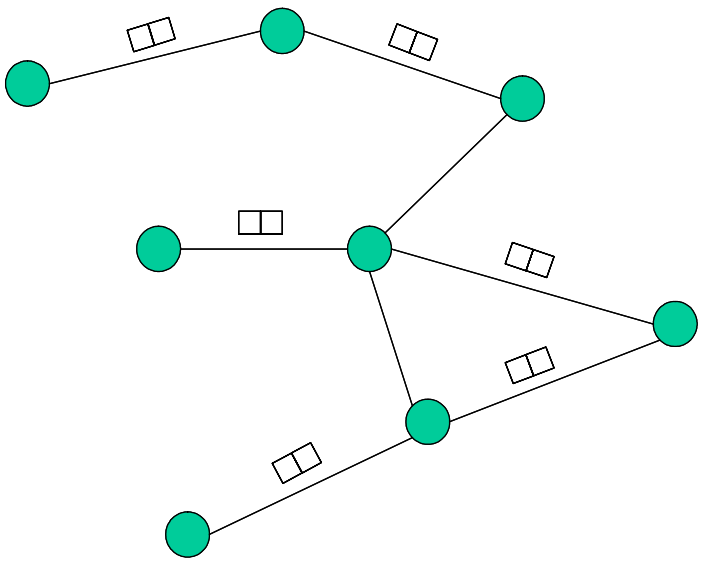
FOI-R--1390--SE
November 2004

Underlagsrapport

Kvantitativa beslut i nätverksbaserat försvar

Lars Falk



Försvarsanalys
172 90 Stockholm

TOTALFÖRSVARETS FORSKNINGSINSTITUT
Försvarsanalys
172 90 Stockholm

FOI-R--1390--SE
November 2004

Underlagsrapport

Kvantitativa beslut i nätverksbaserat försvar

Lars Falk

Utgivare Totalförsvarets Forskningsinstitut - FOI Försvarsanalys 172 90 Stockholm	**Rapportnummer, ISRN** FOI-R--1390--SE	**Klassificering** Underlagsrapport
	Forskningsområde 6. Telekrig och vilseledning	
	Månad, år November 2004	**Projektnummer** E 1421
	Verksamhetsgren 5. Uppdragsfinansierad verksamhet	
	Delområde 61 Telekrigföring med EM-vapen och skydd	
Författare/redaktör Lars Falk	**Projektledare** Roland Heickerö	
	Godkänd av	
	Uppdragsgivare/kundbeteckning	
	Tekniskt och/eller vetenskapligt ansvarig	

Rapportens titel

Kvantitativa beslut i nätverksbaserat försvar

Sammanfattning (högst 200 ord)

Funktion och tålighet hos militära ledningssystem beskrivs genom att studera informationsflödet i ett nätverk. En analys från sensorer till beslutsfattare kräver detaljerad kunskap om osäkerheterna i systemet men leder också till optimala beslut. Metoden kan användas för att beskriva nätverkens prestanda vid telekrig och andra former av bekämpning samt för att dra slutsatser om stabiliteten hos olika nätverksstrukturer. En viktig slutsats är att en sannolikhetsbeskrivning ofta måste omfatta såväl sensorer som observatörer. Analysen visar att tvetydigheter är ett problem även i ett system av sensorer och att vilseledning är en effektiv metod för bekämpning av nätverk.

Nyckelord

telekrig, sensorsystem, störning, information, informationsflöde, tvetydighet

Övriga bibliografiska uppgifter	**Språk** Svenska
ISSN 1650-1942	**Antal sidor:** 33 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--1390--SE	Base type report
	Programme Areas 6. Electronic Warfare and deceptive measures	
	Month year November 2004	**Project no.** E 1421
	General Research Areas 5. Commissioned Research	
	Subcategories 61 Electronic Warfare including Electromagnetic Weapons and Protection	
Author/s (editor/s) Lars Falk	**Project manager** Roland Heickerö	
	Approved by	
	Sponsoring agency	
	Scientifically and technically responsible	

Report title (In translation)
Quantitative decisions in a network of sensors

Abstract (not more than 200 words)

The performance and robustness of military command systems have been investigated by studying the information flow in a network of sensors. This kind of analysis extending from sensors to decision makers requires a detailed knowledge of uncertainties in the system but can lead to optimal decisions. The method described can be used to analyse the performance of sensor networks affected by electronic warfare and other forms of attack. One can also draw conclusions concerning the stability of different network structures. The main conclusion is that a description in terms of proability in general must include both sensors and operators. The analysis reveals that ambiguities remain a problem in a network of radar sensors and that deception is an effective method of attacking sensor networks.

