn (SAR)[19] ger exempelvis allt bättre upplösning. SAR används bl.a. i JSTARS, ett system som redan nämnts ovan. Det är också möjligt att separera sändare och mottagare, s.k. bi- eller multistatisk radar.

HF-radar (frekvensområde ca 10-100 MHz) kan ge förbättrade möjligheter att upptäcka signaturanpassade mål. HF-radar skapar resonanser, eftersom våglängden hos strålningen är av samma storleksordning som vanliga plattformars fysiska utbredning.

En typ av radarsystem som möjligen kan bli aktuell är tysta radarsystem. Dessa fungerar genom att utnyttja annan, reflekterad, strålning – t.ex. FM-strålning från kommersiella radiostationer – för att detektera och följa flygplan. Ett exempel på ett sådant system under utveckling är Silent Sentry. System av denna typ kan antas fungera bäst i tätbebodda områden där det finns ett antal FM-sändare.

[19] Syntetisk aperturradar (SAR) utnyttjar spaningsplattformens rörelse för att skapa en lång linjär antenn på syntetisk väg. SAR förutsätter digital signalbehandling.

Framtida radarsystem kan således förväntas bli tystare, mer störtåliga och få högre prestanda.

Genom utveckling av allt bättre metoder för att styra antennloben minskar effekten av med- och bakgrundsstörning samtidigt som störföljning gör att konventionell egenstörning får begränsad effekt. Nya störformer baserade på digitala radiofrekvensminnen (DRFM) utvecklas för att möta radarutvecklingen. Släpade eller utskjutna skenmål kan användas för att möta riskerna med störföljning.

6.4 Laser

Laser har potential som vapen, som sensor, som skydd (t.ex. i ett VMS) och för kommunikation. Laservapen diskuteras i hela skalan från bländning av sensorer till förstörande verkan mot ballistiska missiler.

Antisensorlasrar finns utvecklade för användning på fordon, fartyg och flygplan och av enskilda soldater mot sensorer inom både det visuella och det infraröda området mot såväl spanings- som målsökarsystem.

Högenergilasrar utvecklas också. I USA har lyckade försök att förstöra ballistiska missiler utförts och Airborne Laser (ABL) är under utveckling. Systemet tas fram för att bekämpa taktiska ballistiska missiler redan i startfasen. Då kan även en liten skada (spricka) i missilen räcka p.g.a. de stora spänningarna i materialet. Sannolikheten är också större att resterna av missilen (och ev. innehåll) ramlar ner över det område från vilket den skjutits upp. Även markbaserade lasersystem för luftförsvarstillämpningar är under utveckling. En lyckad demonstration där en laser användes för att bekämpa artillerigranater skall ha genomförts i USA.

Laser kan enligt ovan också vara en komponent i ett varnings- och motverkanssystem (VMS). Här fokuseras allt mer intresse mot s.k. DIRCM-system (Directed IR Countermeasures) för att kunna bekämpa moderna elektrooptiska robotar, vilka kan diskriminera traditionella motmedel som facklor.

Även om lasertekniken inte fungerade fullt ut i Kosovo – vädret var i vägen för laserstyrda bomber etc. – finns det således många intressanta militära tillämpningar av lasertekniken. Vilka som verkligen kommer att införas är oklart.

Utvecklingen av skydd mot avsiktliga och oavsiktliga ögonskador från olika typer av stridsfältslasrar har hög prioritet i många länder. Ögonsäkra lasrar utvecklas också för allt fler tillämpningar.

Laser som störare och vapen är ett nytt och kraftfullt medel inom ramen för krigföringen i det elektromagnetiska området – telekrigföringen.

6.5 HPM (High Power Microwaves)

Med HPM-vapen avses vapen baserade på HPM-strålningens störande eller förstörande verkan på elektroniksystem samt konventionella mikrovågskällor, t.ex. kraftiga radarkällor, om syftet med deras användning är att störa eller förstöra. HPM-vapen är icke-dödliga, och kan därför bedömas ha en låg insatströskel. Vapnen kan sättas in i inledningsfasen av en konflikt för att lamslå motståndaren, eventuellt som en del i en strategi för informationskrigföring.

Viktiga orsaker till att HPM utgör ett hot mot militära och civila system är:

- Den allt flitigare användningen av elektronik, också för säkerhetskritiska funktioner
- Den snabbare och allt mer miniatyriserade – och därmed känsligare – elektroniken
- Trenden mot reducerad skärmverkan på grund av användning av elektriskt halv- eller oledande material, såsom plaster och kompositmaterial, för de höljen som omger elektroniken.

Strålning från HPM-vapen kan tränga in i målet på två sätt, via framvägskoppling eller via bakvägskoppling. Vid framvägskoppling tränger strålningen in genom antenner etc. Vid bakvägskoppling tränger strålningen in via öppningar i höljen och via kablage för att sedan koppla till elektroniken.

En central fråga är om framtida HPM-vapen kommer att vara så effektiva och kunna verka på så stora avstånd att de kan uppfattas som intressanta alternativ eller komplement till andra vapen. Utvecklingen kan starkt komma att påverka krigföringen beroende på verkansavstånden. HPM-vapen kommer att utvecklas mot allt högre effekter, pulsrepetitionsfrekvenser och antennförstärkningar samt förses med intelligens i form av signalmodulering.

Idag är generering av och skydd mot HPM etablerade forskningsområden. USA och Ryssland dominerar forskning och utveckling av kraftfulla stationära HPM-källor. Beträffande skydd mot HPM bedrivs relativt omfattande verksamhet i ett flertal länder.

Enligt uppgift användes Tomahawkrobotar med HPM-stridsdel i Gulfkriget och Kosovokriget. Det förekommer även uppgifter om att HPM-vapen och låg-frekventa pulsvapen har använts som sabotage- och terroristvapen mot civila system.

Laser och HPM – elektromagnetiska vapen – är idag etablerade civila och militära forskningsområden. Modern materiel blir allt mer avancerad och beroende av elektronik. Det är därför viktigt att följa utvecklingen inom skydds- och verkansområdet. Elektromagnetiska vapen kommer att vara en viktig del av telekrigföringen i framtiden.

6.6 IR-system

Inom IR-området utvecklas små bildalstrande sensorer. Pris och prestanda på dessa sensorer kan innebära att mängden slutfasstyrda vapen för mark-, sjö- och luftmål ökar drastiskt. Dessa sensorer är mycket svåra att vilseleda på konventionellt sätt med facklor.

Störmetoder är under utveckling, bl.a. laserbländning, avancerade skenmål och metoder för att minska signaturen såsom signaturanpassning, termisk rök och vattendimma. Olika typer av nya sensorer kommer att ha olika sårbarhet. Scannande sensorer kan t.ex. förväntas vara mindre sårbara än stirrande sensorer. I gengäld ger stirrande sensorer bl.a. säkrare upptäckt av mål inom synfältet.

6.7 Satellitbaserade system

Satelliter medger stora möjligheter nu och i framtiden och kan användas t.ex. för navigering, kommunikation och spaning.

Moderna (satellit)navigeringssystem har redan idag stor betydelse för vapeninsatser och ledning av förband. Utvecklingen går mot bättre prestanda, lägre pris och civil teknik. Äldre vapensystem kan på detta sätt ges förbättrade prestanda. Detta leder till ett ökat intresse av att störa satellitnavigeringssystem, s.k. navigationskrigföring (NavWar). Se även avsnitt 3.4 och 8.2.4.

Den ökande användningen av satellitkommunikation, inte minst billiga civila system med höga prestanda, ställer nya krav på både spaning och bekämpning.

I framtiden kommer det sannolikt att finnas satellitbilder med hög upplösning som säljs av kommersiella aktörer till den som är villig att betala. Jfr IKONOS.[20] Ett exempel på en bild tagen av denna satellit ges i fig. 6.1. Den föreställer Washingtonmonumentet i Washington.

[20] IKONOS är en kommersiell satellit. Den spanar i våglängdsområdet 0,45-0,90 μm. Upplösningen är 1 meter. De första bilderna togs över Washington 30 september 1999. Bilder går att köpa via internet. Se www.spaceimaging.com.

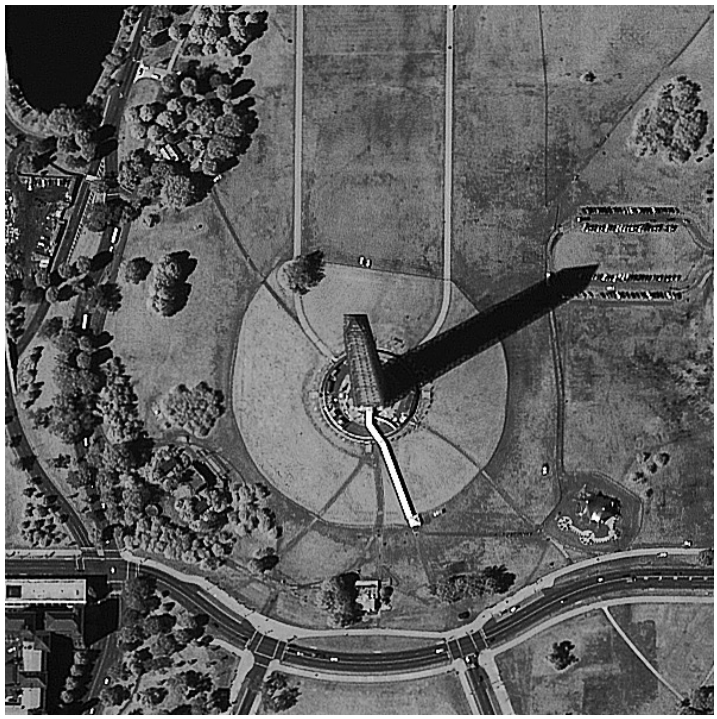

Fig. 6.1. Washingtonmonumentet i Washington fotograferat av den kommersiella fotospaningssatelliten IKONOS. Källa: http://www.spaceimaging.com.

Förekomsten av sensorutrustade satelliter kan göra det svårt att dölja trupprörelser och andra verksamheter och skapar därmed incitament för satellitkrigföring. Hot mot satelliter kan t.ex. vara störning, spoofing (att luras, vilseleda), fysisk bekämpning och laserbländning av satellitens sensorer. Det har också förekommit uppgifter om hackare som tillfälligt tagit över satelliter och påverkat deras banor. Antisatellitvapen, rymdbaserade lasrar m.m. diskuteras också (eller finns kanske redan).

För att möta hoten kan det bli aktuellt med signaturkontroll, manövrerbara plattformar, aktiva motmedel m.m.

Att satelliterna kan ägas av kommersiella aktörer, d.v.s. ej av stater, kan ge speciella problem.

