FOI-R--1410--SE
December 2004
ISSN 1650-1942
Underlagsrapport

Tobias Jonason, Lars Falk, Per Hyberg, Roland Heickerö, Björn Modéer

Värdering av telekrig i nätverksbaserat försvar - verksamhet och metodutveckling under 2004

Försvarsanalys
172 90 Stockholm

TOTALFÖRSVARETS FORSKNINGSINSTITUT
Försvarsanalys
172 90 Stockholm

FOI-R--1410--SE
December 2004
ISSN 1650-1942
Underlagsrapport

Tobias Jonason, Lars Falk, Per Hyberg, Roland Heickerö, Björn Modéer

Värdering av telekrig i nätverksbaserat försvar - verksamhet och metodutveckling under 2004

Utgivare Totalförsvarets Forskningsinstitut - FOI Försvarsanalys 172 90 Stockholm	**Rapportnummer, ISRN** FOI-R--1410--SE	**Klassificering** Underlagsrapport
	Forskningsområde 6. Telekrig och vilseledning	
	Månad, år December 2004	**Projektnummer** e1421
	Delområde 61 Telekrigföring med EM-vapen och skydd	
	Delområde 2	

Författare/redaktör Tobias Jonason Lars Falk Per Hyberg Roland Heickerö Björn Modéer	**Projektledare** Roland Heickerö
	Godkänd av E. Anders Eriksson
	Uppdragsgivare/kundbeteckning Försvarsmakten
	Tekniskt och/eller vetenskapligt ansvarig

Rapportens titel

Värdering av telekrig i nätverksbaserat försvar - verksamhet och metodutveckling under 2004

Sammanfattning (högst 200 ord)

Verkan och konsekvenser av telekrig/CNO-dueller i form av kombinatoriska angrepp på nät, system, plattformar påverkar utfallet av hela stridsförloppet.

Under ett flertal år har medlemmar i projektet studerat problematiken runt hur information hanteras och beaktas i ett informationsflöde. I arbetet har ingått att identifiera diverse tekniska och mänskliga aspekter av sårbarheter för telekrigshot samt möjligheten till att skapa robusta nätverk och processer. Arbetet har därmed blivit uppdelat i två mer eller mindre oberoende spår. Där det första spåret tittar på teoribildning runt informationsflöden i sensorbaserade försvarssystem och det andra spåret undersöker metoder för att analysera nätverk och informationsflöden.

De teoretiska studierna som behandlat grundläggande informationsbegrepp, främst entropi har i år utökats med element från modern detekterings- och estimeringsteori, samt även i viss mån med begrepp från perceptions- och socialpsykologi. Parallellt har de teoretiska studierna kompletterats med en utvärdering av praktiska tillämpningar av teorierna genom skapandet av en värderingsmodell.

Nyckelord

inofrmationsflöde, telekrig, bayesianska nätverk, entropi, StriC, STRIL, vilseledning

Övriga bibliografiska uppgifter	**Språk** Svenska
ISSN 1650-1942	**Antal sidor:** 27 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--1410--SE	Base data report
	Programme Areas 6. Electronic Warfare and deceptive measures	
	Month year December 2004	**Project no.** e1421
	Subcategories 61 Electronic Warfare including Electromagnetic	
	Subcategories 2	

Author/s (editor/s)	Project manager
Tobias Jonason Lars Falk Per Hyberg Roland Heickerö Björn Modéer	Roland Heickerö
	Approved by E. Anders Eriksson
	Sponsoring agency Swedish defense
	Scientifically and technically responsible

Report title (In translation)

Assessment of Electronic warfare in network based defense 2004: Activities and Methodology during 2004

Abstract (not more than 200 words)

Information flow has been studied within modern military networks. A number of technical weaknesses have been identified from an electronic warfare perspective and compared with the effect on operators, within the network.

Theoretical studies have been concentrated on the effect of entropy and uncertainty using concepts adapted from modern detection and estimation theory. Experiments have been initiated to evaluate the effect of electronic warfare on networks. The project has tried to evaluate a model of a network based defence with bayesian network.

Keywords

EW, information, entropy

Further bibliographic information	Language Swedish
ISSN 1650-1942	**Pages** 27 p.
	Price acc. to pricelist

Sammanfattning

Utvecklingen mot ett nätverksbaserat försvar förändrar förutsättningarna för att både bedriva telekrig på ledningsnivå, och förmågan till att skydda sig mot verkningar av telekrig. Förändringen är av såväl doktrinär och teknologisk art som organisatorisk och beteendemässig. Ett mål med NBF är att nå informationsöverläge gentemot framtida kontrahenter och därmed kvalitets- och tidsmässiga strategiska och taktiska fördelar. Nätverkstanken innebär att försvarsmakten effektivt kan samordna, styra och fördela resurser över hela det operativa fältet. Genom förmågan till kraftsamling inom ramen för uppdragstaktik och manöverkrigföring, bedöms verkan mot olika typer av mål bli bättre än tidigare.

Sammanfattningsvis kommer telekrig, i en utvidgad form, att bli allt mer integrerat i den militära verksamheten. Verkan och konsekvenser av telekrig/CNO-dueller i form av kombinatoriska angrepp på nät, system, plattformar påverkar utfallet av hela stridsförloppet. Under ett flertal år har medlemmar i projektet studerat problematiken runt hur information hanteras och beaktas i ett informationsflöde. Årets studie har främst riktats dels mot att utveckla teorier kring störning av informationsflöden dels att få igång ett samarbete med StriC och förstå hur ledningssystemet är organiserat, vilka uppgifter som utförs och av vem. I arbetet har ingått att identifiera diverse tekniska och mänskliga aspekter av sårbarheter för telekrigshot samt möjligheten till att skapa robusta nätverk och processer. Arbetet har därmed blivit uppdelat i två mer eller mindre oberoende spår. Där det första spåret tittar på teoribildning runt informationsflöden i sensorbaserade försvarssystem och det andra spåret undersöker metoder för att analysera nätverk och informationsflöden.

De teoretiska studierna som behandlat grundläggande informationsbegrepp, främst entropi har i år utökats med element från modern detekterings- och estimeringsteori, samt även i viss mån med begrepp från *perceptions- och socialpsykologi*. Parallellt har de teoretiska studierna kompletterats med en utvärdering av praktiska tillämpningar av teorierna genom skapandet av en värderingsmodell.

Att skapa en modell baserad på bayesiansk statistik och som hanterar informationsflödet i ett nätverksbaserat försvar är idag svårt. Det beror främst på att de empiriska kunskaperna rörande följder av vilseledningsattacker är bristfalliga samt att de bayesianska nätverken endast hanterar riktade förhållanden och inte interaktioner (loopar).

INNEHÅLLSFÖRTECKNING

1 Inledning

1.1 Bakgrund

Utvecklingen mot ett nätverksbaserat försvar förändrar förutsättningarna för att både bedriva telekrig på ledningslnivå, och förmågan till att skydda sig mot verkningar av telekrig. Förändringen är av såväl doktrinär och teknologisk art som organisatorisk och beteendemässig. Ett mål med NBF är att nå informationsöverläge gentemot framtida kontrahenter och därmed kvalitets- och tidsmässiga strategiska och taktiska fördelar. Nätverkstanken innebär att försvarsmakten effektivt kan samordna, styra och fördela resurser över hela det operativa fältet. Genom förmågan till kraftsamling inom ramen för uppdragstaktik och manöverkrigföring, bedöms verkan mot olika typer av mål bli bättre än tidigare.

Sammanfattningsvis kommer telekrig, i en utvidgad form, att bli allt mer integrerat i den militära verksamheten. Verkan och konsekvenser av telekrig/CNO-dueller i form av kombinatoriska angrepp på nät, system, plattformar påverkar utfallet av hela stridsförloppet.

1.2 Syfte

Värdering av telekrig i nätverksbaserat försvar är ett treårigt FoT-finansierat projekt vid Försvarsanalys, institution 18. Det påbörjades första januari 2003 och avslutas sista december 2005. Budgeten uppgår totalt till ca 10 Mkr varav 3,1 Mkr fördelas under 2004. Fem personer ingår i projektets kärna. Under 2003 genomfördes två delprojekt [1]; ”Värdering av VMS för Flyg” samt ”Informationsflöden i lednings- och sensorsystem”.

Syftet med projektet ”Värdering av Telekrig i NBF” är att studera hur försvarsmakten kan optimera telekrigsförmågan på högre systemnivåer. Målet är att förstå hur det nätverksbaserade systemet kommer att påverka telekrigföringen och hur NBF kan påverkas av telekrig. I arbetet ingår att dels beskriva hur ett modernt spanings- och ledningssystem fungerar under störda förhållanden dels utveckla metoder, teorier och begreppsapparat för modernt telekrig på C2-nivå.

Rapporten syftar till att sammanfatta och redovisa årets arbete.

1.3 Arbetsinriktning 2004

Under ett flertal år har medlemmar i projektet studerat problematiken kring hur information hanteras och beaktas i ett informationsflöde [2], [3]. Årets studie har främst riktats dels mot att utveckla teorier kring störning av informationsflöden dels att få igång ett samarbete med StriC och förstå hur ledningssystemet är organiserat, vilka uppgifter som utförs och av vem. I arbetet har ingått att identifiera diverse tekniska och mänskliga aspekter av sårbarheter för telekrigshot samt möjligheten att skapa robusta nätverk och processer.
Arbetet har därmed blivit uppdelat i två mer eller mindre oberoende spår. Där det första spåret tittar på teoribildning runt informationsflöden i sensorbaserade försvarssystem och det andra spåret undersöker metoder för att analysera nätverk och informationsflöden.