Keywords
electronic warfare, sensor system, jamming, information, information flow, ambiguity

Further bibliographic information	**Language** Swedish
ISSN 1650-1942	**Pages** 33 p.
	Price acc. to pricelist

1. Inledning

Militära ledningssystem är konstruerade för att snabbt komma till beslut baserade på all tillgänglig information. Inför viktiga beslut behöver man uppskatta riskerna och minska osäkerheten med hjälp av information från omvärlden. Modern kommunikationsteknik gör det möjligt att bygga upp ett nätverk av sensorer och beslutsfattare som kan lösa sådana frågor på ett effektivt sätt.

All information från sensorer är utsatt för brus och störningar. Inverkan av störningar har studerats för enstaka länkar och i dueller mellan plattformar. Märkligt nog saknas detaljerade studier som behandlar störning av ett nätverk av sensorer, trots att en viktig fördel med nätverksbaserat försvar (NBF) anses vara att ett sådant system är robust mot störning och andra former av bekämpning.

Inom Försvarsmakten existerar många nätverk med beslutsfattare och kommunikationscentra som stöds av fristående sensorer och vapenbärare, t ex Stril och FV 2000. Samtidigt pågår en utveckling mot NBF, som bygger på principen att moderna plattformar kan lösa flera uppgifter och vid behov ersätta varandra. Ett sådant system är flexibelt och uthärdar olika former av bekämpning, t ex telekrig.

Nätverksprincipen har länge använts vid konstruktion av tekniska system, men inom den militära världen var det något av en revolution när motsvarande principer började tillämpas för tjugo år sedan. Termen ”Revolution in Military Affairs” (RMA) har ofta använts för att antyda en snabb förändring i militära synsätt och metoder. Avsikten under senare år har främst varit att lösa upp de hierarkiska systemen, som varit så framgångsrika, och ersätta detaljerade föreskrifter med en organisation där besluten kan fattas snabbt och självständigt på grundval av exakt information.

Ett problem är att människor i nätverk inte kan betraktas som utbytbara komponenter med föreskrivna egenskaper. Det är svårt att analysera nätverk med mänskliga operatörer i kvantitativa termer. I denna rapport behandlas problemet med hjälp av sannolikhetsteori. Fördelen med metoden är att det finns en etablerad teori som ger kvantitativa resultat. Den är främst användbar på nätverk av sensorer, där informationsflödet är en viktig parameter. Besluten är också relativt väldefinierade. Det krävs ytterligare steg för att analytiskt beskriva strid i bebyggelse och liknande konflikter, där informationsflödet är svårt att överblicka.

Analysen har koncentrerats mot nätverk av sensorer, som ofta påstås fungera bättre än traditionella militära system. Ändå saknas det mått på förbättringen. Det existerar inte heller någon vägledning om hur nätverkets struktur bör väljas för att optimera beslut. Utvecklingen går framåt genom att befintliga system utrustas med datorer, kommunikationssystem och navigering med GPS. Denna process leder till snabba förbättringar av befintliga system, men man måste också kunna beräkna hur sådana nätverk fungerar i besvärliga situationer, t ex om de utsätts för telekrig och annan bekämpning.

2. Syfte

Avsikten med denna rapport är att visa att ett nätverk av sensorer kan beskrivas i kvantitativa termer. Formalismen har valts för att kunna beskriva alla tänkbara förbättringar i systemet. Beräkningarna blir visserligen komplicerade, men kan ofta förenklas om man nöjer sig med

att söka optimala resultat. Övre gränser för prestanda är särskilt viktiga när man studerar system som befinner sig under utveckling och ännu inte prövats i praktiken.