I USA ser man p.g.a. militärens och samhällets större beroende av rymdbaserade system att det kan bli aktuellt att försvara rymdintressen. Satellitkrigföring – eller rymdkrigföring – kan således vara en nisch där telekrigföring kan fylla en viktig funktion. I och med att USA i mitten av december 2001 officiellt meddelade att man skall dra sig ur ABM-avtalet (Anti-Ballistic Missile Treaty), som ingicks 1972 med dåvarande Sovjetunionen och innebär en kraftig begränsning av möjligheterna att bygga upp ett försvar mot ballistiska missiler, ökar också sannolikheten för en upprustning i rymden.

6.8 Obemannade farkoster

UAV:er finns idag, men kommer förmodligen att bli mer och mer använda i framtiden. Man kan t.ex. fråga sig hur många av framtidens flygplan som behöver vara bemannade. Jämför t.ex. B-2, som var stationerade i USA och flög fram och tillbaka till Kosovo varje gång en insats gjordes. Av alla timmar i luften var de ca 10 minuter över målet, var skyddade och släppte sina bomber. Behövs människor i flygplanen för att göra detta? Så kallade UCAV:er (UCAV = Unmanned Combat Air Vehicle) studeras redan i många länder och utveckling av sådana kommer sannolikt att ske.

UAV:er är också intressanta ur ett telekrigperspektiv, eftersom de både kan användas som telekrigplattformar och bekämpas med telekrig (störning etc.).

6.9 Vilken väg?

Men hur blir det? Det har många gånger visat sig hur svårt det är att sia om teknikutvecklingen. Det är som att spå väder – en del blir rätt och en del blir fel. Vissa delar av utvecklingen bedöms ganska rätt, andra underskattas och ännu andra överskattas. Det är dock likväl viktigt att försöka sia om utvecklingen eftersom det är en av de viktigaste byggklossarna när vi föreställer oss framtidens samhälle. Och en av de tydligaste utvecklingstrenderna vi ser idag inom den militära sektorn är ett större beroende av civil teknik och civila system, t.ex. för kommunikation. Det är således den civila teknikutvecklingen som driver på.

7 Värdering

Efter att i de tidigare avsnitten ha diskuterat behovet av att se nya möjligheter för telekrig och att se dessa i ett vidare perspektiv – t.ex. kopplat till försvarsmaktens utveckling eller till beroendet av civila strukturer (satelliter, kommunikation) – är det dags att komma in på värdering, d.v.s. metoder för att bedöma effekten av olika system och åtgärder. Inledningsvis kommer en av de viktigare metoderna för värdering – spel – att beskrivas översiktligt. Ibland kan gränsytan mellan spel och värdering vara otydlig, eftersom spel kan utnyttjas bl.a. för värdering medan värdering bl.a. kan bedrivas med hjälp av spel. Även när värderingsverksamheten inte kallas spel är det inte ovanligt att scenarier eller typsituationer ligger som en grund för de resonemang som förs.

7.1 Spel

Spel kan ha olika syften. Det kan vara att lära ut, generera kunskap (genom den dynamik som uppstår i grupper), värdera, förankra (det är ett viktigt syfte) samt pröva och kontrollera.[21]

De spel som bedrivs av FOI och Försvarsmakten är i allmänhet öppna, d.v.s. de som deltar vet ”allt” om förutsättningar, strukturer m.m. Denna typ av spel är vanliga vid värdering. Ibland finns dock behov av att bedriva mer eller mindre slutna spel – d.v.s. att bara ge de deltagande begränsad kunskap. Detta innebär t.ex. att deltagarna tvingas reagera snabbt på den andra sidans åtgärder. Denna typ av spel är kanske mest lämpade för övningssammanhang, men kan också vara rimliga vid vissa värderingssituationer.

Vid spel (och värdering) behövs en hel del underlag. Tre typer av underlag är avdömningsunderlag, modeller och spelkort. Avdömningsunderlag är beräkningsunderlag som kan utnyttjas för att avdöma uppkomna situationer under spelet. Det kan vara verkan av ett vapensystem eller räckvidden för en radar under olika ostörda och störda förhållanden. Vid spel på lägre nivå, systemnivå, kan detta underlag behöva vara ganska detaljerat, medan det vid spel på operativ nivå kan och bör vara betydligt mer översiktligt. Här talar man t.ex. om aggregerade verkansvärden för förband. Det är ofta svårt att upprätta avdömningsunderlag, d.v.s. att göra faktiska beräkningar. Ofta tar sådant mycket lång tid och idealt bör även simuleringar genomföras. Således tvingas man ofta i en värdering nöja sig med att finna viktiga faktorer, studera dessa strukturerat och avdöma med hjälp av enkla ”tumregler”.

---

[21] För en diskussion om spel utifrån ett telekrigperspektiv hänvisas till Kindvall, G., Looström, C. och Tarras-Wahlberg, B., ”Idéer till värdering av telekrig i krigsförloppsspel”, FOA-R--96-00251-1.1--SE, december 1996. För en bredare diskussion kring spel hänvisas till Dreborg, K-H., ”Spela för att lära”, FOA rapport C 10356-1.2, 1993.

Modeller kan vara såväl beskrivningar av fenomen som fullfjädrade simuleringar. I fallet simuleringar är problemet att de ofta vore bra att ha tillgång till, men ganska sällan finns utvecklade, verifierade och validerade när de hade behövts. Simuleringsmodeller tar ofta ganska lång tid att utveckla. Dels behövs kunskap om problemet för att kunna göra en modell, dels är programmering, verifiering och validering tidsödande processer. En väg ut ur detta är att förenkla problemen och göra mycket enkla simuleringar. Detta kan ibland fylla behoven. En annan lösning kan vara att utnyttja olika ramverktyg för att göra det möjligt att snabbare få fram översiktliga simuleringar. Simuleringsmodeller behövs också för att ta fram avdömningsunderlag.

Spelkort är helt enkelt system- eller förbandsbeskrivningar av varierande detaljeringsgrad beroende på tillämpning.

Oftast syftar inte spel primärt till att värdera telekrig och möjligheterna att diskutera telekrigåtgärder kan vara mycket begränsade under det faktiska spelet. Detta pekar på ett behov av efteranalys då en djupare analys av ett antal situationer m.a.p. telekrig kan genomföras. Ibland är det också relevant att efter spelet bedöma huruvida telekrig utnyttjats rätt eller om det behövs ändringar och genomförande av variationsspel.

7.2 Värdering av teknik

7.2.1 Allmänt

Det pågår kontinuerligt arbete med värdering av teknik i försvarstillämpningar. Som grund för detta bedrivs arbete med förutsägelser om framtida teknikutveckling, bl.a. inom ramen för den teknikavtappning som årligen sker från FoT-verksamheten till Försvarsmaktens långsiktiga planering (Perp-processen). Utöver detta genomförs workshops om framtida trender (möjligheter, militära konsekvenser) och studier av intressanta tekniker.

Teknikvärdering kan också komma att bli aktuellt som ett underlag för inriktning av forskningsverksamheten på FOI, d.v.s. som en utvärdering av gjorda eller planerade satsningar mot kriterier som t.ex. kan handla om möjlighet att förvärva kompetensen på annat håll, den potentiella tillämpbarheten av resultaten etc. Som en konsekvens av terrordåden i USA den 11 september 2001 blir det också sannolikt viktigt att se på teknikutvecklingen ur ett aktörsperspektiv, d.v.s. vad kan olika aktörer tänkas utnyttja för olika tekniker och vad kan de åstadkomma med dem.

En typ av övergripande studier som bedrivits kopplat till teknikutvecklingen är de Teknisk-Strategiska Studierna (TSS).[22] Dessa har bedrivits av FOI på Försvarsmaktens uppdrag, med deltagande från bl.a. FMV och försvarsindustrin. Således har ambitionen varit att samla den kompetens som finns inom landet. Studierna har i huvudsak varit av två typer, antingen ett studium av ett teknikområdes möjligheter (t.ex. HPM[23]) eller ett studium av möjliga tekniker för att klara en uppgift (t.ex. luftförsvarsradar[24]). Ambitionen har varit att ta ett grepp över hela spännvidden från tekniska system till strategiska/operativa konsekvenser.

För närvarande bedrivs ett motsvarande arbete – den s.k. FoRMA-verksamheten (FoRMA = Forskning om RMA). Denna syftar till att studera och värdera framtida möjligheter för försvaret. Inom ramen för denna verksamhet tas ett antal teknikbeskrivningar, spelkort, koncept m.m. fram. Tanken är också att studera strukturernas sårbarhet för telekrigföring såväl som telekrigföringens möjligheter inom ramen för det nätverksbaserade försvaret (NBF).

7.2.2 Värdering

Värdering handlar konkret om att bedöma förmåga att uppfylla ett eller flera mål. Värdering kan vara av absolut eller relativ karaktär. Vid absolut värdering fordras någon form av kalibrering mot i verkligheten prövade data. När detta inte är möjligt kan fortfarande värdering av relativ/jämförande karaktär, där de olika alternativens relativa förmåga bedöms, vara möjlig.

Målet med en värderingsprocess kan grovt sägas vara antingen:
- en genomförd avvägning mellan befintliga alternativ (värdering av relativ karaktär),
- en bedömning av ett eller flera alternativs förmåga att uppfylla några fastställda mål (värdering av absolut karaktär), eller
- generering av nya alternativ genom sammanställning av underlag från studieprocess, forskning m.m. I detta fall kan de nya alternativen i sig vara intressantare än en jämförelse mellan dem.

Värdering kan ske på olika nivåer, alltifrån teknisk nivå (enkla renodlade dueller) till beslutsstödsnivåer (taktisk och operativ nivå). Värdering skall ske mot något krite-

---

[22] Metoderfarenheterna från den första Teknisk-Strategiska Studien finns beskrivna i Wikström, P., Isacson, T. och Lindström, H., ”Teknisk-Strategiska Studier, TSS, Pilotprojekt HPM, Metod/erfarenhetsrapport”, FOA rapport C 10351-1.1, april 1993.

[23] Wikström, P., Isacson, T. och Lindström, H., ”Teknisk-Strategisk Studie av Högeffekt Pulsad Mikrovågsstrålning, TSS/HPM”, FOA rapport DH 10056, december 1992. En fortsättning av denna studie finns rapporterad i Wikström, P. och Isacson, T., ”TSS/HPM fortsättningsstudie”, FOA, Huvudavdelningen för Försvarsanalys, 94-H749/S, 1994-09-01. Fortsättningen sågs som nödvändig p.g.a. nya tekniska rön inom området.

[24] Wikström, P. och Isacson, T., ”Teknisk-Strategisk Studie av Modern luftförsvarsradar, TSS/LFrr”, FOA-RH--94-00009-1.1, september 1994.

rium. För en sjömålsrobotinsats kan olika värderingsnivåer exemplifieras enligt nedan.