De teoretiska studierna som behandlat grundläggande informationsbegrepp, främst entropi har i år utökats med element från modern detekterings- och estimeringsteori, samt även i viss mån med begrepp från perceptions- och socialpsykologi. Parallellt har de teoretiska studierna kompletterats med en utvärdering av praktiska tillämpningar av teorierna genom skapandet av en fysisk värderingsmodell.

1.4 Avgränsningar i årets studie

Fokus i detta skede har inte legat på att utveckla teorier kring olika slag av nätverk och deras förmåga till telekrigföring respektive skydd från dito. Det arbetet kommer att utföras under 2005.

1.5 Närliggande projekt, resultatöverföring och externa relationer

Närliggande projekt och studier inom FOI är ”Telekrig i breddad hotbild”, ”Nätverksbaserat försvar i ett internationellt perspektiv”, ”Telekrig mot GNSS” respektive ”FoRMA-nät”. Koordinering och resultatöverföring mellan projekten har skett regelbundet. Teorier kring nätverksbaserat försvar har bl. a delgivits av programkontoret på FHS.

Som ett led i att utveckla den teoretiska begreppsapparaten har kontakt inletts med FOI:s brittiska motsvarighet DSTL för utbyte av information. Det har varit ett sätt, därtill ett formellt krav från FoT, att från projektets sida dels förstå utvecklingen av NEC-konceptet i relation till NBF, dels belysa deras syn på telekrigsföring kopplat till störning av informationsflöden i nätverk. Utbytet kommer att fortgå under 2005.

1.6 Årets produktion:

1.6.1 Milstolpar

”Omvärldsuppfattning i sensorbaserade luftförsvarssystem”,
Hyberg P. FOI-R—1392--SE, November 2004.

”Kvantitativa beslut i nätverksbaserat försvar”,
Falk L. FOI-R--1390, December 2004.

1.6.2 Övriga bidrag:

”Telekrig i nätverksbaserat försvar: litteratursökning jan-feb 2004”
Hyber P, Jonason T., FOI-D—0164—SE, April 2004

"Information in radar - a tribute to P. M. Woodward”
Falk L., Waveform Diversity and Design Conference, Edinburgh, November 2004. Conference CD.

”Information Flow in an Air Defence System”
Falk L., föredrag på DSTL, Farnborough, 6 maj 2004.

2 Teorier och metoder för att analysera nätverk samt informationsflöden

Informationsflöden i ett nätverksbaserat försvar omfattar en mängd skilda ämnesområden, som nätverksteori, organisationsteori, psykologi etc. För att lättare kunna hantera ämnesområdets strävar projektet efter att bygga upp en begreppsapparat som skall bidra till en enklare hantering av frågeställningar. Projektet studerar informationsflöden utifrån begrepp som entropi och bayesiansk statistik. Nedan sammanfattas essensen hos dessa begrep.

2.1 Information

Moderna ledningssystem konstrueras ofta som nätverk där man kan fatta beslut baserat på all tillgänglig information. Nätverken är robusta eftersom plattformarna kan lösa flera uppgifter och vid behov ersätta varandra.

Flexibiliteten är en grundtanke i nätverksbaserat försvar (NBF), men det finns gränser för vad systemet kan uthärda, t ex vid bekämpning med telekrig. En viktig slutsats är att vilseledning kan vara effektivare än störning med rent brus (Falk 2004). Nätverk som vuxit fram organiskt under längre tid (t ex Stril med sin 50-åriga historia) uthärdar ofta slumpvisa störningar väl, men är känsliga för störningar riktade mot beslutssystemet. Detta är en allmän iakttagelse som bekräftats vid studiet av organiskt framvuxna nätverk både i naturen och samhället [4],[5].

RMA (Revolution in Military Affairs) antyder att avsikten var att lösa upp de hierarkiska systemen och ersätta detaljerade föreskrifter med friare beslut för att åstadkomma snabbare och effektivare insatser.

Sådana insatser kräver omfattande information. En häftig debatt har förts om vilken mängd information som bör föras över till olika förband, men verkligheten har redan överflyglat diskussionerna. Under operation Iraqi Freedom fördes information framgångsrikt ut till bataljonsnivå och man kan vänta sig en förbättring även på lägre nivåer.

En fråga som blivit mindre belyst, men är lika viktig, är hur denna information passar in i de beslut som ska fattas, d v s dess relevans. Frågan är också hur stabil informationen är mot störning som kan förekomma i en mindre asymmetrisk konflikt än den i Irak. För att beskriva problemet behövs ett kvantitativt mått på den information som finns tillgänglig och på den som saknas.

Shannons beskrivning av information (kapitel 2.2.2) passar väl in på militära problem. Man vet ofta rätt väl vilken information som saknas inför ett beslut. Frågan hur en sådan beskrivning används för att uppskatta hotet mot nätverksbaserat försvar har tidigare diskuterats [3], [6]. I denna rapport inriktas diskussionen mot specifika system där kvantitativa mätningar kan ske.

2.2 Sannolikhetsteori

Problem rörande information och informationstillförsel beskrivs enklast med sannolikhetsteori. För att få en uppfattning om prestanda måste osäkerheterna som påverkar ett beslut beaktas. Ändamålet kräver även att systemets uppgift och de faktorer som påverkar beslutet är kända.

Bland dessa sannolikheter och osäkerheter finns också personalens kunskap och förmåga. Det kan vara en svår uppgift att beskriva dessa faktorer, men ett militärt system är ofta så väldefinierat till sina uppgifter att man har en god uppfattning om personalens förmåga. Dessutom behöver man bara väga samman de väsentliga bidragen i informationsflödet för att uppskatta systemets förmåga. Personalens ”tysta” kunskap är inte särskilt svår att komma åt i detta fall. Problemet är snarare att veta när situationen blir så komplicerad att människan är hjälplös.

Fördelen med sannolikhetsteori är främst att den ger en allmän princip för att värdera systemets prestanda:

Ett optimalt beslut kan (i medeltal) bara fattas om all information avvänds på rätt sätt.

Denna enkla princip gäller enbart inom sannolikhetsteorin [7], [8]. Det låter överraskande, eftersom vi kan vara utsedda för falsksignalering. Poängen är att det står oss fritt att avstå från misstänkta data, men detta måste ske efter en förnuftig bedömning. Regeln tvingar oss alltså att fatta *rationella beslut*, vilket är anledningen till att den rekommenderas här.

2.2.1 Osäkerheter

Regeln ovan leder till rationella beslut men den kräver att man har ett gemensamt mått för objektiva och subjektiva sannolikheter, kvantiteter som vi normalt är vana att hålla åtskilda. Med hjälp av sannolikhetsteorin kan man uppskatta osäkerheter i uppmätta parametrar och även i kunskapsläget hos en person.

Sannolikhetsteorin är rent matematisk och innehåller i sig inga motsägelser. Den svåra frågan är om den kan tillämpas på vår verklighet. Överraskande nog går det bra att behandla objektiva och subjektiva sannolikheter på samma sätt. Så länge man behandlar sannolikheter rationellt (enligt reglerna i sannolikhetsteorin) går det bra att använda sina egna uppfattningar, som vid vanliga beslut. Den enda förutsättningen är att sannolikheterna kan uttryckas med positiva tal och att resultatet av våra resonemang ska vara oberoende av i vilken ordning informationen används.

Alla egenskaper hos ett nätverk av sensorer kan beskrivas med sannolikheter. Det krävs enbart att hypoteserna kan uttryckas med första ordningens logik, vilket inte är något särskilt restriktivt villkor. Svårigheten ligger i att göra beräkningarna i praktiken. De måste ofta förenklas utan att det väsentliga i teorin går förlorat, eftersom goda beslut kräver att alla väsentliga osäkerheter kommer med.

P. M. Woodward använde tidigt denna princip för att härleda en ideal metod för radarmätningar. Woodward formulerade principen så att signalbehandlingen i en radar måste vara omvändbar om resultatet ska bli optimalt [7], [9]. Detta villkor innebär att all information bevaras under processen, eftersom man då alltid kan återvinna sina ursprungliga data.

Datorerna har gjort det lätt att tillämpa Woodwards princip i de tekniska lagren av ett sensorsystem. Svårigheten ligger i att beskriva de mänskliga operatörerna, som behövs om man ska kunna använda nätverket för att lösa säregna och ovanliga situationer.

2.2.2 Sannolikhet som kunskap

Sannolikheten för en händelse beskriver vår osäkerhet om vad som kommer att hända i en viss situation. Det vanligaste exemplet är en tärning som antas ha sannolikheten 1/6 att ge ett visst antal prickar vid ett kast. Detta påstående betyder sällan att vi har granskat tärningen eller studerat den under många kast, som den klassiska teorin föreskriver.

Snarare anger sannolikheten att vi för ögonblicket inte ser någon anledning att föredra en sida framför en annan. Det handlar alltså om vår egen uppfattning som beskrivs av en subjektiv sannolikhet beroende på vår bristfälliga kunskap om situationen. En liknande situationen kan uppstå i en ledningscentral, där man snabbt behöver komma till beslut.

Den som har gott om tid att kontrollera prestanda, t ex genom att kalibrera en sensor, kan genomföra en mätning som ger nästan objektiva resultat, men för det mesta är sannolikheten mer subjektiv än vi vill erkänna. Sannolikhet är ett naturligt mått i många militära situationer, t ex vid spaning och målföljning med radar. Frågan är då hur noga man kan beskriva kunskap och sannolikheten för felaktiga mänskliga bedömningar utförda av observatörer. Detta problem diskuteras av Per Hyberg för en radarcentral [10].