Nätverk är robusta därför att noderna kan utföra olika funktioner och skicka data längs skiftande vägar. En egenhet med militära nätverk är att beslut ofta fattas i en enda punkt. En jämförelse mellan olika strukturer kräver ett kvantitativt mått som är användbart även då systemen utsätts för telekrig eller annan bekämpning. Målet med detta arbete är att visa att Shannons mått för information har lämpliga egenskaper för ändamålet och passar in i en beskrivning av beslutsprocessen.

3. Tillämpningar

Nätverksprincipen tillämpas redan inom många vapensystem som kräver snabba och säkra beslut, t ex luftvärn och artilleri. Ofta behöver man använda flera typer av sensorer för att täcka in ett bevakningsområde. Dessa sensorer knyts samman i ett nätverk som centralt bestämmer vilka sensorer som ska prioriteras och vilken förmåga operatörerna bör ha.

Spaningssystem för ledning av jaktflyg har också nätverkstruktur. Syftet är begränsat jämfört med NBF, men ambitionerna har vuxit i takt med att systemen får nya uppgifter. Det svenska Stril-systemet har vuxit fram under lång tid och operatörerna är välutbildade och erfarna. Stril har därför använts som exempel under arbetet och avsikten är att fortsätta undersökningen i experimentell form på Stril.

Spanings- och ledningssystem har funnits länge men bara några få studier beskriver inverkan av elektronisk störning. De flesta scenarier beskriver brusstörning mot enstaka radarsensorer, men modern elektronik bjuder nya möjligheter att störa och vilseleda beslutsfattare. Det är därför angeläget att studera hur ett nätverk av sensorer och beslutsfattare påverkas av modernt telekrig.

En allmän analys ger upplysningar om vilka delar av befintliga nätverk som kan förbättras. Luftvärn, artilleri och stridsledningssystem kan förnyas med enkla medel om man knyter samman vapen- och sensorsystem med datorer och kommunikationslänkar. Sådana uppgraderingar pågår just nu på många håll i världen. Processen kallas ibland NEC (Network Enabling Capability) till skillnad från NBF eller NCW (Network Centric Warfare), som innebär en fullständig förnyelse av systemet. Terminologin varierar mellan något olika länder; termen NCW används genomgående i USA medan NEC gynnas i UK (King 2004).

4. Metod

Syftet med detta arbete är att utveckla en formalism som beskriver nätverk och deras tålighet mot telekrig. Den valda metoden bygger på tidigare studier av möjligheten att modellera informationsflödet i nätverk (Falk 2002, Hyberg 2002, Falk och Hyberg 2003). Avsikten har varit att kvantitativt bestämma hur mycket information som krävs för beslut. Informationsflödet blir ett mått på systemets förmåga som kan användas för att beskriva processen i allmänna termer. Nackdelen är att specifika beräkningar ofta blir komplicerade.

Figur 1.

Nätverk i moderna militära system uppstår ofta genom att sensorer med olika räckvidd och vinkelupplösning kombinerar sin information. Bilden visar spaningsradarn i ett luftvärnssystem och två typer av eldledningsradar som knyts samman med kommunikationslänkar (den lägre antennen på vänster bild) och datorer. (Rysk utrustning på Moscow Air Show 2003).

Kontakt har tagits med olika förband för att undersöka hur analysen kan tillämpas i praktiska studier. Den teori som beskrivs nedan underlättar planeringen av kommande försök och leder till slutsatsen att tekniska sensorer måste jämföras med kunskapen och förmågan hos människor i nätverket. Först då är det möjligt att ange ett optimum för systemets förmåga.

Metoden förutsätter att man kan definiera ett kvantitativt mått på systemets funktion baserat på mängden information. Nodernas och länkarnas egenskaper beskrivs med den information som passerar genom dem. Detta flöde påverkas av nätverkets struktur och uppbyggnad.

En beskrivning av informationsflödet kräver att man kan uppskatta sannolikhetsfördelningen för olika parametrar (Falk 2002, Jaynes 2003). Proceduren är besvärlig men ger i gengäld en uttömmande beskrivning av problemet. För att finna korrekta mått på prestanda behöver man beakta alla osäkerheter som inverkar på besluten. Man måste alltså känna till systemets uppgift och alla faktorer som påverkar förloppet. Detta villkor inte bara objektivt mätbara data, utan också personalens erfarenhet och förmåga med tanke på att beslut ofta är en subjektiv process som omfattar mänsklig kunskap och värdering.