- Teknisk nivå - enskild robot, utsatt för motmedel
- Taktisk nivå - hur skjuta salvor för att mätta fartygs luftförsvar
- Operativ nivå - hur samordna mellan Marinen och Flygvapnet avseende sjömålsrobotinsatser (hur få underrättelseinformation, hur leda?)

Det är givetvis ibland lite otydligt var man skall sätta gränser mellan nivåer. Värderingen kan också förenklas genom att stega sig fram genom de delar som ingår i t.ex. en robotinsats (upptäcktsduellen, förneka skott, försvåra robots målsökning/-följning, hur få robot att missa,...). Vad kan påverka roboten i de olika stegen?

Då denna rapport ytterst syftar till att beskriva frågeställningar med anknytning till projektet Taktisk värdering telekrig kommer fokus i fortsättningen att läggas på taktisk värdering.

Den studieprocess i vilken värdering vanligen utnyttjas innehåller följande moment:
- Problemformulering
- Kunskapsuppbyggnad
- Värdering
- Resultat/rekommendationer

I **problemformuleringsfasen** ställs frågan: 'Vad är egentligen problemet?'. En analys av detta är ofta ett stort steg på väg mot lösningen. Här kan man t.ex. underlätta dynamiken i en grupp genom att utnyttja kreativitetsmetoder, vilka egentligen ofta bara syftar till att alla skall våga framföra sina åsikter.

Kunskapsuppbyggnadsfasen handlar om att beskriva hur själva värderingen skall gå till samt att ta fram nödvändigt underlag, d.v.s. skapa ett tillräckligt kunskapsläge inför värderingen. Häri ingår att beskriva vilka hot som finns, att göra tekniska beskrivningar av system (spelkort), att beskriva hur vi avser agera taktiskt med våra förband etc. Det ingår också att ställa upp alternativ inför värderingen. Det är också viktigt att formulera de mål mot vilka värderingen skall ske. I den mån simuleringsmodeller behövs måste framtagning av dessa börja så tidigt som möjligt.

Den egentliga **värderingen** handlar om att genomföra prövningen mot de uppsatta målen. Detta görs i allmänhet inom ramen för scenarier/typsituationer, d.v.s. som någon form av spel.[25] De typsituationer som används ligger typiskt på relativt låg nivå, t.ex. enstaka plattformar med kompletta sensorpaket. Ett vanligt sätt att genomföra värderingen är genom dialog i en balanserat sammansatt grupp, som en

[25] Ibland används dock bara översiktliga värderingsmått för att bedöma hur strukturer/system/förband klarar någon viss uppgift. Det är dock inte ovanligt att spel utnyttjas tidigare i processen för att bygga upp kompetens om strukturer/system/förband och omvärldsförutsättningar.

strukturerad diskussionsvärdering. I samband med värderingen genomförs också känslighetsanalyser och variationsresonemang. Värderingen kan behöva följas av fördjupade analyser av osäkerheter m.m.

Grunden för genomförande av strukturerade diskussioner är att samla kompetenser från ett antal olika relevanta områden och diskutera gemensamt över ett antal typfall. Detta ger, förutsatt att rätt kompetenser finns och att tillräckliga förberedelser gjorts, ett brett underlag som kan utnyttjas för att dra slutsatser. Dessutom fås ett relativt snabbt resultat. En viktig parameter är värderingsgruppens sammansättning. En bred kompetensprofil bör eftersträvas, vilken täcker alla viktiga aspekter – tekniska och taktiska – i det som skall värderas. Det är av praktiska skäl svårt för någon enskild person att få en sådan överblick. Behovet av att ha med människor med olika bakgrund leder dock snabbt till att värderingsgruppen blir antalsmässigt stor. Här måste en avvägning göras eftersom en allt för stor grupp (>10 personer) i allmänhet blir mindre effektiv. Risken finns också att den aktiva delaktighet från alla deltagare som är en förutsättning för att den samlade kompetensen i gruppen skall kunna utnyttjas fullt ut, försvåras i en större grupp. En annan viktig faktor till vilken hänsyn bör tas vid sammansättning av en värderingsgrupp är att förankringen av resultaten i en organisation underlättas om personal från organisationen deltar i genomförandet av värderingen.

De resultat som sedan erhålls tolkas och ligger till grund för **resultat och rekommendationer**, d.v.s. beskrivning av slutsatser för kund/beslutsfattare.

Under alla steg i processen måste man, då behov uppstår, kunna ta ett eller flera steg tillbaka. T.ex. har man kanske missat något i problemanalysen eller har behov av mer underlag.

Efter en genomförd taktisk värdering finns ofta intresse av att överföra resultaten till högre nivåer, d.v.s. att översätta taktiska resultat till operativa konsekvenser. Detta är ofta mycket svårt.

Ett typiskt exempel på arbetsgång under en värderingsinriktad studie på taktisk nivå är enligt fig. 7.1 nedan.

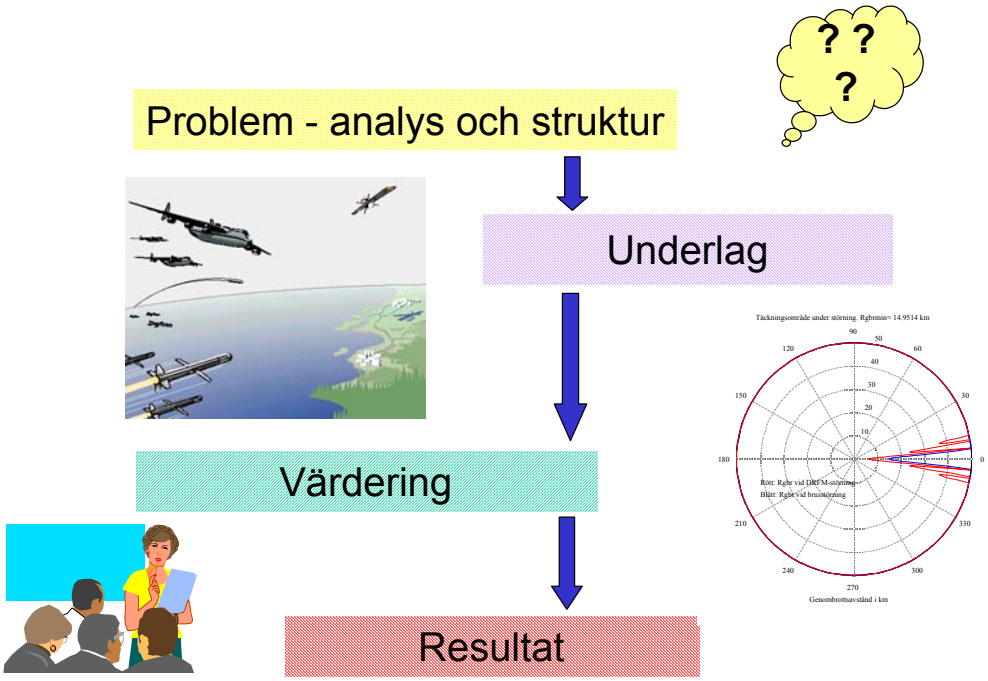

Fig. 7.1. Ett typiskt exempel på arbetsgång i en värderingsinriktad verksamhet.

Vid taktisk/operativ värdering är det ofta nödvändigt att studera komplexa samspel. Det kan t.ex. handla om att skapa sig en modell av ledningsstrukturen för att kunna bedöma hur och var angrepp mot denna kan ske, vilka effekter detta kan ge och hur systemet kan skyddas.

Nya avancerade nätverkslösningar kan komma att innebära att traditionella sätt att använda telekrigföring blir mindre verkningsfulla och att det blir än viktigare att tänka igenom hur vi skall utnyttja telekrigföring i samverkan med andra medel. T.ex. kan förekomsten av många sensorer och sensornära datafusion göra det svårare att nå effekt genom att störa enstaka sensorer.

Det handlar inte heller bara om teknik utan även om hur man genom att ändra uppträdande kan påverka sin sårbarhet. Det handlar idag oftast inte om stridande parter i traditionella krigsförloppsscenarier utan om uppträdande i samband med internationella insatser m.m. I dessa ”nya” situationer är ofta förluster ”oacceptabla”, vilket innebär att alla tänkbara hot måste tas på allvar och skyddsaspekter blir viktiga.

8 Verksamhet i projektet Taktisk värdering telekrig

8.1 Inledning

För att sätta projektet Taktisk värdering telekrig på rätt plats i strukturen sammanfattas här den verksamhet som bedrivs på FOI inom ramen för FoT-området Telekrigföring. Taktisk värdering telekrig faller här under punkten ”Värdering och simulering av telekrig”.

FOI-verksamhet inom telekrigområdet
Den långsiktiga inriktningen av forskningsområdet är att genom egen forskning förstå teknikutvecklingens möjligheter och begränsningar och mot bakgrund av detta lämna underlag för beslut avseende egna system för telekrigföring samt skyddsåtgärder mot telekrig.

Forskningsområdet Telekrig omfattar tillämpad forskning för försvaret inom delområdena:
- Värdering och simulering av telekrig
- Teknisk hotsystemanalys
- Telekrig mot styrda vapen och sensorer
- Telekrig mot samband och kommunikationssystem
- Plattformstillämpad VMS
- Vågutbredning
- Elektromagnetiska vapen och skydd
- Signaturanpassningsteknik.

Här är en viktig del i verksamheten en värderingskedja från teknisk nivå upp till operativ nivå där tekniska systemlösningar och idéer värderas mot taktiskt uppträdande för att slutligen bedömas med avseende på operativa konsekvenser. Syftet är att sätta in tekniken i sitt taktiska och operativa sammanhang.

Inom området värdering och simulering kan de existerande projektens relation beskrivas enligt fig. 8.1.