Kunskap betraktas traditionellt som en additiv kvantitet som ökar med mängden information. Hartley definierade på 1920-talet information som det antal digitala enheter som behövs för att lagra kunskapen i oförvanskad form. Mängden information svarar då mot längden på meddelandet, d v s mot logaritmen av talet själv vilket svarar mot begreppet *bit*.

Enligt den kommunikationsorienterade informationsteorien ses det intuitiva begreppet information som synonymt med *opredikterbarhet*. Shannon löste nämligen problemet genom att i stället för kunskap beskriva bristen på kunskap, som han kallade *entropi*. Denna kvantitet är ett mått på osäkerheten i en given situation och uttrycker hur mycket information man i medeltal får från en mätning av en variabel med olika tänkbara utfall.

Detta innebär att ett meddelande med ett till fullo förutsägbart innehåll inte bidrager till någon kunskapsökning hos mottagaren eftersom det inte innehåller någon genuint ny information. Motsatsen, d.v.s. ett innehåll som i princip är oförutsägbart, innehåller maximal information.

Figur 1: Exempel på en valsituation där entropin (osäkerheten) är 1 bit.

Uttryckt på detta sätt är information uppenbarligen en kvantitet som ger möjligheter att skingra osäkerhet och mer exakt analysera den stora mängd information som hanteras i ett spaningssystem eller ett nätverk av sensorer.

2.3 Bayes formel

Engelsmannen Bayes studerade i mitten på 1700-talet hur många gånger man borde kasta ett mynt för att avgöra om det är äkta eller falskt. Liknande frågor uppkommer ofta inom modern medicin och läkemedelsindustrin, om man vill förkorta sina försöksserier och i modern sensorteknik: vilken signalstyrka krävs för att man ska kunna upptäcka ett fluktuerande mål i klotter och brus?

Det ansågs länge motbjudande att förknippa hypoteser med ”subjektiva sannolikheter,”, men subjektiva bedömningar är alltid med vid bedömning av sannolikheter och de flesta militära beslut bygger på en blandning av ”objektiva” och ”subjektiva” bedömningar, som hämtas från sensorer och experter. I militära bedömningar tillkommer dessutom att man måste bedöma motsidans avsikter och förmåga.

Om man låter *(i)* beteckna hypotesen H_i och *(k)* utfallet x_k av ett försök ger Bayes’ formel ett uttryck för att uppdatera sannolikheten för en hypotes.

$$p(H_i|x_k) = p(x_k|H_i)p(H_i)/p(x_k) \qquad (1)$$

Formeln visar hur mycket sannolikheten av (eller tron på) en hypotes H_i ändras genom mätresultatet x_k,

Bayes’ formel värderar all information lika oavsett i vilken ordning den används. Den skiljer sig därvidlag från otränade mänskliga bedömare som gärna värderar den första faktor som väcker uppmärksamhet mycket högt. Människan har dessutom svårt för att värdera sannolikheter som ligger långt från vardagliga värden och förnekar gärna möjligheten av osannolika hypoteser. Erfarenheterna av schackdatorer visar att kombinationen toppspelare tränad av datorer är formidabel. Liknande effekter kan väntas för sensor- och beslutssystem om man systematiskt tränar observatörerna i speciellt besvärliga situationer valda med datorns hjälp.

Bayes’ formel uppgraderar ständigt vår uppfattning med nya data. Man måste börja någonstans och de ursprungliga osäkerheterna brukar kallas sannolikheter *a priori* (engelskans ”priors”). De nybildade osäkerheterna kallas sannolikheter *a posteriori*. Eftersom Bayes’ formel jämför osäkerheter före och efter en observation kan man helt enkelt tala om sannolikheter före och efter en mätning.

Den stora fördelen med Bayes’ formel är att den visar att man inte beskriver kunskap utan *osäkerhet* om ett läge. Detta synsätt är särskilt nyttigt i sensorsystem. Givet en viss uppgift skapar man förutsättningar för visst beslut med hjälp av sensordata. Systemet behöver snarare undanröja osäkerhet än skaffa ny, detaljerad kunskap inför vissa beslut. Det innebär i många fall att det är enklare att bekämpa ett sensorsystem med systematisk falsksignalering än med brus. Det är viktigare att skapa förvirring än att dölja detaljerad kunskap om verkliga mål [9].

2.4 Verktyg

2.4.1 Bayesianska nätverk

De praktiska tillämpningarna av Bayes' formel kom med datorernas genombrott. Man kunde plötsligt kosta på sig att uppdatera alla omdömen efter en enda mätning. Den största fördelen är dock att Bayes' formel bevisligen leder till en optimal bedömning under givna förutsättningar; det innebär att man har optimala förutsättningar för en beslutsprocess.

Bayesianska nätverk är ett verktyg för att beräkna sannolikheten att någonting "inträffar" utifrån en mängd olika premisser. Bayesianska nätverk ger inget svar på hur en situation skall behandlas utan visar endast en sannolikhetsuppskattning baserad på de i modellen implementerade sannolikhetsvärdena.

Bayesianska nätverk är uppbyggt av en mängd noder. Noderna representerar en aktivitet eller tillstånd och består av variabler som representerar olika tillstånd inom noden. De noder som påverkar varandra binds samman av riktade länkar. Varje nod i nätverket är förknippad med en sannolikhetstabell. Sannolikhetstabellen består av fördelade apriorivärden över sannolikheten för nodens utfall.

Sannolikhetsvärdena beräknas genom Bayes sats (1). De implementerade sannolikhetsvärdena i modellen behandlas som subjektiva och deras ursprung kan vara av olika art, som expertbedömningar eller mätningar. Det görs ingen skillnad på sannolikhetsvärdets härkomst.

Det finns ett antal olika verktyg för att skapa bayesianska nätverk på marknaden [11]. Projektet använde verktyget GeNIe version 2.0.

2.4.2 Morfologisk analys

"Morfologisk analys (formlära) är en generell metod för icke-kvantifierad modellering. Metoden används för att skapa modeller av mångdimensionella sociala, politiska och tekniska problemkomplex som inte på ett meningsfullt sätt kan kvantifieras. Sådana problemkomplex kännetecknas av att de är extremt olinjära, att de innehåller så kallade osäkerheter och att de måste hanteras på basis av bedömningar" [15].

Morfologisk analys är en metod för de första stegen i bearbetningsprocessen av problem. Metoden utnyttjas för att strukturera problem och frågeställningar som befinner sig i ett initialt tillstånd av oreda. För problem eller frågeställningar som är mer väldefinierade är verktyget/metoden lämplig att utnyttja för att ta fram och undersöka olika lösningar. Projektet valde att utnyttja det morfologiska verktyget MA/Casper(Computer Aided Scenario and Problem Evaluation Routine).

Verktyget består av ett fält i matrisform. Fältet är uppdelat i en mängd kolumner, som i sin tur är indelade i celler. Varje kolumn har en rubrik kallad parameter. Parametern definierar kolumntypen som exempelvis ”geografisk prioritering” i figuren nedan. De övriga cellerna i kolumnen kallas tillstånd och består av de olika värdena som en parameter kan anta. Flera olika tillstånd från olika parametrar kan samexistera i det morfologiska fältet och skapar då en konfiguration.

Geografisk prioritering	Funktionell prioritet	Storlek och trängsel	Nybyggande	Underhåll	Skyddrums-filosofi
Endast största städerna	Alla socio-tekniska functioner	Stora, ej trånga	Med nybyggande	Mer frekvent	Alla får samma skydd
Städer med minst 50,000	Tekniska stödsystem	Stora, trånga	Kompensation för nuvarande brister	Nuvarnade nivå	Alla tar samma risk
Förorter och landsbygden	Humanitär inriktning	Små, ej trånga	Endast under "återtagning"	Inget	Funktionella nyckelpers. prioriterade
Ingen geografisk prioritering	Bostäder	Små, trånga			De svaga priorterade

Figur 2: exempel på ett morfologiskt fält

3 Arbetsinriktning 1: Teoribildning runt informationsflöden i sensorbaserade luftförsvarssystem

I följande kapitel dokumenteras årets inriktning av arbetet inom den teoretiska delen av projektet.

Arbetet är baserat på den tidigare förstudien [2], och syftar till att vidga perspektivet, från den rent informationsteoretiska/radartekniska nivån upp till den mänskliga beslutsfattningsnivån. Detta gjordes genom att betrakta en ensam operatör av ett manuellt stöttat luftvärnssystem, samt en mindre grupp beslutsfattare i en luftförsvarscentral (STRIL-central).

Analysen utökas med element från modern detekterings- och estimeringsteori, samt även i viss mån med begrepp från perceptions- och socialpsykologi. Detta för att utvidga den begreppsapparat som hittills använts för att studera nätverksbaserade försvar, speciellt telekrig i och mot NBF. Ett viktigt syfte med utvidgningen är att medge kvantitativ analys av telekriginsatser mot ett nätverksbaserat försvar, speciellt på sådana delområden där man hittills varit hänvisad till enbart bedömningar.

3.1 Människor i beslutsprocessen

Människan kan beskrivas som ett informationsbehandlande system, som har flera olika funktioner var och en behäftad med sina begränsningar. I stora drag består det av tre delsystem: ett perceptuellt, ett kognitivt och ett motoriskt.