För detta ändamål är det nödvändigt att uttrycka mänsklig kunskap och osäkerhet så att de passar in i sannolikhetsteorin. Inom AI (Artificial Intelligence) har man försökt komma undan med enklare metoder men då uppstår stora problem eftersom metoderna inte blir heltäckande utan får karaktären av recept (Pearl 1997). En bättre teori erbjuder bayesiansk statistik (Jaynes 2003), trots att metoden i princip kräver en fullständig beskrivning av alla parametrar för att kunna tillämpas på praktiska problem.

I många fall är faktorerna okända och svåra att uppskatta. De tekniska parametrarna kan vara oåtkomliga eller svårtolkade för personalen och deras kunskap är svår att uttrycka i formella termer (”tyst kunskap”). På senare år har man ägnat stor uppmärksamhet åt att beskriva mänskligt handlande vid beslut. I enkla situationer ligger det mänskliga handlandet nära teorins optimum, men i komplicerade situationer är människan hjälplös. Den metod som beskrivs här ger en överblick över den information som krävs för att fatta optimala beslut och på sikt automatisera nätverket. Inom sannolikhetsteorin kan man nämligen formulera en allmän princip som gör det möjligt att värdera systemets funktion.

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

Principen är effektiv, fast svår att tillämpa (Woodward 1953, Jaynes 2003). Dess användning kräver i praktiken att objektiva och subjektiva parametrar i systemet kan beskrivas på samma sätt. Först då är det möjligt att ange hur databehandlingen ska se ut för att leda till optimala beslut.

Systemets prestanda är direkt kopplade till informationsläget. Tidigare studier (Falk 2002) har visat att strilsystemet och luftvärnet erbjuder goda möjligheter att pröva denna beskrivning i praktiken. I båda systemen finns välutbildad personal med stor erfarenhet av att tolka information från olika sensorer. Kontakter har tagits med olika förband för att pröva teorins giltighet och undersöka hur den bör tillämpas på praktiska problem.

5. Internationella kontakter

Ett besök i England visade att Dstl i Farnborough redan studerar informationsflöden i nätverk. Ett exempel är studier av informationsflöden i en stab som utförs av James Moffat och Tim Gardiner vid ”Policy and Capability Studies”. Det finns ett gemensamt intresse för att kvantifiera informationsflödet och avläsa de förbättringar som uppnås (Moffat 2003).

Lars Falk gav vid sitt besök på Dstl en beskrivning av svenska erfarenheter i ett seminarium med titeln ”Information Flow in an Air Defence System” (Falk 2004a).

David King vid Dstl i Portsmouth har granskat informationsflödet i en studie av fartygs robotförsvar och uttryckt det i termer hämtade från Shannons teori (King 2004). Detta arbete kan jämföras med en tidigare studie utförd vid FOI av Jan Kjellgren som visade att det behövs överraskande lite information för att styra en robot (Kjellgren 2003).

Lars Falk gav en inbjuden föreläsning om "Information in radar – a tribute to P. M. Woodward” vid den första internationella ”Waveform Diversity and Design Conference” i Edinburgh i november 2004 (Falk 2004b). Gensvaret visade att detta synsätt är aktuellt både inom sensorområdet och kommunikation.

6. Resultat och fortsatt arbete

Den viktigaste slutsatsen av studien är att en fullständig beräkning av prestanda hos ett nätverk av sensorer kräver en sannolikhetsbeskrivning för både sensorer och observatörer. Denna beskrivning gäller även om systemet utsätts för modernt telekrig med skenmål och vilseledning. Förberedelser pågår för att pröva denna formalism på system med nätverksstruktur. För att undvika alltför omfattande mätningar undersöks möjligheten att använda befintliga träningsanläggningar där beslutssituationer och telekrig kan simuleras.

7. Information inför beslut

If a man will begin with certainties, he shall end in doubts; but if he will be content to begin with doubts, he shall end in certainties. – Francis Bacon (1561-1626).