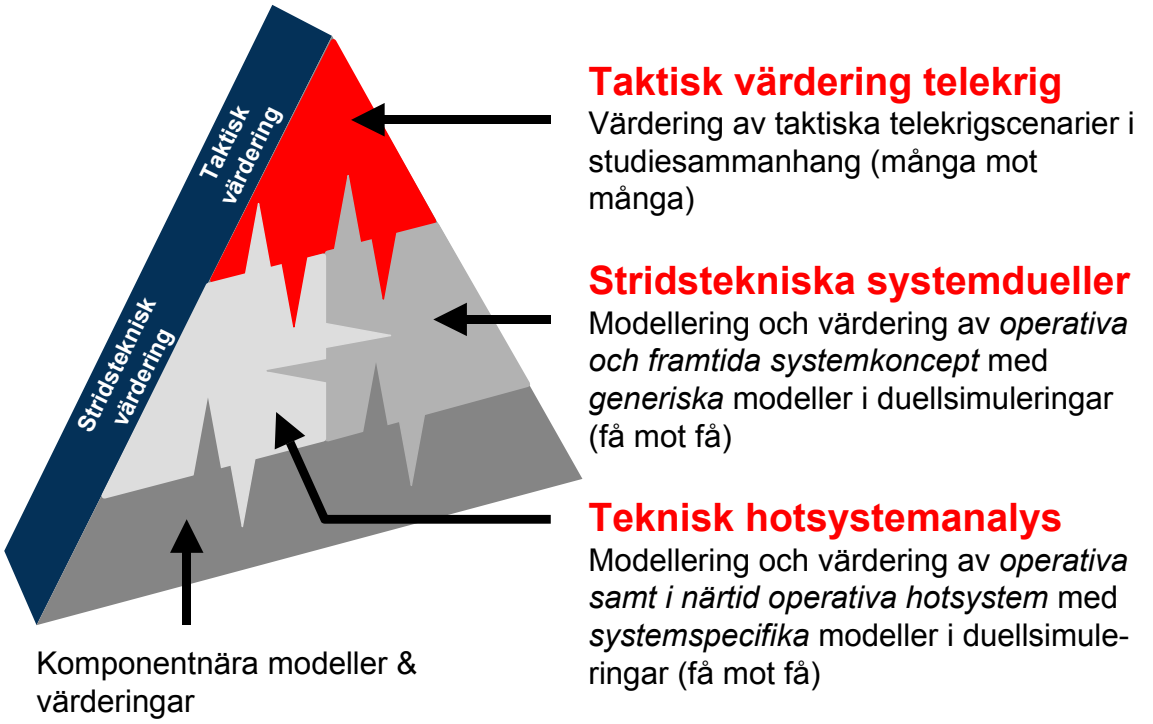

Fig. 8.1. Ett försök att åskådliggöra relationen mellan existerande projekt som arbetar inom området värdering och simulering av telekrigföring.

I fortsättningen gäller beskrivningen projektet Taktisk värdering telekrig.

Projektets frågeställning:
Hur skall system och tekniker inom telekrigområdet värderas på taktisk nivå och hur skall resultaten överföras till operativ nivå?

Projektets mål:
- Utveckla värderingsmetoder och genomföra värdering av telekrigåtgärder på taktisk och operativ nivå
- Utveckla modeller för att åskådliggöra taktiskt utnyttjande av telekrigsystem
- Stödja Försvarsmaktens studier genom medverkan och värderingsunderlag
- Bygga upp kompetens för att beskriva telekrigåtgärder i systemtermer (t.ex. hur viss spaningsinformation kan påverka hela stridsförloppet)
- Stödja andra projekt inom FOI med värderingskompetens inom telekrigområdet.

Frågeställningen speglar tydligt det problem som skall hanteras. Här är det viktigt att inse att värdering av telekrigföring har stora likheter med annan taktisk värdering. Det handlar snarare om var fokus skall läggas. Ett viktigt syfte är att stödja Försvarsmakten bl.a. genom medverkan i studier. Dels för att därigenom stödja

dessa studier, dels för att genom denna medverkan få bättre insyn i de för kunden mest aktuella problemen. Det senare är en hjälp för FOI att göra rätt saker.

8.2 Genomförda verksamheter

Några verksamheter som bedrivits inom projektet framgår nedan:
- Utvärdering av FbSim
- Utvärdering av Ship EDF - en modell för elektromagnetiska beräkningar
- Nya algoritmer för SMIT-modellen - en modell för beräkning av strilsystemets täckning
- Utveckling av simuleringsmodellen JASRAD för simulering av BVR-strid
- Värdering av VMS för fartyg
- Värdering av VMS för flyg
- Satellitbaserade navigeringssystem
- Cross-eye-störning av monopulsmålsökare
- Informationsflöde i nätverk
- Medverkan i FM-studier och FOI-projekt.

De bägge första punkterna ovan behandlar modeller som analyserats utifrån tillämpbarheten för projektets ändamål. I bägge fallen befanns modellerna – FbSim (förbandssimulering), vilken sammanhålls på FMV och som ursprungligen började utvecklas för att simulera vapensystem som en del av IT4-projektet, och Ship EDF (Ship Electromagnetic Design Framework), vilket är ett italienskt modelleringsramverk för elektromagnetisk design av fartyg – vara av begränsat intresse för oss och utvärderingarna följdes inte av något praktiskt utnyttjande av dem. Arbetet finns beskrivet i rapporter såväl för FbSim[26] som för ShipEDF.[27] Därutöver finns sammanfattningar av dessa verksamheter i den första utgåvan av detta dokument[28]. De ingår därför ej här. Andra delar i de bägge tidigare utgåvorna av detta dokument har dock behållits då de är av större intresse.

Förutom ovan listade verksamheter har kurser och föredrag hållits för att bidra till att sprida kunskap om telekrig inom såväl FOI Försvarsanalys som i andra sammanhang – t.ex. inom ramen för Högre Kurs Telekrig (HKT).

---

[26] Johansson, R., ”Metodik för värdering av VMS för stridsfordon med hjälp av FbSim”, FOA-R--98-00799-616--SE, juni 1998; Moberg, H., ”Granskning av FbSim-modellen”, Institutionen för Optimeringslära och systemteori, KTH, 1999.

[27] Brämming, P., Wallström, D. och Kindvall, G., ”Utvärdering av modelleringsramverket Ship EDF”, FOA-R--00-01338-202,612,615--SE, februari 2000. En utvärdering av modelleringsramverket Ship EDF utfördes också av FOI Sensorteknik. Den finns dokumenterad i Erickson, R., Fagerström, J., Frennberg, H., Rahm, J. och Welander, N., ”Utvärdering av ADF och ShipEDF, programpaket för elektromagnetiska beräkningar”, FOA-D--99-00444-504,612,615--SE.

[28] Kindvall, G.(red), ”Värdering av telekrig – Metoder, verktyg och verksamheter vid FOA 1”, FOA Memo 00-5672/S, 2000-12-20.

Allmänt kan projektets resultat delas in i *kunskap*, *modeller* och *avtappning*. Se även fig. 8.2, vilken visar några av projektets viktigaste resultat.

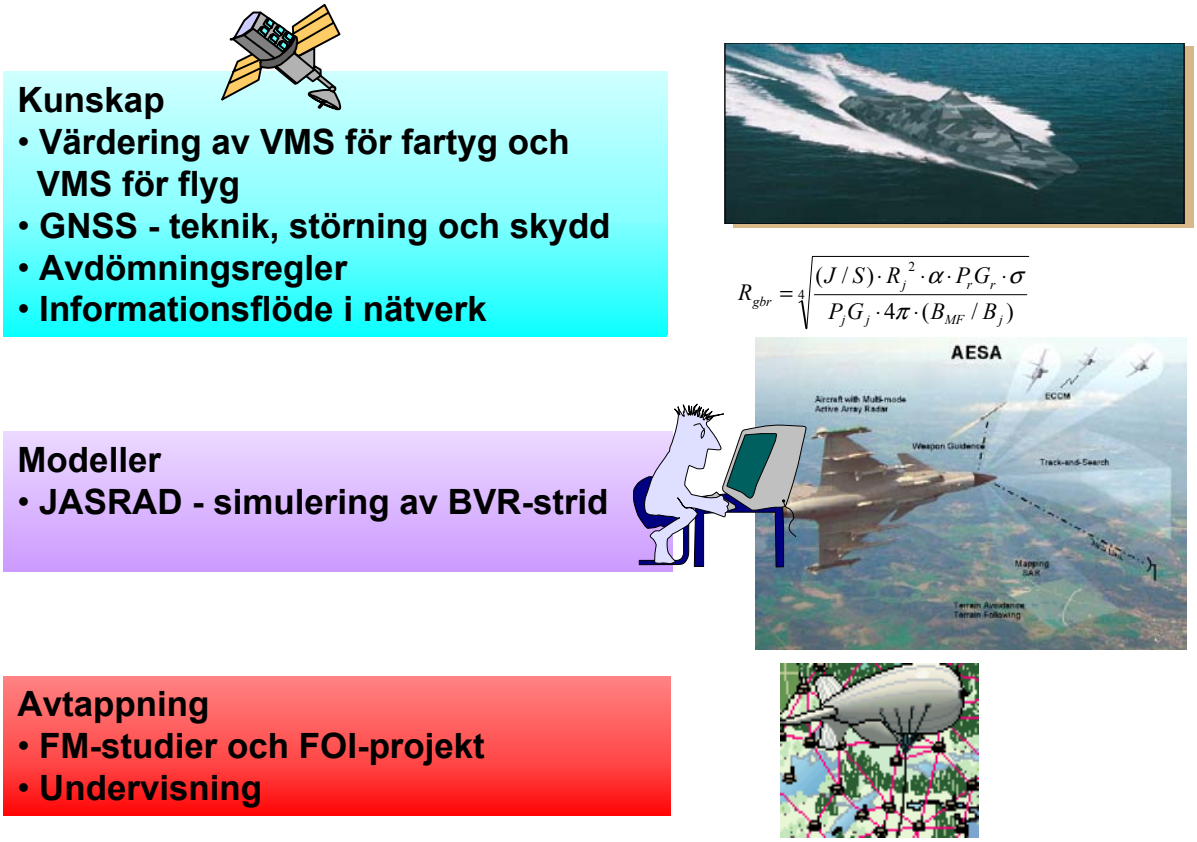

Fig. 8.2. En sammanställning av några resultat från projektet Taktisk värdering telekrig.

Eftersom telekrigverksamheten på FOI Försvarsanalys bedrivs gentemot en högre studienivå, d.v.s. syftar till att analysera telekrigföringens konsekvenser snarare på förbands- än systemnivå, är resultaten av detaljerade beräkningar och simuleringar ett ingångsvärde som skall inhämtas från de därför ansvariga och metodmässigt överföras till underlag för taktisk (och operativ) värdering. På den högre nivån är det istället av vikt att identifiera de viktigaste faktorerna och att göra förenklingar som medger hanterbarhet i spel- och värderingssituationer samtidigt som det finns relevans i resultaten. Detta måste vara vägledande vid all utveckling av simuleringsverktyg.

8.2.1 SMIT-modellen

SMIT 2 har tagits fram i samarbete med FOI-projektet ANABASIS, vilket arbetar med utveckling av luftstridssimuleringar i modelleringsramverktyget FLAMES. SMIT 2 är en simuleringsmodell som beräknar och presenterar räckvidder för luftförsvarsradarsystemet. Den är en vidareutveckling av en tidigare simuleringsmodell.

En viktig del i SMIT-modellen är att visa vilka upptäcktsavstånd man får i ett strilsystem som är utsatt för telekrigangrepp. De fördröjningar beträffande egen insats som blir följden är ofta avgörande för stridens förlopp.