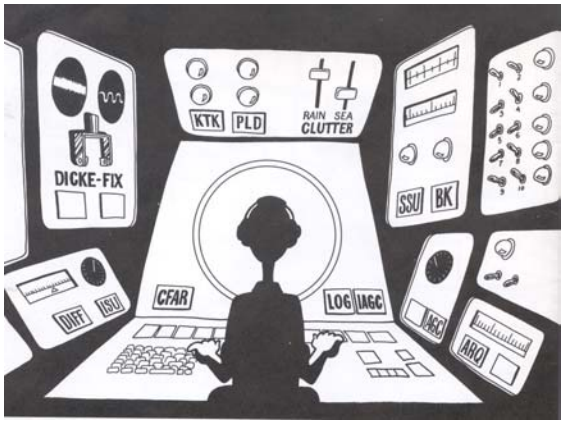
Människan har begränsningar i minnes- och bearbetningskapacitet men också många egenskaper som tekniska system ännu så länge saknar, exempelvis flexibilitet, kreativitet, fantasi och abstrakt tänkande. Människors kapacitet med avseende på de olika egenskaperna varierar högst väsentligt mellan olika individer. Olika faktorer som fysisk och social stress, trötthet och hunger, kan även avsevärt försämra hur man presterar.

3.2 Operatörsperspektivet

Enligt modern perceptionspsykologi sätter operatören omedvetet upp ett antal möjliga scenarier mellan vilka han sedan väljer. Vilka scenarier som därvid uppfattas som möjliga bestäms av faktorer som egen allmänkunskap, tidigare erfarenhet och intuition, utbildning, ordergivning samt organisatoriska faktorer. Om ett auktoritärt ledningsparadigm (order-givning) får ersätta någon av de övriga faktorerna, ökar risken för att exempelvis en radarsensors utdata associeras med felaktigt scenario.

3.2.1 Entropi och perception

I detta avsnitt tillämpas entropi- och informationsbegreppen på ett luftvärnsförband och en mänsklig operatör i det betraktade beslutssystemet där operatören skall fatta beslut och genomföra, (*i*) val av mål, (*ii*) följestöttningsåtgärder och (*iii*) bekämpning avanfallande flygplan.



Figur 3. Antalet handlingsalternativ för en operatör av en lokalspaningsradar i ett luftförsvarssystem kan vara stort. Handlingsalternativreducerande instruktioner och d:o utbildning måste vara mycket väl utformade, och förutseende, för att inte de korrekta handlingsalternativen skall uteslutas. Telekrigåtgärder sätts lämpligen in mot just sådana brister i utbildning och instruktioner.

I enheten för luftbevakning i en STRIL-central har de mänskliga operatörerna en viktig roll i att upptäcka och identifiera mål. Detta är även den funktion som är mest sårbar för olika telekriginsatser. Även i många andra system måste mänskliga operatörer tolka information som påverkas av telekriginsatser. Operatörerna påverkas av hot som är kopplade till olika former av telekrig. Det är därför viktigt att beakta den mänskliga operatören när effekterna av olika former av telekrig skall värderas.

För en operatör vid exempelvis en lokalspaningsradar finns en rad åtgärder som kan vidtagas beroende på hur operatören ifråga tolkar den rådande situationen, d.v.s. beroende på hans rådande *omvärldsuppfattning*. Operatörens omvärldsuppfattning uppdateras ständigt och byggs upp i relation till utbildning och tidigare erfarenhet, och med ledning av vad sensorn visar. Omvärldsuppfattningen kompletteras dessutom med annan information utifrån.

För att minska antalet handlingsalternativ utbildas operatören i handhavande av sensor-utrustningen. Med automatik och datorer kan presentationen förenklas och handlings-alternativen därmed kraftigt minska i antal. Detta kan vara frestande för den som anskaffar och vidmakthåller systemet eftersom operatören då inte behöver ha annat än en översiktlig kunskap om sensorsystemets tekniska funktion och möjliga förekommande scenarier. Emellertid ligger det en mycket stor risk i att driva denna form av entropireducering för långt: Sannolikheten att inte klara av oförutsedda drifttillstånd, och oförutsedda scenarier, ökar. Med telekrigperspektivet pålagt blir denna sannolikhet stor, eftersom motståndaren når maximal effekt om han konstruerar och sätter in sina telekrigsystem *just för att exploatera dessa svagheter*. Motståndarens beteende kan förväntas vara sådant att han når stor effekt, d.v.s. han kan förväntas exploatera dessa svagheter.

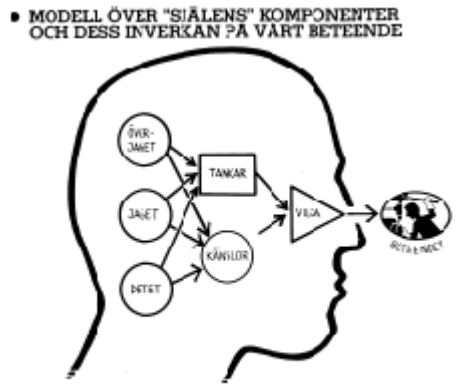
Ovanstående problematik kan tydliggöras i termer av entropi och informationsteori (kapitel 2.1 – 2.2). Graden av handhavandeförenkling man uppnår med en förbearbetad och symbol-orienterad sensorpresentation kan kläs i mätetal med hjälp av Shannons informationsteori. Antalet förbisedda eller avsiktligt uteslutna indatakombinationer till sensorn (exempelvis trovärdiga grupper av koherenta skenekon) viktade med bedömda sannolikheter, kan också kläs i mätetal. Mer komplex signalbehandling och mer komplex presentation och utbildning, kostar ekonomiskt, men kan leda till färre uteslutna scenarier, d.v.s. färre scenarier man inte klarar av.

Ett exempel på risken med för kraftig entropireducering är projekt TYRA där ett antal värnpliktiga radarluftvärnsoperatörer testades före och efter sin utbildning i en radarsimulator. Resultatet visade att de värnpliktigas förmåga att följa radarmål under konventionella störformer hade förbättrats märkbart av utbildning medan den hade försämrats mot moderna störformer som de inte övat emot.

Detta illustrerar hur felaktig, d.v.s. alltför snäv, utbildning, i den vällovliga ambitionen att reducera entropin, tyvärr kan utesluta viktiga delar av sanningen. När dessa delar inträffar, d.v.s. i detta fall de nya typerna av störmönster, försämrar en sådan snäv utbildning förmågan att lösa uppgiften. Den kvantitativa analys som dessa begrepp medger kan därför tillföra nya och tydligare insikter, och möjlighet att värdera resultat av förändringar.

3.2.2 Val mellan inlärda tolkningskategorier, tröskelsättning och beslut

För den ensamme beslutsfattaren tillkommer som en viktig aspekt personliga egenskaper och böjelser, tillfälligt sinnestillstånd, m.m. Dessa parametrar kan i ett stressat läge avgöra vilket tolkningsalternativ av presenterade sensordata som mer eller mindre intuitivt väljs.



Figur 4: Perceptionen är avgörande för hur människan fungerar tillsammans med apparater. Tolkning av presenterade symboler och skeenden beror bl.a. av individrelaterad, personlighetspsykologiska faktorer. Denna operatörsindividualism kan motverkas med utbildning, träning, och allmänt grundtekniskt kunnande om det system människan skall samfungera med. Även kunskap om rådande scenario och motståndare är betydelsefull. Figuren visar den psykoanalytiska modellen, uppställd av bl.a. Homburger-Eriksson.

Att perception påverkas av motivation och andra med- eller omedvetna psykologiska processer och tillstånd, är ett tidigt resultat inom perceptionspsykologin [12]--[14].

3.3 Tröskelsättning och beslut

Operatörens arbete kan beskrivas som en sekvens av beslut som kontinuerligt fattas mot bakgrund av realtidsindata från indikatorer och kommunikationsvägar. Ofta fattas dessa beslut omedvetet, dvs grundade på intuition och reflexer, ungefär som vid bilkörning.

Handlingsalternativen är intimt kopplade till hur operatören uppfattar situationen. Hur han uppfattar situationen beror av de ovan nämnda bakgrundsfaktorerna plus de (medvetna eller omedvetna) situationsalternativ vilka upplevs som möjliga. Det är känt från perceptions-psykologin att sensorintryck som entydigt borde peka ut ett visst scenario (bland andra alternativa), kan blockeras. Ofta beroende på att man redan är "låst" i en viss uppfattning. Denna låsning kan ha skett därför att sensordata sekunderna innan tydde på ett välkänt alternativ som man då låste sig för. Sedan "filtreras" efterföljande sensordata /sinnesintryck så att de stämmer med den redan valda omvärldsuppfattningen. Detta är ett effektivt sätt för hjärnan att reducera sinnesintryckens entropi och bringa ordning. Att förkasta en redan vald omvärldsuppfattning är påfrestande, utlöser inre skyddsmekanismer, och leder till s.k. kognitiv dissonans. Detta är grunden för all vilseledning (kognitiv avhakning), riktad mot människor. Motsvarande mekanismer (fast på en annan nivå) finns i duellen mellan sofistikerade störskydd i sensorer och vilseledande störning riktad mot sådana sensorer.

3.4 Neyman-Pearsons teorem

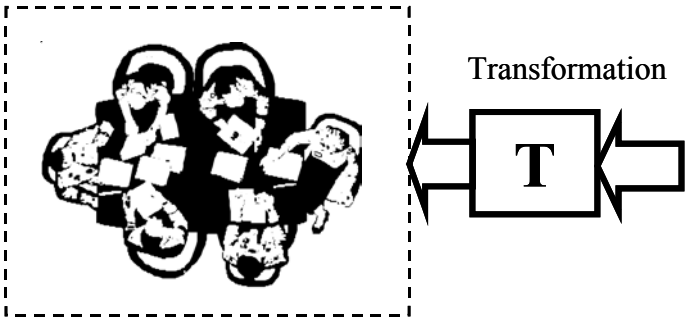
Shannons informationsteori pekar på att det optimalt kodade, d.v.s. det optimalt informations-täta dataflödet, i princip inte skiljas från Gaussiskt brus, åtminstone inte för stora data-mängder. För ett framtida nätverksbaserat försvar där en mycket stor mängd information strömmar runt, blir alltså den Gaussiska modellen bättre, ju bättre informationen i detta nätverk är kodad. Av ekonomiska och andra skäl kan man förmoda att informationen i ett sådant nätverk bör vara optimalt kodad, d.v.s. dataströmmarna kan modelleras som Gaussiska. Neyman-Pearsons detektor kan visas vara en optimal detektor för sådana dataflöden. Prestanda hos denna detektor kan därför användas för att analysera möjligheterna att upptäcka små ändringar i informationsflödet i ett större nätverk.