7.1 Bakgrund

Vid studier av sensorsystem kan man utgå från principen att beslut bara blir optimala om all information beaktas under förutsättning att all informationen beskrivs med sannolikhetsteori. Det finns mindre krävande beskrivningar, men där saknas ett kriterium som gör det möjligt att bedöma prestanda. Dempster-Shafer-metoden saknar t ex flexibilitet för att behandla partiell kunskap (Pearl 1997). Man tvingas i stället tillgripa experiment och simuleringar, vilket kan bli mycket dyrt.

Liksom beslut i näringslivet och vardagslivet bygger militära beslut på en total bedömning av kunskap och risker. Skillnaden är att militära beslut ofta har politiska och humanitära konsekvenser som innebär att ansvaret förs högt upp i hierarkin. I en traditionell hierarki fattas avgörande beslut bara på ett ställe, medan kunskapsläget på lokal nivå förblir oklart. Det leder till problem vid beslut eftersom osäkerheten i data är svår att förmedla till högre nivåer där många beslut måste fattas.

Denna filtreringseffekt leder till att osäkerhet ofta silas bort när informationen förs uppåt. Militärhistorien är fylld av katastrofer som bygger på bristfälliga bedömningar. Det är vanligt att man skyller på chefernas inkompetens utan att beakta filtereffekten. Det nätverksbaserade försvaret är tänkt att minimera riskerna för missgrepp genom att fördela data och order över nätverket och på så vis göra utvärderingen snabbare och effektivare.

Clausewitz ansåg osäkerheter vara typiska för krig och införde begreppet ”krigets dimma” som det pris den traditionella militära hierarkin får betala för sitt rigida sätt att sköta underrättelseverksamheten (Clausewitz 1991). Ofta har spaning skett genom strid, men det bör noteras att just preussarna utvecklade en sofistikerad process med övade staber och krav på självständiga initiativ hos officerare som ledde till överlägsen utvärdering av information.

Situationen har förändrats mycket genom införande av sensorer. Numera kan trupprörelser iakttas på stora avstånd, men i gengäld har motståndarna möjlighet att använda störning och vilseledning för att hindra insyn. Sådana metoder har kommit till ökad användning i moderna konflikter, då de inte varit alltför asymmetriska.

Under Falklandskriget 1982, Gulfkriget 1991 och i Kosovo 1999 var alla parter väl medvetna om riskerna med onödig signalering. Det fanns god kunskap om räckvidden hos sensorer och robotar som gav signalspaning och telekrig en viktig roll. Det taktiska spelet kom att påverka strategin. Vapeninsatserna gav mindre effekt än väntat och avgörandet kom långsammare än politikerna krävde både i Kosovo och på Falklandsöarna (S. Woodward 1994; Craig 2000).

”The fog and friction of war” har länge varit ett vedertaget begrepp inom amerikansk doktrin. Informationsteknologin erbjuder nya möjligheter att undanröja denna begränsning, men för att hantera problemet praktiskt krävs en teori som beskriver informationsläget i skilda situationer och gör det möjligt att dra slutsatser om funktionen hos framtida nätverk.

”Revolution in Military Affairs” (RMA) kan betraktas som ett tidigt amerikanskt försök att lyfta dimman från slagfältet och skapa insyn i alla händelser av betydelse. Vilseledning blir en viktig motåtgärd för motståndaren, eftersom han inte behöver röja eget försvar. Metoden kan vara synnerligen effektiv enligt analysen nedan.

7.2 Informationsflöde

Den risk som är förenad med ett beslut kan beräknas med hjälp av sannolikhetsteori om man har en god uppfattning om osäkerheter i sensorerna och hos personalen. Det är möjligt att uppskatta kunskapsläget i en organisation i termer av sannolikhet, eftersom det även här gäller att uppskatta osäkerhet inför bestämda frågor.

Beräkningarna kan bli avskräckande stora, men i princip erbjuder de inga svårigheter. Problemet ligger i att bestämma kopplingen mellan teori och verklighet, särskilt beträffande mänsklig kunskap. Det krävs förståelse för att skapa en modell, men beskrivningen får inte bli så detaljerad att man inför begränsningar som minskar värdet av modellen för allmänna bedömningar.