Det visade sig att orealistiska upptäcktsavstånd ibland erhölls från den ursprungliga versionen av SMIT-modellen och en närmare undersökning av de ingående algoritmerna utfördes därför. Resultatet var tydligt, radarpulserna behandlades som icke-kodade[29] i algoritmerna och det fel som uppstod blev avsevärt, över 300 %. Tillsammans med Telub korrigerades dessa algoritmer under år 2000 och en bättre presentationsform av räckvidderna har införts. Vidare har gränssnittet mot användaren ändrats, allt i syfte att göra modellen mer tillförlitlig.

Behovet av att utveckla en modell av denna typ har sin grund i att de algoritmer som inköpta luftförsvarsmodeller av samma typ som SMIT bygger på sällan redovisas fullt ut.

Projektet Taktisk värdering telekrig har förutom att utveckla de nya algoritmerna även delfinansierat framtagningen av simuleringsmodellen.

8.2.2 JASRAD

JASRAD är ett Windowsprogram som simulerar upptäcktsduellen i BVR-strid (Beyond Visual Range) mellan flygplan utrustade med radar, brusstörare, radarvarnare och robotar. Simuleringen av upptäcktsduellen baseras på grundläggande samband för räckvidder och genombrottsavstånd. Med JASRAD är det möjligt att bygga upp scenarier där störinsatsens verkan kan studeras, att variera data för system och se hur utfallet påverkas och att studera följderna av förändringar av det taktiska uppträdandet. Upptäcktsduellen är central såväl då det handlar om att följa upp med en vapeninsats som då det gäller att övervaka t.ex. en ”no-fly zone” genom patrullering. En rapport föreligger.[30]

Möjliga användningsområden för modellen är:
- Illustrera kopplingen mellan teknik och taktik
- Stimulera till diskussion kring tekniska/taktiska överväganden
- En ”räknedosa” för räckvidder, genombrottsavstånd m.m.
- En lättanvänd ”scenariogenerator”
- Undervisning.

Den kan även belysa specifika frågor som:

---

[29] Vårt moderna strilradarnät innehåller nästan enbart radarstationer med s.k. pulskompressionsteknik, d.v.s. pulserna är förlängda och kodade.

[30] Berefelt, F., ”JASRAD – Ett program för att simulera upptäcktsduellen i luftstrid på stora avstånd: Modellbeskrivning”, FOA-R--99-01319-202,616--SE, december 1999.

- Givet vissa prestanda på sensorer och motmedel, hur skall plattformar positioneras?
- Hur skall en tänkt eskortstörare uppträda: skall den störa ”brett” eller ”punktvis”?
- Kan vi vinna övertag genom att kinematiskt optimera det taktiska uppträdandet?
- Hur och när skall en undanmanöver utföras på basis av information från radarvarnaren?

Se även fig. 8.3.

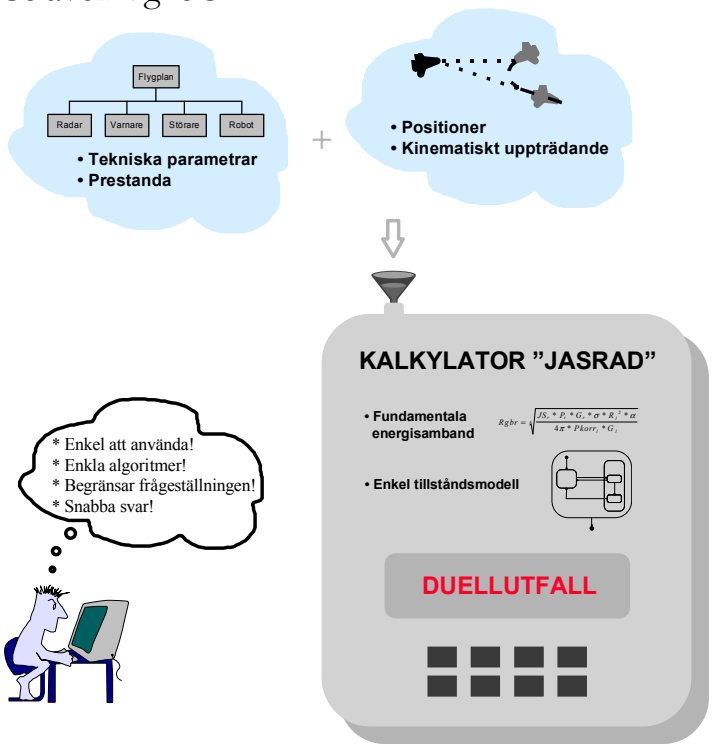

Fig. 8.3. Schematisk beskrivning av JASRAD.

8.2.3 Värdering av VMS för fartyg[31]

Varnings- och motverkanssystem (VMS) för plattformar får större betydelse i samband med att Sverige planerar att ställa allt fler typer av försvarsresurser till förfogande för samordnade multinationella fredsfrämjande insatser. I sådana samman-

[31] Verksamheten finns rapporterad i:
- Andersson, C. och Moberg, H., ”Metodrapport för VMS-värdering”, FOA Memo 00-H383/S, 2000-09-20.
- Andersson, C. och Moberg, H., ”Värdering av VMS för fartyg – Resultat från genomförd värdering hösten 2000”, FOA-RH--00-00546-616--SE, december 2000.
- Andersson, C. och Kindvall, G., ”Protokoll från värderingsinternat VMS för fartyg 6-7 juni 2001”, FOI Memo 01-H313, 2001-08-27.
- Andersson, C. och Kindvall, G., ”Värdering av VMS för fartyg – Metodbeskrivning och rapportering av genomförd värdering”, FOI-RH--0122, augusti 2002.

hang ställs ofta krav på egenskydd för dessa plattformar för att få deltaga. Behovet av skyddsnivå bestäms av ansvarig Force Commander för respektive insats. Delvis av detta skäl men också för att tillse att svenska deltagande förband har tillräcklig skyddsnivå för att möta eventuella hot blir det allt viktigare att värdera VMS.

Under år 2000 och 2001 har det skett ett samarbete mellan FOI-projekten Taktisk värdering telekrig vid FOI Försvarsanalys och "VMS fartyg" vid FOI Ledningssystemteknik avseende värdering av VMS för fartyg på taktisk nivå inom ett perspektiv av 10-20 år framåt i tiden.

Som grund låg antaganden om den framtida hotbilden för ytstridsfartyg. Därefter studerades och värderades effekten av olika varnings- och motverkanskonfigurationer. Det handlade således om att pröva och bygga upp förståelse för samspelet mellan teknik och taktik. Syftet med verksamheten var att utgöra ett underlag för val av framtida inriktning av varnings- och motverkanssystem för marina plattformar.

Hösten 2000 kom den första rapporten.[32] I den ges en allmän beskrivning av den värderingsmetod som tagits fram och en hotbildsbeskrivning, samt resultatet av ett provspel där verkan av laservarnare studerades med den angivna metoden. Avsikten var att testa och förfina metoden inför det spel-/värderingsinternat som genomfördes senare under hösten 2000. Metoden för att analysera dessa komplexa situationer härrör från FAS-studien.[33] Metoden är applicerbar både på datorsimuleringar och spel, eftersom det i båda fallen är viktigt att strukturera arbetet.

Metoden innehåller följande steg som behöver genomföras i samband med värderingen:

1. Beskrivning av hotet - teknisk hotbild
2. Beskrivning av scenariot - taktisk hotbild
3. Beskrivning av fartyget
4. Beskrivning av fartygets sensorsystem
5. Beskrivning av fartygets motverkanssystem
6. Analys av sensorsystemets förmåga att upptäcka hotet
7. Analys av motverkanssystemets förmåga att möta hotet
8. Analys av motverkanssystemets förmåga att möta hotet i komplexa situationer
9. Sammanvägt försvar/taktik i olika scenarier
10. Upprepa momenten med andra typsituationer, hot-, sensor- och motverkanssystem.

[32] Andersson, C. och Moberg, H., ”Metodrapport för VMS-värdering”, FOA Memo 00-H383/S, 2000-09-20.

[33] Berglund, E. et al, ”Försvar av fartyg mot attack- och sjömålsrobotar”, FOA-RH--98-00324-314, mars 1998.

Således handlar det mycket om att inhämta kunskap (underlag) innan värderingen de facto genomförs.

Som grund för den värderingsverksamhet avseende effekten av olika varnings- och motverkanssystem som genomförts togs följande åtta typsituationer fram:

1. Laserstyrd robot mot eget fartyg
2. Kustrobot mot eget fartyg
3. Laserstyrda bomber mot fartyg
4. Sjömålsrobot mot fartyg
5. Artilleri mot fartyg i rörelse
6. Signalsökande robotar mot fartyg i rörelse
7. Lv-skydd av konvoj
8. Laserstyrd robot mot eget förband.

Avsikten med de åtta typsituationerna är att spegla rimligt utnyttjande av fartyg och möjliga hot på ett någorlunda heltäckande sätt inom Försvarsmaktens uppgifter. Typsituationerna är tänkta att täcka även agerande inom ramen för internationella insatser. Framtagande av typsituationer bör ske som en iterativ process för att erhålla situationer som innehåller alla aspekter av det som skall värderas. Typsituationerna får heller inte ses som statiska i värderingen. Troligen behöver de ändras även under själva värderingen. Så var också fallet. Typsituationernas mål är inte att ge en heltäckande beskrivning av framtida tänkbara situationer, de skall snarare spegla olika möjligheter.

En typsituation är en beskrivning av scenario, hot samt egen plattform inklusive befintliga och möjliga varnings- och motverkanssystem. De tekniska begränsningar hos grundfunktionerna som enskilda fartyg och VMS har måste framträda i situationen. Yttre faktorer som kan påverka systemen – vind, siktförhållanden etc. – bör beskrivas, främst som grund för senare analys av varnings- och motverkanssystemens förmåga att upptäcka och möta hoten. Samtidigt måste typsituationen vara realistisk, d.v.s. fartygets operativa förmåga, verkans- och egenskyddsfunktioner, måste ställas i relation till ett fartygsförbands operativa målbild.

Tid och avstånd är viktiga parametrar som typsituationen måste beakta. Till exempel är den maximala visuella räckvidden knappt 20 km, för en sensor placerad 9 meter upp mot ett mål på 5 meters höjd. Detta gör att tiden för ett VMS att verka blir starkt begränsad. En robot som kommer inflygande med Mach 3 träffar målet 20 sekunder efter det att den tidigast kan upptäckas med målets egna sensorer. Det är således ofta relevant att diskutera i termer av tid, t.ex. den tid det tar att vidtaga olika åtgärder.