3.4.1 Bayes riskkriterium

Bayes riskkriterium behandlar diffus förhandskunskap för att stötta beslut. Det sker genom att felbeslut åsätts vissa kostnader [10]. En slutsats av detta är att det bayesianska angreppssättet vid perfekt förhandskunskap närmar sig den optimala Neyman-Pearsonska detektorn. Strikt gäller detta sådan förhandskunskap som kan beskrivas analytiskt, men denna optimalitet bör kunna vara vägledande för analyser även på högre nivå.
Fördelen med Bayes synsätt är att även diffus och intuitiv förhandskunskap kan hanteras.

3.5 STRIL-central: Uppdatering av omvärldsuppfattning

Beslutsfattare i en STRIL-central skall med hjälp av den nyinkomna sensorinformationen, plus annan tillgängliginformation, dels tolka och *uppdatera omvärldsuppfattningen*, och dels fatta beslut om åtgärder.

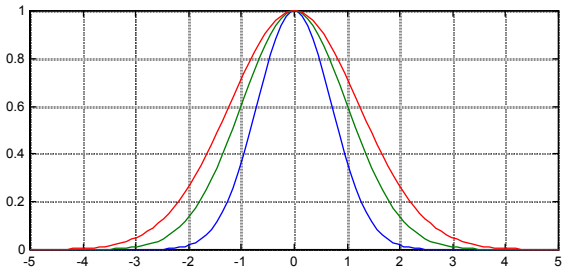


*Figur 5. Situationen i ett bergrum där ett antal beslutsfattare skall tolka det inkommande informationsflödet för att i detta försöka detektera någon viss viktig förändring (händelse) som kräver åtgärder i form av analys, beslut och kanske ordergivning. Matrisen **T** symboliserar den transformation på informationsflödet som bl.a. telekrigsinsatser kan utgöra.*

Ett sätt att studera *övergripande begränsningar* i möjligheterna att dra nytta av det inkommande dataflödet är att betrakta detta som en Gaussisk stokastisk process, d.v.s. inför fattandet av ett visst beslut då viss specifik information behövs, så måste denna specifika information filtreras fram ur en stor mängd annan för stunden irrelevant information. Denna senare irrelevanta information kan modelleras som Gaussiskt brus om källorna är många och oberoende, speciellt om de är optimalt kodade. Detta öppnar vägen för användandet av känd teori för detektering och parameterestimering i större nätverk.

3.6 Cramér-Rao -gränsen och Bayes synsätt, förhandskunskapens betydelse

Sett ur detta övergripande perspektiv blir en intressant fråga hur små förändringar i det totala flödet av information som i princip kan detekteras, d.v.s. hur tydligt måste ett inkommande budskap vara för att inte försvinna i den totala mängden av budskap som strömmar in.



Figur 6. När människan betraktar ett komplext informationsflöde bildar hon en omedveten kriteriefunktion, d.v.s. ett intuitivt summamått på hur starkt informationsflödet pekar ut ett visst händelsealternativ. Skärpan i denna kriteriefunktion (andraderivatan) avgör risken att reagera fel, d.v.s. reagera på näraliggande händelser som på ett likartat sätt avspeglar sig i informationsflödet. I figuren är alla kriteriefunktionernarna normerade till max 1.

Cramér-Rao–gränsen [10] beskriver den minsta skillnaden mellan avtrycken i dataflödet som måste underskridas för att skenhändelser i princip inte skall kunna skiljas från sanna händelser, detta under förutsättning att estimatorn, det vill säga den apparatur eller de inlärda tolkningsreglerna hos personalen är ideala. En typisk tillämpning är successiv vilseledning som tar avstamp i en ”sann” omvärldsuppfattning.

Den som planerar en telekriginsats mot besluten bör enligt ovan beakta följande punkter:

- Generera störsignaler som i CRB-meningen ger avtryck i indataflödet till STRIL-centralen vilka minimalt skiljer sig från de avtryck som svarar mot den felaktiga omvärldsuppfattning man vill skall uppstå i stället för den sanna i STRIL-centralen.
- CRB-kriteriet ger ett sätt att bestämma ett siffervärde för detta maximalt tillåtna åtskiljande
- Störsändning mot viorna in till STRIL-centralen skall svara mot optimal käll- och kanalkodning för det näraliggande sken-scenariot, d.v.s. även kommunikations-störningen bör signalanpassas (DRFM-teknik).
- För att skensignaleringen eller skenmålsgenereringen inte skall kunna motverkas (tappa intensitet och andraderivator (se toppen på kurvan i figur 6) i CRB-meningen) i filtret in till bergrummet, bör skeninformationen i alla avseenden, såväl till form (modulation, gränssnitt, statistik), som innehåll (taktisk nivå, flygföretags gruppering och beteende) minimalt skilja sig från det som beslutsfattarna i bergrummet kan förmodas anta vara verkliga och sanna. (taktisk vilseledning). Helst bör även kunskap om utbildning, träning, instruktioner, förväntade psykologiska spärrar, rädslor, m.m vägas in (kognitiv vilseledning).

3.7 Slutsatser arbetsinriktning 1

De viktigaste resultaten under året är att dessa etablerade begrepp och teorier från informations- och detekteringsteorin mycket väl kan användas för att i kvantitativa termer beskriva det samlade informationsflödet, d.v.s det kvantitativa innehållet i det underlag som nyttjas vid viktiga beslut i ett luftförsvarssystem på nationell nivå

Den störinsats/vilseledning som optimerats på alla dessa punkter har optimala möjligheter att lyckas. Med hjälp av den ovan angivna formalismen (Shannons informationsbegrepp, CRB-gränsen, detekteringsteori och estimeringsteori i Bayes version) kan ett optimalt utfört STRIL-system ställas mot en optimalt utförd telekriginsats. Följderna av avvikelser från det optimala på någondera sidan kan då också värderas i kvantitativa termer.

Att peka på principiella (nya) metoder för detta har varit en viktig målsättning med den nu pågående studien in projektet.

Notera slutligen att på grund av generaliteten i de förda resonemangen och de använda resultaten från (den tekniska) informationsteorien, kan dessa slutsatser generaliseras dels till kommunikationsnät i allmänhet, och till ett nätverksbaserat försvar i synnerhet.

4 Arbetsinriktning 2: metoder för att analysera nätverk och informationsflöden

Utöver det teoretiska arbetet genomfördes även praktiska moment där en stridsledningscentral studerades. Objektet studerades för att se hur en lägesbild byggs upp samt för att omvandla de teoretiska informationsflödesteorierna till en modell.

4.1 Studieobjekt StriC

Som studieobjekt har projektet valt StriC vid F20, Uppsala. StriC har ett flygledningssystem som beaktar samtliga enheter och moment i beslutsprocessen från att en flygande plattform detekteras till beslut tas om åtgärd. StriC arbetar på en taktisk/operativ nivå. StriC har en viktig funktion inom STRIL (stridsledning) som är en del i FV 2000 (flygvapnet). Vid StriC sammanställs och tolkas all omvärldsinformation som kommer in via sensorsystemen (framförallt radarinformation). Hela FV 2000 är nätverksbaserat och har många av de egenskaper som ett nätverksbaserat försvar torde eftersträva.

4.2 StriC-övning

Projektet deltog vid en StriC-övning i februari 2004 där ett antal flygledningsscenarier genomfördes. Syftet var att samla in subjektiva data från operatörerna för att i ett senare skede värdera vilken effekt som kan åstadkommas på operativ nivå med olika typer av telekrigsaktioner. Det genomfördes dock ingen systematisk variation av betingelserna, som till exempel med och utan telekrig.

Mätningarna genomfördes under ett ordinarie övningstillfälle för ett Stril-förband. Övningspassen bestod huvudsakligen av civila scenarier och varade ungefär två timmar. Övningsdeltagarna bestod av ordinarie personal från Stril-förbandet.

Data samlades i huvudsak in med hjälp av en enkät som efter genomfört pass delades ut till samtliga övningsdeltagare. Dessutom observerades gruppen under pågående arbete, framförallt i syfte att identifiera kommunikationsvägarna inom förbandet.

4.2.1 Resultat

Genom övningen skapades en insikt om hur StriC bygger upp en luftlägesbild. Därutöver identifierades StriC:s organisationsstruktur samt det logiska flödet inom arbetsprocessen.

4.2.2 Hur en luftlägesbild byggs upp

Strils luftlägesbild blir i princip aldrig klar, utan är under ständig förändring. Med dagens moderna radarsystem sker i regel all måluppträckt automatiskt. Systemens känslighet och grad av autonomi kan dock ställas in av operatörerna.

Systemet läger ut symboler på misstänkta mål och om systemet inte kan identifiera dem genom flygplanens transpondrar, markeras dessa som oidentifierade mål. Det är framförallt de oidentifierade målen samt de identifierade mål som avviker från den angivna rutten som är intressanta för luftbevakningen.