Metoder som bygger på sannolikhet fungerar ofta bäst när de tillämpas på översiktliga modeller och används för att dra allmänna slutsatser. En detaljerad modell leder till exakta slutsatser i specialfall men kan inte användas för att dra allmänna slutsatser om prestanda.

Sannolikhetsteorin utarbetades med stor framgång på 1700-talet av Bernoulli och Laplace, men deras metoder rönte motstånd så snart de tillämpades på mänskliga omdömen. Numera råder det inga tvivel om teorins riktighet även i det fallet. Jeffreys och Cox visade att sannolikhetsteorin är den enda matematiska teknik som ger optimala resultat vid modellering och prediktering av osäkerhet (Jaynes 2003).

Ett viktigt resultat är att alla slutsatser måste bygga på sannolikheter som beskriver såväl objektiv som subjektiv information om läget. Mätdata från sensorerna måste kompletteras med personalens kunskaper och uppfattningar för att ge en användbar bild av systemet.

Det enda villkoret för att teorin ska gälla är att sannolikheterna kan uttrycks med positiva tal och att slutsatserna är oberoende av i vilken ordning informationen används (Jaynes 2003). Detta villkor är logiskt, men människan har mycket svårt att iaktta just denna regel. Mänskliga beslutsfattare övervärderar i regel den första information som bedöms som relevant för bedömningen (prima facie-bevisning). Ur denna synpunkt är människan ingen perfekt

beslutsfattare. Bristen kan undanröjas med utbildning och träning som i sin tur kan medföra att observatören tenderar att observera vissa fenomen framför andra (Hyberg 2004).

En viktig fråga är om alla egenskaper hos ett nätverk kan beskrivas med sannolikheter. Svaret är jakande så länge systemet är ett nätverk av sensorer för spaning och följning. De hypoteser och frågor som uppkommer kan i princip avgöras med sannolikhetsteori om hypoteserna kan uttryckas med första ordningens logik. Denna beskrivning kan användas på de flesta sensorer. Även operatörernas frågor kan i allmänhet formuleras i sådana termer. Svårigheten ligger snarare i att genomföra beskrivningen i praktiken. Räkningarna blir oerhört komplicerade och förenklingar måste utföras utan att något väsentligt går förlorat. Detta är en besvärlig uppgift och det finns knappast något fall där ett militärt system beskrivits fullt ut med objektiva och subjektiva sannolikheter.

Vanligen nöjer man sig med en deterministisk beskrivning som låter sig överblickas, men tyvärr är en sådan formulering i princip felaktig. Korrekta beslut kräver att alla osäkerheter tas med. Woodward använde för femtio år denna princip sedan för att härleda grundlagarna för radarmätningar (Falk 2004b).

Woodward formulerade principen så att alla steg i signalbehandlingen måste vara omvändbara för att ge optimalt resultat (Woodward 1953). Villkoret innebär att all information som behövs för en korrekt bedömning bevaras i processen. Informationen omformas men kan i princip alltid återvinnas. Detta villkor innebär att man kan tala om ett *informationsflöde* som utbreder sig inom nätverket. De teorier som behandlar nätverk i flödestermer kan alltså tillämpas på detta fall.

Begreppet informationsflöde är abstrakt och hänför sig bara till den information som är nödvändig för att lösa en viss *uppgift*. Sambandet mellan information och uppgift är fundamentalt i den kommande analysen. I våra dagar kan man spara stora mängder data, men i början på 1950-talet var det omöjligt. Först med datorerna kom möjligheten att tillämpa Woodwards principer. Principen om informationens bevarande kan användas för att härleda sannolikhetsteorin och ge den en djupare motivering (Jaynes 2003). Beräkningarna är besvärliga, eftersom man måste spara hela sannolikhetsfördelningen, men behöver sällan utföras i detalj om man nöjer sig med en uppskattning.

7.3 Mänskliga faktorer

Det föregående resonemanget visar att man måste föra in subjektiv sannolikhet i form av mänsklig kunskap och osäkerhet för att få en fullständig beskrivning av nätverk. Människan är dålig på att bedöma sannolikheter och kan på sin höjd ordna risker i stigande följd.