Den värdering som utfördes under hösten 2000 finns beskriven i rapport.[34] Den manuella värderingsmetod som använts kan närmast beskrivas som "strukturerade diskussioner". Denna metod valdes för att problemställningarna var relativt diffusa. För att hålla nere deltagarantalet samt för att få bättre förståelse för hur metoden fungerar begränsades värderingen inledningsvis till att studera åtgärder inom det optroniska området.

I juni 2001 genomfördes ytterligare en värdering, även den i form av strukturerade diskussioner. Samma åtta typsituationer som vid värderingen hösten 2000 utnyttjades, men vissa revideringar hade gjorts. Vid värderingen i juni 2001 behandlades varnings- och motverkanssystem inom hela det elektromagnetiska spektrumet. Ett preliminärt resultat från värderingen finns utgivet.[35] Under värderingen deltog personal från FM, FMV och FOI. Utifrån typsituationer, spelkortsunderlag och frågeställningar diskuterades möjligheter, brister och osäkerheter för olika varnings- och motverkanssystem.

Grunden för genomförande av strukturerade diskussioner är en väl sammansatt värderingsgrupp, se avsnitt 7.2.2. Förutsatt att kompetensprofilen totalt sett täcker tillräcklig bredd och att tillräckliga förberedelser gjorts kan ett relativt snabbt resultat erhållas. För att undvika de problem som kan uppstå vid en för stor värderingsgrupp utnyttjades ibland två parallella grupper. Härvid kom vissa av typsituationerna att analyseras av bägge grupperna medan andra bara kom att analyseras av den ena gruppen. Vissa personer med specialkompetenser blev här i viss grad "ambulerande", d.v.s. ingick i den ena gruppen men kunde avropas av den andra gruppen vid behov.

Under hösten 2001 genomfördes en fördjupning av tre av de åtta tidigare studerade typsituationerna.[36] Syftet var att noggrannare penetrera en del av de osäkerheter som identifierats under tidigare genomförda värderingar. Detta arbete genomfördes tillsammans med 2. ytstridsflottiljen, HMS Kalmar. De utvalda typsituationerna spelades upp för relevanta operatörer i stridsledningscentralen genom utnyttjande av simuleringsmoden i fartygets ledningssystem. Slutsatserna från denna fördjupade värdering ligger tillsammans med tidigare resultat till grund för de resultat och slutsatser som presenteras i slutrapporten.[37]

---

[34] Andersson, C. och Moberg, H., ”Värdering av VMS för fartyg – Resultat från genomförd värdering hösten 2000”, FOA-RH--00-00546-616--SE, december 2000.

[35] Andersson, C. och Kindvall, G., ”Protokoll från värderingsinternat VMS för fartyg 6-7 juni 2001”, FOI Memo 01-H313, 2001-08-27.

[36] De utnyttjade typsituationerna (nr 1, 4 och 6 enligt den tidigare numreringen) utvecklades ytterligare då det bl.a. krävdes mer detaljerad information om robotbanor samt underlag för manuella inspel av sensorer som inte var integrerade i ledningssystemet.

[37] Andersson, C. och Kindvall, G., ”Värdering av VMS för fartyg – Metodbeskrivning och rapportering av genomförd värdering”, FOI-RH--0122, augusti 2002.

Vid värderingen ombord på HMS Kalmar var endast en ur besättningen (luftförsvarsofficeren, LFO) helt införstådd med typsituationerna vid starten. LFO hade i förväg lagt in robotbanor etc. som underlag för spelet. Övriga fick grova förutsättningar, d.v.s. vilken uppgift fartyget hade, ungefär hur hotmiljön såg ut tekniskt och taktiskt, väder etc. Därefter fick de reagera på händelseförloppet. Efter detta vidtog en diskussion om typsituationen, förutsättningar och slutsatser och ibland kördes ytterligare simuleringar av samma situation. Vid några tillfällen togs paus i simuleringen efter en stund för diskussion innan den fortsatte. Detta var speciellt relevant då indata från sensorer som ej fanns integrerade i systemet behövde spelas in.

Som en mall för värderingsarbetet utnyttjades följande matris, se fig. 8.4. Dess syfte var att vara en struktur kring vilken diskussionen kunde föras och i vilken slutsatser kunde föras in. Viktig är här indelningen i befintliga (planerade) respektive nya varnings- och motverkanssystem. För varje typsituation gjordes en bedömning av vilka varnings- och motverkanssystem som var nödvändiga för att klara hotet och vilka som var ett bra komplement genom att ge information som ökade möjligheterna att identifiera hotet, minskade falsklarmsfrekvensen etc.

Motverkan / Varning	**Befintlig motverkan**	**Ny motverkan**
Befintliga sensorer	Referens	Tekniska konsekvenser Taktiska/stridstekniska konsekvenser
Nya sensorer	Tekniska konsekvenser Taktiska/stridstekniska konsekvenser	Tekniska konsekvenser Taktiska/stridstekniska konsekvenser

Fig. 8.4. Matris som utnyttjades som stöd vid värdering av VMS.

Med tekniska konsekvenser menas rent teknisk inverkan på sensorsystem. Med taktiska/stridstekniska konsekvenser avses påverkan på stridsutfallet i typsituationen när ett visst system används.

För att styra diskussionen under värderingen utnyttjades ett antal frågeställningar. Dessa berörde såväl scenariot (är det troligt, vilka sensorer bör ingå, är uppträdandet rimligt, väderberoendet m.m.) som rutorna i matrisen. I det senare fallet handlade det om frågor av betydelse för att bedöma de tekniska och taktiska/stridstekniska konsekvenserna, t.ex. vilka hot en viss sensor klarar av, falsklarmsfrekvens, hur tidsförloppen ser ut, psykologiska effekter av bl.a. falsklarm, vilka hot övriga sensorer kan upptäcka m.m.

8.2.4 Satellitbaserade navigeringssystem (GNSS)

Projektet Taktisk värdering telekrig vid FOI Försvarsanalys har, i samarbete med FOI Systemteknik och FOI Ledningssystem, bedrivit ett arbete syftande till att studera effekterna av telekriginsatser mot precisionsvapen. Det handlade om att titta på möjligheterna att påverka moderna navigeringssystem, framförallt satellitbaserade sådana (Global Navigation Satellite System, GNSS). Idag finns främst GPS (Global Positioning System), medan det ryska Glonass har begränsad täckning. I Europa planeras ett eget system, Galileo, vilket inte beräknas vara i full drift förrän ca år 2008. En viktig del i arbetet har varit att beskriva funktionen hos det enda fullt fungerande systemet, GPS. Arbetet har rapporterats.[38]

Moderna (satellit) navigeringssystem har idag stor betydelse för vapeninsatser och ledning av förband. Utvecklingen går mot bättre prestanda, lägre pris och civil teknik. Äldre vapensystem kan på detta sätt ges förbättrade prestanda. Samtidigt blir också satellitnavigering mer tillgängligt för såväl militära som civila tillämpningar. Systemen blir beroende av GNSS för navigering. Kvalificerade militära system kommer även att ha andra navigeringssystem – t.ex. tröghets- eller terrängnavigering – som komplement till GNSS.

Ett viktigt syfte med arbetet har varit att beskriva störformer och störskyddsmetoder. Även om det tekniskt är relativt lätt att störa t.ex. GPS är det heller inte svårt att bygga in störskydd i systemet. Ett antal förslag till scenarier/typsituationer har diskuterats. Dessa behöver dock fördjupas för att kunna ligga till grund för värderingar, t.ex. genom diskussionsspel och/eller simuleringar.

En GPS-mottagare kan påverkas av avsiktliga och oavsiktliga störningar. De oavsiktliga störningarna är främst övertoner från kommersiella sändare såsom radio, radar, TV etc., vilkas frekvens ligger i närheten av GPS-frekvenserna. Detta gör i sin tur att signalerna störs mer, vilket innebär att civila användare som inte kan kompensera med två GPS-frekvenser, kan märka detta.

Det finns flera sätt att störa en GPS-mottagare:

- Brusstörning - Ofta med en bredd på flera MHz. Avser att maskera satellitsignalerna, försämra signalbrusförhållandet och försvåra mottagarens inlåsning. Icke-optimal maskerande störform.
- CW-störning - Maximalt smalbandig variant av brusstörning. Optimal bland maskerande störformer men kräver att störaren mer noggrant kan mäta upp satellitsignalens bärvågsfrekvens.
- Pulsat brus/CW - Kan vara mindre effektkrävande än kontinuerlig störning om mottagaren är olämpligt byggd, t.ex. om den har en alltför enkelt utförd automatisk förstärkningsreglering

[38] Berefelt, F., Falk, L., Hyberg, P., Kindvall, G. och Moberg, H., ”GNSS – hot eller möjlighet?”, FOI Memo 01-2419, 2001-12-12.

- Svepande CW - Kan i vissa fall bryta upp en redan etablerad inlåsning
- Skensändning - Lurar mottagaren att låsa in på felaktig position genom att i närheten av mottagaren återutsända på olika sätt manipulerade versioner av satellitsignalerna. Ett mycket enkelt sätt att utföra detta är att flytta den fältbild som mottagaren känner genom återutsändning av satellitsignalerna förstärkta men via en förslagsvis 100 meter lång kabel mellan störarens mottagare och sändare. GPS-mottagaren kommer då att få ett positionsfel av samma längd.

Det är stor skillnad mellan olika mottagare i fråga om störkänslighet. En enkel (civil) mottagare kan relativt lätt störas ut, medan mer kvalificerade mottagare klarar sig bättre genom större dynamik och mer signalbehandling. Allmänt är det lättast att störa en mottagare innan den har låst på satelliterna och räknat fram en position.

För att veta om en GPS-mottagare är störd är det önskvärt att den innehåller en krets som detekterar onormalt höga signalnivåer över bakgrundsbruset. Detta kan ge användaren en indikation om fel, eller utnyttjas för att internt i navigeringssystemet sätta in motåtgärder, t.ex. stöttning med tröghetsnavigeringssystem.

Ett antal metoder att öka störtåligheten nämns i rapporten,[39] t.ex. tekniska åtgärder i mottagarna och stöttning av annat navigeringssystem, t.ex. tröghetsnavigering. Ett annat sätt är att minska antennvinsten i störriktningen och öka den mot satelliterna. Detta kan ske med antenner bestående av flera antennelement. På detta sätt kan lämplig lobformning och adaptiva nollställen genereras. Generellt kan en gruppantenn bestående av ett antal (m) separata element generera m-1 sådana nollställen. Signal-/störförhållandet kan förbättras med 30-40 dB för ett bra system.

Troligen finns flera av de störskydd som diskuteras i rapporten implementerade i militära GPS-mottagare, då ett störskydd inte är tillräckligt. Dessutom ger den krypterade militära koden (P/Y-koden) bättre störövervikter på grund av större bandbredd.