Luftbevakningsgruppen är först i informationskedjan och tar emot den fusionerade informationen från radarsensorena. Som en följd är det luftbevakningsgruppen som blir mest utsatt för telekriginsatser. Deras uppgift är att ta fram en luftlägesbild där alla verkliga mål följs och identifieras så snabbt som möjligt. Det övergripande ansvaret för gruppens arbete har Lbevled (luftbevakningsledaren). Lbevled övervakar hur luftlägesbilden utvecklas och

bedömer om några ändrade direktiv till gruppmedlemmarna behöver ges. Det kan exempelvis innebära order om att specifika områden övervakas noggrannare. Lbevled kommunicerar med samtliga gruppmedlemmar och påverkar hur FSR och stationära radarstationer utnyttjas.

Därutöver sker ett samarbete med JAL (jaktledare), som i fred är ansvarig för insatsberedskapen. JAL fattar alla beslut om insatts mot upptäckta hot. I krig sköts denna uppgift av Lufled (luftförsvarsledaren) som sitter på FTK A3.

Utöver den övergripande uppgiften att skapa en luftlägesbild delas luftbevakningsgruppens verksamhet in i tre funktioner:

- *målupptäckt och följning*, som genomförs av Måled, Bimåled och Målobsar
- *målidentifiering*, som Iled ansvarar för,
- *styrning av FSR* (flygande spaningsradar).

Målupptäckt och följning genomförs av Måled (målföljningsledaren) och Bimåled (biträdande målföljningsledaren). De ansvarar för var sin del av gruppens övervakningsområde. Till sin hjälp hade de en eller flera Målobs (målobservatörer). Arbetsfördelningen mellan funktionerna är väldigt flexibel och vid behov avlöser eller stöttar målobservatörerna Måled eller Bimåled.

Måled, Bimåled och Målobs hade under övningen i stort sett samma uppgifter. Målobs tilldelades i regel ett mindre område, där det var stor fientlig flygaktivitet med många nya mål. Arbetsuppgiften innebar att kontrollera alla oidentifierade mål (rosa symboler) som det automatiserade systemet av radarsensorer hade upptäckt. En viktig skillnad i befogenhet är att Målobs inte har rättigheter att tömma PPI:t på symboler/företag.

Systemet grundar sig på MRT (multi radar tracking) och visar målspår av tre typer beroende på varifrån de härrör. Målspåren kan vara interna, d.v.s. de härrör från de stationära radarstationerna (betecknas med I-nr), från FSR (8-nr) eller från JAS (J-nr).

Luftbevakningsgruppen kontrollerar inkommande måldata, framförallt med avseende på höjd, fart och ett kvalitetsmått. Dessutom iakttas hur målspåret ser ut. De ser om målet hela tiden uppträder på samma ställe eller om det förflyttar sig på ett flygplansliknande sätt. Om kvalitetsmåttet är högt och fart och höjd ligger inom vissa gränser så klassas målet som ett relevant mål och Målobs lägger ut en symbol med en fartvektor  över målet. Det innebär att det markeras som ett så kallat systemföretag, det vill säga ett mål som ännu inte är identifierat. Dessa symboler blir omedelbart tillgängliga för alla som har tillgång till luftlägesbilden.

Måled och Bimåled kommunicerar relativt mycket med Lbevled och med målobservatörerna eftersom de delvis har överlappande områden och stöttar varandra vid behov. Det förekommer även att de har kontakt med CFSL (chef flygstridsledning). Målobservatörerna har liknade kommunikationsmönster och kontaktytor men det sker i mindre omfattning då deras bevakningsområden är mindre.

Iled (identifieringsledaren) ansvarar för målidentifieringen och hanterar alla målföljda företag som inte automatiskt identifierar sig med hjälp av transponder. Genom att ta kontakt med luftfartsverket, flygplatser, FRA m.fl. så försöker man att identifiera målet. Om det inte lyckas skickas en beredskapsrote för att visuellt identifiera målet. Mål som identifieras som falska tas bort. Iledaren är kanske den som kommunicerar med flest funktioner både inom och utom

luftbevakningsenheten. Iled kommunicerar relativt mycket med Lbevled men inte alls med CFSL.

Den tredje funktionen styrning av FSR skiljer sig en del från de övriga. Den flygande spaningsradarn är en mycket effektiv sensor som hela tiden förflyttar sig. Det behövs därför en särskild operatör som hela tiden övervakar att denna resurs utnyttjas effektivt.

4.2.3 Resultat från enkätsvaren

Enkätsvaren bekräftar den befintliga rollstrukturen. Organisationen visade sig vara flexibel genom att bemanningen i de olika funktionerna kan anpassas utifrån uppgiften och vid behov kan bevakningen av ett visst område tillfälligt förstärkas. Det är dock inte ekvivalent med att rollerna eller kompetensen inom gruppen är identiska och att gruppen därmed kan betraktas som en enhet.

De ledande befattningarna Lbevled och Bilbevled (biträdande luftbevakningsledaren) har klart skilda arbetsuppgifter även om de övervakar resultatet av den övriga gruppens arbete. Iled och FSR-operatören kan vid ett ytligt betraktande se ut att ha ungefär samma roll som Måled och Målobs, men det är stora skillnader. Detta innebär att svaren på t.ex. frågan ”Hur svårt var passet” grundar sig på olika arbetsuppgifter och därför inte är direkt jämförbara.

Ileds roll verkar vara svårare än övriga att snabbt stödja. Iled är ofta ensam om sin uppgift. Om det skulle ske en telekrigsinsatts som innebär att många falska mål genereras, så är det framförallt Iled som överbelastas. Härigenom ökar givetvis risken för att farliga mål inte identifieras i tid. Ett exempel från övningen som pekar på denna risk är att vid ett tillfälle hann inte Iled med att lösa sin uppgift utan tvingades att rensa bort samtliga oidentifierade mål för att kunna hantera situationen.

De flesta målen rör sig i ett förutbestämt mönster vilket gör det möjligt att hålla reda på det stora antalet symboler och tillräckligt snabbt upptäcka nya mönster. Flygtrafiken är strängt reglerad och det finns bara ett begränsat antal flygkorridorer som det reguljära flyget måste hålla sig till. När man väl har lärt sig detta mönster är det relativt lätt att upptäcka mål som avviker från detta mönster.

Enkätresultatet pekar på att operatörernas förmåga inte på allvar sattes på prov. Uppgifterna under övningen bedömdes som medelsvåra medan den egna arbetsbelastningen uppskattade som låg, samtidigt som situationsmedvetandet var högt.

4.3 Modellanpassning av informationsflödesteorierna

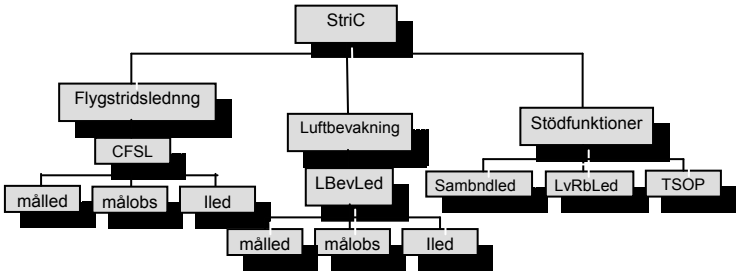
Följande avsnitt beskriver projektets strävan efter att skapa en modell baserad på teorierna runt informationsflöden. De metoder/verktyg som värderats är bayesianska nätverk och morfologisk analys. Bakgrunden till den praktiska teoriomvandlingen var att projektet OAM (operationsanalytiska metoder) år 2004 skulle utvärdera metoden/verktyget bayesianska nätverk och sökte tillämpningar inom studier och projekt. Därutöver fanns det ett intresse från projektets sida att praktiskt utnyttja verktyg vars ursprung är relaterat till de informationsflödesteorier som hanteras i projektets teoretiska del.

Syftet med modellarbetet var att ta fram en modell som skulle beskriva ett nätverksorienterat system och värdera hur informationsflödet inom systemet påverkas av olika telekrigsaktioner mot olika noder och systemnivåer.

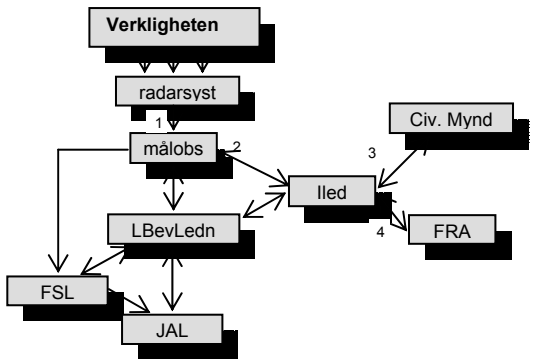
Som studieobjekt utnyttjades flygledningssystemet StriC (kap 4.1).

4.3.1 Arbetsprocess

Nedan beskrivs arbetsprocessen för att ta fram verktygsmodellen:
Vid StriC-övningen (kapitel 4.1) identifierades StriC:s organisationsstruktur (figur 7)och under dess scenarier detekterades informationsflödet (figur 8) mellan de olika arbetsrollerna.