Människan lyckas bäst om de sannolikheter som ska bedömas är få och faller inom ett snävt intervall. I sådana fall kommer människan till snabba fast inte särskilt exakta resultat. I många fall krävs det långvarig träning för att komma till rimliga beslut. Människan ersätts därför alltmer med datorer i komplicerade tillämpningar.

Studier av hasardspel visar att människan genom träning kan öva upp sig i konsten att lösa sannolikhetsproblem, men i praktiken förblir underlägsen maskinerna. Människan är svag när det krävs snabbhet och koncentration. Det är nödvändigt att känna till dessa brister om man ska värdera ett nätverk med mänskliga observatörer och beslutsfattare. Mänskliga

observatörer behövs i systemen för att tillföra särskild kunskap i frågor som är svåra att beskriva. En metod att bedöma förmågan är att fråga ut experter med stor erfarenhet. Frågorna måste vara praktiskt formulerade och referera till konkreta beslut, eftersom personalen ofta har svårt att beskriva sin kunskap i formella termer. Under dessa omständigheter har det visat sig att experter har stor förmåga att finna varierade och okonventionella lösningar på nya problem (Klein 1998). Detta är anledningen till att tränade experter ofta används för att kartlägga möjligheter inför en sannolikhetsberäkning

Maskinerna kan inte överblicka alla situationer och det är svårt att utforma regler som täcker samtliga fall. Erfarenheten visar att förenklade regelverk kan leda till fatala misstag vid identifiering under strid. Misstagen kan reduceras genom att man använder mer information. Nätverk kan fatta goda beslut även i ovanliga situationer om man tillför en liten mängd mänsklig kunskap (Hyberg 2004).

8. Sannolikheter i nätverk

8.1 Subjektiva och objektiva sannolikheter

Sannolikheten för en händelse beskriver vår osäkerhet inför en situation. Att en tärning har sannolikheten 1/6 att ge sex prickar vid ett kast betyder vanligen bara att vi inte granskat tärningen närmare. Vi saknar rimliga skäl för att föredra en sida framför de andra och ger dem av symmetriskäl samma odds. Det är sällan man har tillfälle att undersöka om en tärning verkligen är symmetrisk eller hinner pröva den i ett tillräckligt antal kast.

Sannolikheten är en subjektiv kvantitet, även i många fall där den i princip kan mätas objektivt. Vi är beroende av andras kunskap och värderingar för försök. Det gäller i ännu högre grad i en ledningscentral, där man bara undantagsvis har tid att kontrollera prestanda hos en sensor i detalj. För det mesta är det subjektiva sannolikheter som används för att formulera militära problem, men lyckligtvis följer de samma matematiska beskrivning som objektiva sannolikheter (Jaynes 2003).

Spaning med radarsensorer är ett problem som innehåller både objektiva och subjektiva sannolikheter. Frågan är hur man ska kunna bestämma sannolikheter för de bedömningar människor gör i en ledningscentral. Detaljerade synpunkter ges i en rapport av Per Hyberg (Hyberg 2004). Så länge man sysslar med typiska spaningssituationer är det möjligt att beskriva en operatör i generella termer beroende på utbildningsnivå. Hans kunskap och förmåga beskrivs av svaren på enkla frågor vid spaning mot enstaka mål. Först vid spaning mot många mål och identifiering av enstaka mål uppstår den blandning av objektiva och subjektiva sannolikheter, som är typisk för avancerad analys. För närvarande pågår en snabb utveckling på detta område för att på sikt ersätta människan med datorer (Griffiths 2003)

8.2 Osäkerhet och entropi

Traditionellt betraktas kunskap som en additiv kvantitet. Kunskapen anses ständigt öka och förvaras i växande bibliotek. Detta synsätt har anammats av tekniken. Hartley definierade på 1920-talet information som det antal digitala enheter som krävs för att lagra kunskap i

oförvanskad form. Mängden information svarar då mot längden på det lagrade meddelandet uttryckt i binära tal, d v s information är proportionell mot logaritmen av talet.

Hartley införde på så sätt begreppet *bit*. Informationen är proportionell mot logaritmen av antalet möjliga utfall. Om alla meddelanden är möjliga måste de tillskrivas sannolikheter om man vill lagra dem på ett effektivt sätt. Genom sådana betraktelser knöts begreppen *information* och *sannolikhet* tidigt samman, men information måste betraktas som ett mer fundamentalt begrepp.