För att kunna beskriva möjligheterna att störa GNSS respektive möjligheterna att skydda GNSS mot störning är det viktigt att definiera relevanta scenarier/typsituationer i vilka vi kan bedöma effekten av navigerings- och störtekniker tillsammans med andra system och åtgärder.

Kvalificerade system av typ kryssningsrobotar kan förväntas utnyttja flera olika navigeringstekniker (GNSS, tröghetsnavigering, terrängnavigering) parallellt och därigenom besitta ett relativt gott skydd mot störning av GNSS. Här behöver man

[39] Berefelt, F., Falk, L., Hyberg, P., Kindvall, G. och Moberg, H., ”GNSS – hot eller möjlighet?”, FOI Memo 01-2419, 2001-12-12.

värdera hur noggrannheten påverkas om GNSS störs ut, d.v.s. det är viktigt att ha kunskap om de andra navigeringstekniker som används – t.ex. hur stor avdriften hos ett tröghetsnavigeringssystem är.

Det kan även vara intressant att studera hur förbands aktiviteter påverkas om satellitnavigeringssystem störs ut. Exempel på en situation kan vara: ”Mekaniserad bataljon anfaller och man vill under tiden störa ut GPS för att förhindra motståndarens utnyttjande av det samtidigt som man själva förberett utnyttjande av andra navigeringstekniker. Hur skall störare placeras ut för att åstadkomma detta?” Omvänt kan det vara intressant att analysera situationen: ”Antag att mekaniserat förband förlitar sig på GPS för lägesbestämning och att GPS oväntat störs ut under anfall i mörker. Hur kommer man att agera då? Hur kan man förbereda sig för detta?”

I många sammanhang kan det handla om system som på grund av sin storlek eller sitt antal inte har några alternativ till satellitnavigering – just p.g.a. att satellitnavigeringsteknik kan implementeras relativt enkelt i små system till en relativt låg kostnad och ändå ge god positionsnoggrannhet. Sådana små system och mängdsystem kan t.ex. vara mindre UAV:er, granater och personlig utrustning hos soldater. Är de risker man härvid tar acceptabla? Vad är alternativet? En artillerigranat kan t.ex. ha GPS-navigering inbyggd. Vad behövs för att få en sådan granat att missa sitt mål med > 100 meter, vilket kan vara fullt tillräckligt för att förhindra verkan i målet?

Det är viktigt att sätta in hotet mot satellitnavigeringstekniken i ett sammanhang. När är det troligt att störning sätts in? Frågan är hur tekniska möjligheter kan komma att utnyttjas i praktiken.

Hur det framtagna underlaget skall utnyttjas och vidareutvecklas måste bestämmas av kommande behov i studiesammanhang. Det torde dock finnas behov av att genomföra scenariobaserad värdering av hotet mot satellitnavigering och möjliga skyddsmetoder.

8.2.5 Medverkan i FM-studier och FOI-projekt

Projektet har även deltagit i aktiviteter i samverkan med kunden, t.ex. arméns telekrigberedning och temadagar. Projektet har under år 2002 även deltagit i den studie avseende SEAD som genomförts av Flygtaktiska kommandot (FTK).

Deltagande i kundverksamheter är viktigt för kundkontakter och kompetensutbyte. Det är också viktigt att bedriva direkt avtappande verksamhet in i kundens studier m.m. som ett komplement till kunskapsuppbyggande verksamhet.

Som framgår på andra håll i detta dokument har samarbete också skett med ett antal projekt på flera olika avdelningar på FOI. Ett exempel är FoRMA, där samarbete skett inom värdering av informationskrigföring (IW). En del i detta arbete har varit att göra en översyn av begrepp inom området, då de upplevdes som otydliga. Se även avsnitt 3.3.

Spelverksamheten inom FoRMA avseende informationskrigföringsområdet fokuserades inledningsvis i huvudsak på CNO (Computer Network Operations). Senare har dock även andra komponenter inom IW – telekrigföring, vilseledning och psykologiska operationer – hanterats.

8.2.6 Avdömningsregler telekrig (”Tumregler”)

Under år 2001 och 2002 har projektet Taktisk värdering telekrig bedrivit ett arbete med att beskriva generella och relativt enkla metoder för att värdera telekrigets effekter i taktiska sammanhang. En utgångspunkt för arbetet har varit den formelsamling som togs fram inom FOA Huvudprojekt Telekrig (HPTK).

Avsikten är att underlaget skall kunna bidra till att utveckla det avdömningsunderlag som finns, för tillämpning i taktiska och operativa spel. Därutöver är förhoppningen att det skall kunna skapa förståelse för vad telekrig innebär. Dokumentet skall kunna läsas med olika syften. Dess primära syfte är att fungera som en snabb introduktion för att kunna avdöma telekrigsdueller och utnyttjas i spelsituationer. Dokumentet skall även ge en mer fördjupad bild av telekrigföringens grunder. Dokumentet innehåller även exempel och tal. Förkunskapskraven för att kunna tillgodogöra sig de svåraste partierna motsvarar två år av tekniska högskolestudier.

Syftet med teorigenomgången och exemplen är dels att ge läsaren förståelse för viktiga begrepp inom telekrigområdet samt viktiga teoretiska grunder, dels att ge en hjälp åt läsaren att använda formlerna på rätt sätt.

Delrapport 1[40] hade en betoning på radarområdet. Därutöver gjordes en översyn och uppdatering av de formler som ingick i den formelsamling som gavs ut av FOA Huvudprojekt Telekrig (HPTK). I delrapport 2[41] var de tidigare delarna uppdaterade, bl.a. genom inkomna synpunkter. Därutöver hade arbete lagts på att komplettera dokumentet inom optronikområdet avseende teori, exempel och formler. Delrapport 3[42] innehöll fortsatt arbete inom optronikområdet, inledande beskrivning av sambandsområdet samt inledande arbete med nya exempel.

[40] ”Avdömningsregler telekrig – delrapport 1”, FOI Memo 01-2423, 2001-07-06.
[41] ”Avdömningsregler telekrig – delrapport 2”, FOI Memo 01-2423, 2001-12-18.
[42] ”Avdömningsregler telekrig – delrapport 3”, FOI Memo 01-2423, 2002-06-24.

Slutrapporten utges i december 2002[43]. Rapporten inleds med en definition av telekrig och en kort beskrivning av olika närbesläktade sensorsystem. Den innehåller sedan en beskrivning av olika begrepp inom telekrigområdet samt några räkneexempel. Sist i rapporten återfinns en omarbetad version av de formler som först gavs ut av FOA Huvudprojekt telekrig (HPTK).

Den huvudsakliga målgruppen för dokumentet är:
- Personer medverkande i telekrigsspel
- Personer som vill skapa sig en grundläggande förståelse om telekrig.

8.3 Pågående verksamheter

8.3.1 Crosseyestörning

Robotar med radarmålsökare är ett besvärligt hot mot fartyg och flygplan. Bara ett fåtal metoder kan vilseleda en monopulsradar i vinkel. En av de mest lovande men också mest omdiskuterade teknikerna är fasfrontstörning eller cross-eye-störning, som bygger på att två antenner producerar ett skenmål utanför antennerna. Förutsättningen är att signalerna är nästan lika starka och i motfas, så att signalerna nästan tar ut varandra vid roboten, medan fasytan vrids och leder roboten förbi målet. Se fig. 8.5.

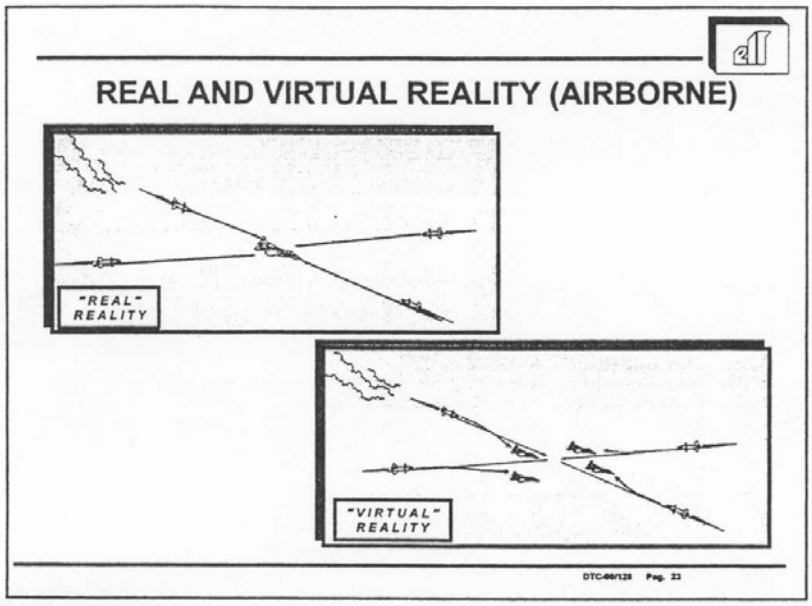

Fig. 8.5. Effekten av cross-eye vid ett anfall med fyra robotar.

[43] Andersson, C., Jansson, B., Jonason, T., Hyberg. P. och Kindvall, G., ”Avdömningsregler telekrig”, FOI-R--0661, december 2002.

Metoden har länge varit känd som teoretisk möjlighet, men inga praktiska erfarenheter har presenterats. De elektroniska problemen är svåra och successivt tycks olika länder ha givit upp sina försök. I samband med att FOI (Lars Falk) presenterade ett bidrag vid AOC-konferensen i Zürich i maj 2000, visade det sig dock att italienska Elettronica under ledning av Filippo Neri fortsatt med cross-eye. Ett färdigt system beskrevs vid AOC-konferensen i Las Vegas i oktober 2000 och vid samma tillfälle inbjöds Lars Falk att tala om teorin för cross-eye-störning under titeln ”Physical Basis for Credibility of Cross-eye for Ship Defense”. Elettronica har senare beskrivit metoden i Aviation Week & Space Technology (June 25, 2001). Alfredo Bacchelli visade filmer från försök utförda med italienska marinen och flygvapnet på AOC-konferensen i Washington i oktober 2001.

På AOC-konferensen i Stockholm i maj 2002 gav FOI (Lars Falk) en översikt av forskningsläget under titeln “Cross-eye Jamming”. För första gången presenterades kvantitativa mått på hur noggrant fas och amplitud måste kontrolleras för att metoden skall fungera. Tidigare beskrivningar har ställt alltför hårda krav genom att man inte i detalj bedömt hur den taktiska insatsen bör ske. Med moderna komponenter, aktiva antenner och datorstyrning kan förloppet regleras bättre än tidigare. Detta föredrag beskrev också hur utbredningsproblemen över hav kan lösas och vilka problem som återstår att studera. Avslutningsvis visades försök utförda vid FOI i Linköping, där ett cross-eye-system gav stabil felpekning på flera baslängder. Alfredo Bacchelli från Elettronica inbjöds sedan att visa bilder från de italienska försöken. Det följdes av frågor om tillförlitligheten hos cross-eye och systemets utformning. Det räcker med två gruppantenner baserade på halvledarkomponenter för att åstadkomma den nödvändiga böjningen av fasfronten utan att antennerna behöver vara placerade extremt långt från varandra.