Figur 7: STRIC:s organisationsstruktur



Figur 8: informationsflödesschemat

Därefter genomförde projektet en workshop tillsammans med deltagare från OAM. Under workshopen togs en modell för ett bayesianskt nätverk (figur 9) fram. Arbetet baserades på StriC:s organisationsstruktur och informationsflödesschemat. Modellens huvudfråga är:

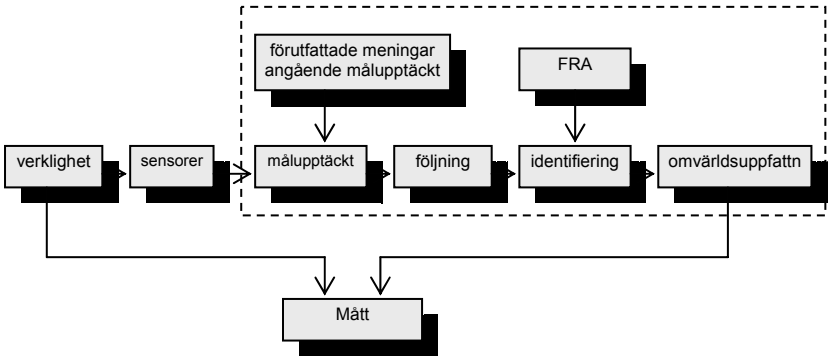
> *”Hur påverkas StriC:s omvärldsuppfattning (genom telekrig) om noderna sätts ur funktion eller tillförs felaktig information?”*

Begreppet omvärldsuppfattning syftar på ”hur StriC precis innan beslut för åtgärder uppfattar situationen inom det för uppgiften relevanta området”.

Modellen beskriver flödet från detektering till skapandet av omvärldsuppfattning. Noden ”verklighet” beskriver hur situationen i området ser ut på riktigt. Noden ”sensorer” beskriver hur sensorerna uppfattar verkligheten. Det streckade området innefattar det område som StriC påverkar och består av den interna kedjan från ”måluppträckt”, ”följning”, ”identifiering” till att StriC skapat sig en ”omvärldsuppfattning” som de grundar sitt beslut på. Noden ”förutfattade meningar…” innefattar den empiriska kunskapen i form av erfarenhet m.m. som

personalen adderar till den visuella informationen vid skapandet av omvärldsuppfattningen. Noden ”FRA” står för den externa kontakt som utnyttjas för att bekräfta identitet eller rutt hos okända objekt.

Modellens slutnod ”omvärldsuppfattning” beskriver sannolikheten att StriC uppfattar objektet, som inget, neutralt eller fientligt.



Figur 9: modell över det tänkta bayesianska nätverket

4.3.2 BN-modellarbete

Projektet har i samarbete med OAM omvandlat nodmodellen till en bayesiansk nätverksmodell. Det innebär att noderna behållits och i viss mån kompletterats. Därutöver har sannolikhetstabeller implementerats i varje nod och därefter värderats.

Projektet valde att börja med en liten modell och successivt utvidga den. Tillvägagångssättet beror till viss del på att ingen i projektet eller OAM hade någon tidigare erfarenhet av bayesianska nätverk. Konsekvensen blev att modellen är av en ganska trubbig och övergripande natur.

Sannolikhetstabellerna i modellen är ifyllda av projektet och OAM utan StriC:s medverkan.

4.3.3 Problematik rörande informationsflöden och telekrigsmodeller

Att utvärdera sårbarheten i ett flygledningssystem är ett komplext problem. Ett flygledningssystem beaktar en delmängd av den ”luftbevakningsprocess” som syftar till att underlätta samverkan mellan olika plattformar för att detektera och avstyra hot. Den sista delen av ”luftbevakningsprocessen” är ”luftstridsduellen”, som syftar till att avstyra företag. Flygledningssystemet är endast ett externt stöd för denna process. Det medför att det är mycket svårt att avgöra i vilken grad den interna processen påverkar utfallet av ett företag som slutar i en luftstridsduell, då den även är beroende av andra faktorer som bl.a farkostens prestanda och pilotens kompetens. Projektet försöker undvika problemet genom att enbart utvärdera den interna flygledningsprocessen. Det innebär att resultatet inte blir ett ”fysiskt utfall” som ”nedskjuten plattform” utan att ”mjukare” svar söks.

Dagens teknik möjliggör telekrigsaktioner som tidigare var mycket svåra att genomföra. När det tidigare endast gick att utnyttja brusstörning finns det idag möjligheter att vilseleda. Det innebär att telekrigsaktionen strävar efter att agera mot en högre nivå än den tekniska sensornivån, d.v.s. den taktiska operatörsnivån. Följden för modellen blir att den skall sträva efter att förutse hur en operatör agerar under hela processen, om han blir vilseledd och i så fall

hur länge. Bortsett från det faktum att modellen därmed hanterar mänskligt beteende har endast ett fåtal experiment/övningar bedrivits där operatörer blir utsatta för denna typ av telekrigsföring (StriC aldrig). Det medför att denna ”konsekvenskunskap” är mycket svårtillgänglig. För att undvika problemet minimeras operatörsprocessen i modellen, det vill säga den del där mänskligt beteende hanteras. Samtidigt är det viktigt att beakta att den bayesianska modellen genom denna begränsning endast kan bli en indikator för sårbarheter/kedjeeffekter.

4.3.4 Resultat

Nedan beskrivs uppnått resultat utifrån perspektiven hur väl det går att utvärdera studieobjektet StriC samt utvärdering av det bayesianska verktyget GeNIe.

StriC

Det är inte möjligt att utifrån modellen dra några slutsatser av större värde angående informationsflödet i ett nätverksbaserat försvar. Modellens karaktär är idag för generell samtidigt som värdena i sannolikhetstabellerna är ifyllda av projektet och inte av experter inom området vilket gör dem mindre pålitliga.

Modellen kan identifiera sambandskedjor mellan telekrigsåtgärder mot en eller flera noder, men modellen är inte tillräckligt tillförlitlig för att besvara i vilken grad noderna påverkas.

Orsak

Att modellen inte blivit mer konkret och användbar beror på en mängd olika faktorer. Den främsta orsaken är att modellarbetet inte är färdigt. Hade tidsutrymmet funnits hade följande parametrar åtgärdats i möjligaste mån;

- *bristande empiri rörande telekrig/vilseledningsaktioner*
- *arbetsprocessen/metodverktyg för strukturering*
- *verktygets begränsningar.*

För att modellen skall bli mer konkret måste den utvidgas med fler noder kompletterat med en högre detaljnivå hos framförallt de tidiga noderna (”aktiva plan”, ”radarklotter”, ”tk mot radar”, ”måluppträckt följning”). Genom att öka detaljnivån skulle de möjliga tillstånden konkretiseras mer. Det skulle innebära att det därmed blir lättare att bedöma sannolikheten hos varje nods tillstånd.

För att gå vidare med modellen krävs tillgång till experter som kan göra expertmässiga sannolikhetsbedömningar. Det innebär att StriC-personal behöver bedöma sannolikhetsutfallen. Eftersom endast ett fåtal experiment/övningar bedrivits där operatörer blir utsatta för denna typ av telekrigsföring (StriC aldrig) saknas det empiriska underlaget för sannolikhets- och konsekvensbedömningar av telekrigsaktiviteter. Det medför att modellen antagligen inte kan bli så mycket mer tillförlitlig förrän empiriskt underlag finns.

Ett flygledningssystem bygger i hög utsträckning på ett interagerande mellan olika funktioner, som kontinuerligt ger varandra upplysningar allt eftersom deras omvärldsuppfattning förändras/förfinas. Bayesianska nätverk baseras på riktade länkar vilket medför att verktyget inte stödjer loopar. En annan viktig parameter som bayesianska nätverk inte stödjer och som måste beaktas indirekt är tidsaspekten. Ett flygledningsscenario är tidskritiskt. Det räcker inte att StriC:s omvärldsuppfattning överensstämmer exakt med verkligheten, omvärldsuppfattningen måste även bildats inom ett tidskritiskt skede.

Uppbyggnaden av modellen genomfördes genom en workshop där ”gula lappar”-metoden utnyttjades för att strukturera problemet. Därefter har modellen förändrats under en mängd iterationer. Som processen nu har sett ut har modellen tvingats att modifieras ett stort antal gånger beroende på att vi/modellen inte beaktat vissa viktiga parametrar. Frågan är om ”gula lappar”-metoden är tillräcklig som struktureringsmetod för så pass komplexa problem som telekrigsfrågor och informationsflöden. Oavsett metodval för nodstrukturering är det viktigt att systemexperter är med och deltar i ett tidigt skede.

Bayesianska nätverk och GeNIe

Arbetet har medfört att kunskapen om bayesianska nätverk och specifikt verktyget GeNIe 2.0 [11] byggts upp. Kunskapen består främst i hur verktyget kan utnyttjas, vilka styrkor och begränsningar det har.

Det är svårt att göra en ordentlig utvärdering av bayesianska nätverk och GeNIe. För en grundlig utvärdering krävs det att verktyget prövas utförligare. Det är dock tydligt att bayesianska nätverk är ett lättbegripligt och visuellt verktyg, som tydligt kan påvisa beroendeförhållanden mellan olika noder även i en längre kedja. Det har antagligen även vissa pedagogiska värden.

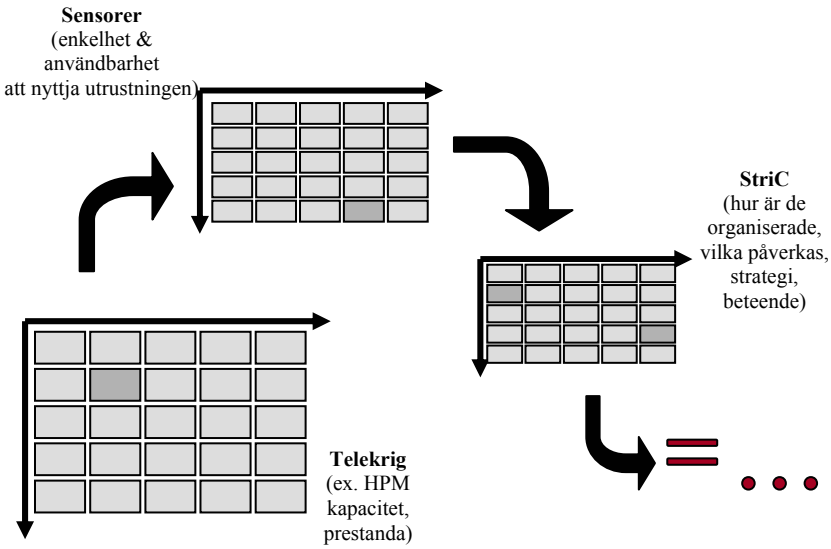
Bayesianska nätverk ämnar sig bäst åt problem där noderna är av statisk natur. Det kan exempelvis vara mycket litet och svara på tämligen enkla frågor som det är lätta få en överblick över. En försvarsmaktstillämpning vore enkla frågeställningar för spelverksamhet då verktyget är visuellt och enkelt skulle kunna generera värden på specifika frågor.

En tillämpning utanför den militära sfären vore till exempel försäkringsbedömningar. En sådan värdering kräver ett mycket större nätverk baserat på expertkunskap inom en mängd områden. Nätverken är så stort att ingen kan ha en övergripande syn men genom expertbedömningarna genereras intressanta svar som kanske inte varit gripbara annars.

4.4 Morfologisk analys

Projektet genomförde även morfologisk analys (kapitel 2.6). Den morfologiska analysen hade två syften. Huvudsyftet var att utvärdera om bayesianska nätverk kan utnyttjas kombinatoriskt med bayesianska nätverk. Morfologisk analys skulle i sådana fall utnyttjas för att generera en stabil nodstruktur som ingångsvärden till den bayesianska nätverksmodellen. Tidsparametern medförde att detta syfte fick bortprioriteras. Det andra syftet var att allmänt utvärdera huruvida morfologisk analys är en lämplig metod i ett initialt skede för att identifiera och strukturera noder samt beroendeförhållanden rörande nätverksfrågor.

Projektet bedrev tre morfologiska analyser, två förberedande morfologiska analyser internt på FOI och en tredje med experter från StriC. Vid de två första skapades ett telekrigsfält samt ett utkast till en struktur över StriC. Målet var att identifiera och strukturera StriC:s externa som interna kontaktytor och deras beroendeförhållanden. Därefter skulle konsekvensen av olika typer av telekrigsaktioner diskuteras utifrån de morfologiska fälten.



Figur 10: morfologisk process

4.4.1 Resultat

StriC och morfologisk analys

Morfologisk analys är en krävande process och skall utföras under åtminstone två dagar för att uppnå ett gott resultat. StriC kunde endast delta en dag vilket gjorde att värderingen med StriC var utsatt för tidspress. Därför hann inte metoden förklaras ordentligt för deltagarna vilket skapade orosmoment och osäkerhet under arbetets gång. Dessutom var telekrigsstrukturen som tidigare tagits fram inte riktigt applicerbar mot StriC (den var för generell). Det medförde att den inte kunde användas ordentligt.

Under dagen skapades en struktur över StriC och beroendeförhållandet mellan noderna kunde dokumenteras. Däremot var denna process onödigt långsam. Det tog mycket lång tid att fylla i dessa kolumner trots att gruppen som sådan var enhällig och insatt i hur strukturen skulle vara. Det gav ett långsamt och klumpigt intryck.

Morfologisk analys är ett kraftfullt struktureringsverktyg i många fall. Just rörande nätverkstrukturer är det inte helt lyckat. Antagligen beror det på att den låga tekniska nivån som stundtals hanterades kräver en för hög detaljnivå. Detta problem åskådliggjordes tydligast när det morfologisk StriC-fältet inte tillät att specifika säkerhetslösningar identifierades för de olika noderna utan det fick ligga på en generell nivå för hela kolumnen. Det gick inte att dedicera säkerhetsdetaljer just till en specifik nod vilket gjorde att strukturen blir otydligare.

Metodikutveckling bayes <-> morfning

Delen han inte genomföras på grund av tidsbrist. Utifrån en snabb jämförelse av de morfologiska fälten och det befintliga bayesianska nätverket över StriC är dock bedömningen att morfologisk analys skapar ett gott underlag till det bayesianska nätverket.

5 Slutsatser

Om störinsats/vilseledning optimerats på alla punkter efter den teoribildning som beskrivits har den optimala möjligheter att lyckas. Med hjälp av den angivna formalismen (Shannon's informationsbegrepp, CRB-gränsen, detekteringsteori och estimeringsteori i Bayes version) kan ett optimalt utfört STRIL-system ställas mot en optimalt utförd telekriginsats. Följderna av avvikelser från det optimal på någondera sidan kan då också värderas i kvantitativa termer.

Att peka på principiella (nya) metoder för detta har varit en viktig målsättning med den nu pågående studien in projektet. Notera slutligen att på grund av generaliteten i de förda resonemangen och de använda resultaten från (den tekniska) informationsteorin, kan dessa slutsatser generaliseras dels till kommunikationsnät i allmänhet, och till ett nätverksbaserat försvar i synnerhet.

Att skapa en modell som hanterar informationsflödet i ett nätverksbaserat försvar utifrån teoribildningen är idag svårt. Det beror främst på att de empiriska kunskaperna rörande följder av vilseledningsattacker är bristfalliga samt att de bayesianska nätverken endast hanterar riktade förhållanden och inte interaktioner.

6 Förslag till fortsatt arbete 2005

Det synes vara av stor vikt att gå vidare med att konkretisera modellerna och de diskuterade analysmetoderna till ett relevant praktiskt fall. Syftet med detta fortsatta arbete bör vara att vidareutveckla modeller och analysmetoder så att de går att tillämpa på hela, eller delmängder av, det kommande nätverksbaserade försvaret. Det nu pågående NBF-arbetet synes vara i stort behov av kvantifierbara analysmetoder, inte minst vad gäller telekrigparametern.

Det kommande året bör därför användas till att utveckla, konkretisera, och tillämpa kvantifierbara analysmetoder enligt dessa tankegångar på någon representativ delmängd av ett kommande nätverksbaserat försvar. Förslaget är att utnyttja Flygvapnets STRIL -resurs och de inbyggda utbildnings- resp. programmeringsmöjligheter som där finns. Med dessa resurser kan inflödet av data till en representativ beslutscentral av avsevärd komplexitet styras, manipuleras och modifieras för att efterlikna telekriginsatser riktade mot beslutsfunktionen ifråga. En sådan *växelverkan* mellan teori- och metodutveckling å den ena sidan, och simulerade försök under kontrollerade förhållanden å den andra, synes mest fruktbar och bör vara det bästa sättet att gå vidare.

Beroende på resultaten från sådana simulerade försök bör nästa steg vara att vidareutveckla och anpassa den skisserade värderingsmetodiken till övrigt näraliggande arbete inom NBF-området. En långsiktig målsättning med TK-NBF -projektet vid FOI arbetet bör vara att på ett kvantitativt sätt så småningom kunna in foga *telekrigparametern* i de kommande etapp-rapporteringarna i det övergripande NBF-arbetet (Demo 05, o.s.v.).

Nätverksprincipen har redan prövats inom flera vapensystem som kräver snabba och säkra beslut. Luftvärn och artilleri behöver t ex flera olika sensorer för att täcka in ett bevakningsområde. Traditionella spaningssystem för ledning av jaktflyg har också nätverkstruktur.

Det svenska Stril-systemet är väl utbyggt och har en lång tradition med väl utbildad personal. Det har genomförts rätt få studier som beskriver inverkan av elektronisk störning. Det rör sig då främst om ren brusstörning mot enstaka radarsensorer. Modern elektronik bjuder helt nya möjligheter till störning och vilseledning och det är det viktigt att studera hur befintliga nätverk som Stril-systemet påverkas av modernt telekrig.

7 Referenslista

[1] *”Värdering av telekrig i nätverksbaserat försvar. Verksamhet och metodutveckling under 2003”* Hyberg, P. FOI---1079—SE, 2003

[2] *"Informationshantering i sensorbaserade luftförsvarssystem”*
Hyberg, P. FOI-R—0564—SE, september 2002

[3] *”Informationsflödet i nätverksbaserat försvar”*
Falk, L., FOI-R—0658—SE, november 2002

[4] *”Inte bara Internet”*
Carling C. och Carlsen H., Framsyn nr 4, 2003.

[5] *“Scale-free networks”*
Barabasi A.-L. and Bonabeau E., Scientific American, pp. 50-59, May 2003

[6] *”Telekrig och information i nätverk”*
Falk L. och Hyberg P. FOI Memo 03-2283, oktober 2003

[7] *“Probability and information theory with applications to radar*”
Woodward P.M., Pergamon Press, London 1953

[8] *“Probability theory: The logic of science”*
Jaynes E. T., Cambridge University Press, Cambridge 2003

[9] *"Kvantitativa beslut i nätverksbaserat försvar”,*
Falk L. FOI-R—1390--SE, december 2004.

[10] *”Omvärldsuppfattning i sensorbaserade luftförsvarssystem”,*
Hyberg P. FOI-R—1392--SE, November 2004.

[11] Blixt J, Jansson B, Mossberg K. FOI-R--1411—SE, 2004

[12] *"Psychology",*
McKeachie, Doyle, Moffet, Addison-Wesley 1976, ISBN 0-201-04607-5

[13] *"Social Psychology and Contemporary Society",*
Edward E. Sampson, Wiley 1971, ISBN 0-471-75117-0

[14] *"Perception- Nogle synpunkter",*
Jörgen Pauli Jensen, Jan Rattleff, Munksgaard 1976, ISBN 87-16-00732-8

[15] *“Morfologisk analys för studien Luftburen förmåga”,*
Kaunitz C., Stenström M. FOI-R—0686—SE, december 2002