Italien kommer inom Eurofighterprojektet att implementera cross-eye-tekniken istället för att utnyttja släpat skenmål.

8.3.2 Värdering av VMS för flyg

Under år 2002 och 2003 kommer projekten VMS flyg och Taktisk värdering telekrig[44] att samarbeta och genomföra en värdering inom området VMS för flyg. Syftet med verksamheten är att belysa vilka behov av varnings- och motverkanssystem som finns för framförallt JAS. Arbetet initierades ifrån HKV efter erfarenheterna från det liknande arbete som projektet Taktisk värdering telekrig genomfört tillsammans med projektet VMS fartyg och som beskrivits ovan i avsnitt 8.2.3.

Syftet med verksamheten är att bidra med underlag för val av framtida inriktning avseende varnings- och motverkanssystem för flygande plattformar (primärt JAS).

[44] Bägge projekten avslutas 2002, men verksamheten fortsätter under 2003 bl.a. inom ramen för det nya projektet – värdering av telekrig i NBF.

Därutöver bör materialet kunna användas som ett underlag för val av framtida inriktning för forskningsverksamheten inom området VMS för flyg

Arbetet kommer att bedrivas som scenariobaserade diskussioner samt ev. simuleringar. I arbetet ingår att klarlägga hotbilden för framtida flygande plattformar samt att studera och värdera effekten av olika varnings- och motverkanskonfigurationer med syfte att erhålla ett väl avvägt VMS.

För att både få med dagens system och morgondagens kommer plattformen (JAS) att beskrivas utifrån ett grundkoncept (motsvarar dagens + dagens planerade (EWS 39)) samt olika tilläggspaket. Genom att lägga upp värderingen på detta sätt kan vi kombinera både en värdering av dagens plattform och jämföra/värdera andra tänkbara tekniker som lyfts fram framförallt inom projektet VMS flyg.

Under hösten 2002 har FOI-projekten Taktisk värdering telekrig och VMS flyg anordnat ett gemensamt värderingsinternat[45] för att titta på framtida generationer av varnings- och motverkanssystem för JAS 39 Gripen. Studien är i inledningsfasen och det genomförda internatet kommer att följas av ett nytt våren 2003 då underlag etc. förhoppningsvis är mer fylligt.

Det är viktigt att underlag om olika system fördjupas före nästa värdering samt att en vidareutveckling av typsituationerna sker. Detta måste ske i samarbete med olika intressenter – FOI:s teknikavdelningar, FMV och FV. Det kan även vara viktigt att föra en dialog med industrin.

Inom denna verksamhet har ett PM avseende robotar tagits fram. Det beskriver de vanligaste robottyperna, vilka navigeringssystem de använder, målinmätning m.m. Tanken är att detta PM skall uppdateras kontinuerligt med viktiga data avseende robotar.

Därutöver har en studie av Eurofighterns varnings- och motverkanssystem (DASS, Defensive Aids Subsystem) genomförts. Inledningsvis ges en kortare beskrivning av Eurofighterprojektet. Därefter ges en beskrivning av DASS, vilken sammanfattar projektets historia samt listar ingående aktörer. Studien redogör också för i DASS ingående funktioner.

[45] Rapportering av det genomförda arbetet finns i: Andersson, C., Jansson, B., Jonason, T. och Kindvall G., ”Värdering av VMS för flyg. Avrapportering av värderingsinternat samt inriktning av verksamheten under 2003”, FOI-RH--0160--SE, december 2002.

8.3.3 Informationsflöde i nätverk

I takt med att vikten av lednings- och informationskrigföring ökar, och då telekrig är ett av de medel som kan utnyttjas för lednings- och informationskrigföring, är det viktigt att bl.a. bygga upp kompetens att värdera sårbarheten i moderna lednings- och informationssystem.

Som ett led i detta har en förstudie bedrivits med syfte att förbereda en kommande större studie inom informationsteoriområdet. Förstudien har dokumenterats i två rapporter[46]. Målet med arbetet under år 2002 har bl.a. varit att i enkla termer motivera användningen av information som mått på funktionen hos ett nätverk. Ett sådant synsätt kan inte ge detaljerade modeller av specifika system men är ofta enklare och överskådligare att använda vid allmänna betraktelser. Metoden medger en snabb överblick och gör det möjligt att enkelt bedöma effekten av störning och vilseledning med moderna telekrigsmetoder.

Tanken är att med begrepp hämtade från modern informationsteori kunna identifiera och kvantifiera olika flaskhalsar, akilleshälar och potentiella förbättrings-möjligheter, dels inom nuvarande ledningssystemstruktur, dels på en mer generell nivå i ett framtida nätverksbaserat försvar.

I förstudien[47] införs några av den moderna informationsteorins grundbegrepp, särskilt entropi och ömsesidig information. Dessa begrepp används sedan för att preliminärt kvantifiera mängden genuin information i en spaningsradarbild, först innehållande enstaka mål, sedan flera, och till slut ett mycket stort antal elektroniskt genererade skenmål. De mätetal för den genuina informationen som därvid räknas fram utgör en första preliminär grund för värdering av nuvarande, och tänkta framtida, informationshanteringssystem ingående i luftförsvar.

Ett direkt resultat redan av förstudien är att luftförsvarsscenarier med ett normalt antal mål, säg 20, innehåller många storleksordningar mindre entropi än motsvarande scenarier fyllda med elektroniska skenmål från repeterstörsändare. Den belastning denna störform innebär på luftförsvarssystemets informations-hantering kan alltså bli besvärande och måste därför bli dimensionerande.

När endast begränsad eller ingen störning föreligger uppstår kraftig redundans i systemet. Denna kan användas för att betydligt bättre än idag effektivisera och

---

[46] Falk, L., ”Informationsflödet i nätverksbaserat försvar”, FOI-R--0658--SE och Hyberg, P., ”Informationshantering i sensorbaserade luftförsvarssystem – En förstudie”, FOI-R--0564--SE. Syftet med den förstnämnda rapporten är att beskriva nyttan av begreppet information och ange system som lämpar sig för fortsatt studium. Avsikten är att praktiskt undersöka nätverk av sensorer och analysera deras begränsningar i form av flaskhalsar i informationsflödet, störbarhet, etc. Den andra rapporten behandlar informationshantering i sensorberoende luftförsvarssystem och bygger på Shannons teori för kommunikation.

[47] Hyberg, P., ”Informationshantering i sensorbaserade luftförsvarssystem – En förstudie”, FOI-R--0564--SE

skydda den information som strömmar genom systemet, d.v.s. ledningssystemet får en belastningsberoende redundans och tillgängliga kanaler utnyttjas optimalt i alla lägen.

Ett nätverksbaserat försvar (NBF) kräver framförallt snabb och tillförlitlig kommunikation för att olika enheter skall kunna ta över varandras uppgifter. Konceptet kräver att man kan uppdatera enheterna (noderna i nätverket) med nödvändiga data på kort tid. En av svårigheterna ligger i att konceptuellt avgöra hur sådan kunskap skall förmedlas i nätverket, en annan i att bestämma hur stor överföringskapaciteten måste vara.

Detta leder till frågan om man kan ge en kvantitativ bild av hur information flyter i nätverket. För att underlätta diskussionen är det önskvärt att studera informationsflödet i olika sensorsystem och undersöka hur det påverkar striden. Informationsmängden är ett mått på funktionen hos en modern radar och gör att den kvantitativt kan jämföras med andra system.

Ett mål har varit att peka ut vilka nätverk som lämpar sig bäst för fortsatt studium. För att kunna använda begreppet information systematiskt är det nödvändigt att följa förloppet hela vägen från sensor till beslut. Målet är att använda information som mått på funktionen hos ett nätverksbaserat försvar genom analys av välkända sensornätverk, t.ex. Stril, och undersökning av hur informationsflödesfunktionen begränsas av flaskhalsar och hinder i informationsflödet.[48]

Information kan också användas pedagogiskt. Begreppet har successivt införts i radarundervisning vid FHS och andra skolor där FOI verkar. Information har visat sig användbart vid diskussioner om framtida system. För att kunna studera nätverk som Stril och FV 2000 i detalj har kontakter tagits med representanter för FMV och FM.

8.4 Planerade verksamhet i det nya projektet Värdering av telekrig i NBF

Projektets mål och syfte är att öka förståelsen för hur telekrig kan sättas in mot och påverka ett nätverksbaserat försvar samt att få ökad kunskap kring hur nätverks-tanken påverkar och påverkas av telekrigets effekter.

Nätverkslösningar kan medföra att enskilda störinsatser får begränsad effekt p.g.a. att lägesbilderna sammansätts av information från många olika källor. Vår sårbarhet mot en angripares telekrigföring kommer också att förändras då vårt försvar blir nätverksbaserat.

[48] Falk, L., ”Informationsflödet i nätverksbaserat försvar”, FOI-R--0658--SE.

För att kunna minska det nätverksbaserade försvarets sårbarhet mot telekrigföring och optimera vår egen telekrigföringsförmåga krävs studier av telekrigföringen på högre systemnivåer. Därmed krävs också mer komplexa simuleringar och värderingar än tidigare för att belysa telekrigets effekter. Ett exempel som kommer att behandlas är den komplicerade strukturen hos moderna spanings- och ledningssystem.

Några av de verksamheter som kommer att bedrivas under 2003 är:

- Studier av informationsflödet i ett typiskt ledningssystem, exemplifierat med ett sensorbaserat Stril-nät. Analys och förslag till förbättringar med hänsyn till befintliga begränsningar i system, säkerhet, robusthet mot störning samt sårbarhet. För att genomföra studien krävs också att kompetensen kring allmän informationsteori fördjupas inom ramen för projektet.
- Vilka taktiska krav ställer dagens försvar på ett VMS för flygande plattformar? Fortsatt värderingverksamhet av VMS för flygande plattformar kommer att bedrivas. Ambitionen är att både bedriva manuell värdering och simuleringar av VMS för JAS. Under våren 2003 kommer ett värderingsinternat att genomföras.
- Uppföljning och värdering av moderna telekrigssystem
- Metodutveckling för värdering av telekrig i nätverksbaserat försvar
- Stöd/medverkan i FM-studier och FOI-projekt
- Information, undervisning, konferenser, seminarier.