Sannolikheter hänför sig till en viss stationär situation eller ett system av händelser, medan information har en bredare innebörd. Det är en kvantitet som skapar klarhet i en osäker situation. Om sannolikheter kan definieras kastar de ljus över begreppet information. Olika alternativ måste klassificeras och om möjligt värderas i termer av osäkerhet. Därefter inför man sannolikheter, som gör det möjligt att jämföra tolkningar och predikteringar kvantitativt.

En tolkning i termer av sannolikheter kräver en avancerad konceptuell analys och löser inte alla frågor. Det är lätt att definiera en kvantitet som mäter skillnaden mellan olika sannolikhetsfördelningar – Kullback-Solomons mått (1950). Problemet är att detta mått inte är något avstånd: man kan inte successivt jämföra olika fördelningar. Sannolikhetsrummet har en komplicerad struktur som speglar nätverkets logik och sensorernas återgivande av verkligheten. Ett avstånd i sannolikhetsrummet motsvarar inte nödvändigtvis avståndet mellan två tolkningar av verkligheten (Kullback 1959). Tvetydligheter är vanliga och ett återkommande problem i sensoranalys som vi ska se.

Shannon visade 1948 hur brus kan elimineras vid kommunikation, men kodningsteoremet kan inte användas på radarsensorer. Radarsignaler kan inte kodas i Shannons mening. Däremot kan man använda Shannons beskrivning av hur mycket information en sensor förmedlar. Måttet ger upplysningar om hur ett nätverk bör disponeras i radarfallet för att ge maximala prestanda (Woodward 1953, Falk 2004b).

Enligt Hartley och Shannon ska måttet på information vara additivt för oberoende källor. Å andra sidan vet vi att för två oberoende händelser kan sannolikheterna multipliceras,

$$p = p_1 p_2$$

Det innebär att informationen i ett enstaka meddelande med sannolikheten p måste vara

$$- \log p.$$

Minustecknet tillkommer därför att sannolikheterna definieras så att de alltid är mindre än 1. Måttet för information blir additivt för observationer av två oberoende händelser,

$$- \log p = - \log p_1 - \log p_2$$

Den digitala revolutionen gjorde det självklart att räkna information i bitar, men kärnan i nätverksproblemet ligger inte i denna observation. Man måste också kunna uppskatta kunskapsläget och beräkna risker med beslut och för det ändamålet behövs andra egenskaper hos information.

Enligt Shannon är information ett mått på de slutsatser man kan dra ur meddelanden behäftade med brus och störning. Problemet är inte att *lagra* information utan att *förmedla och tolka* den i närvaro av störningar. Shannon löste problemet genom att beskriva *bristen på kunskap* i stället för kunskap och införde *entropi* som mått på denna osäkerhet.

Namnet entropi är något olyckligt valt, eftersom Shannons entropi bara i formell mening motsvarar det fysikaliska begreppet entropi. Fysisk entropi är en mätbar kvantitet, medan Shannons entropi borde heta *informationsentropi*. Det är en subjektiv kvantitet som uttrycker osäkerheten i våra bedömningar inom de ramar vi själva valt. Det innebär att måttet är subjektivt, men att vi kan ena oss om en uppfattning som baseras på objektiva mätningar och subjektiva omdömen om de deklareras klart. Proceduren är fullständigt objektiv, trots att sannolikheterna är subjektiva, så länge vi är överens om hur data ska analyseras.

Ett fundamentalt resultat av denna teori är att optimala beslut i medeltal bara kan fattas om all relevant information avvänds på rätt sätt. Det betyder att medelvärdet har en speciell innebörd som är kopplad till begreppet information och sannolikheter. Shannon definierade entropin som medelvärdet av den information som ges av möjliga händelser och meddelanden. Formellt sammanfaller denna definition av entropin, H, med den som används inom statistisk mekanik, eftersom det i båda fallen är frågan om att uttrycka osäkerheten i en beskrivning.

$$H = - \Sigma p_i \ log \, p_i$$

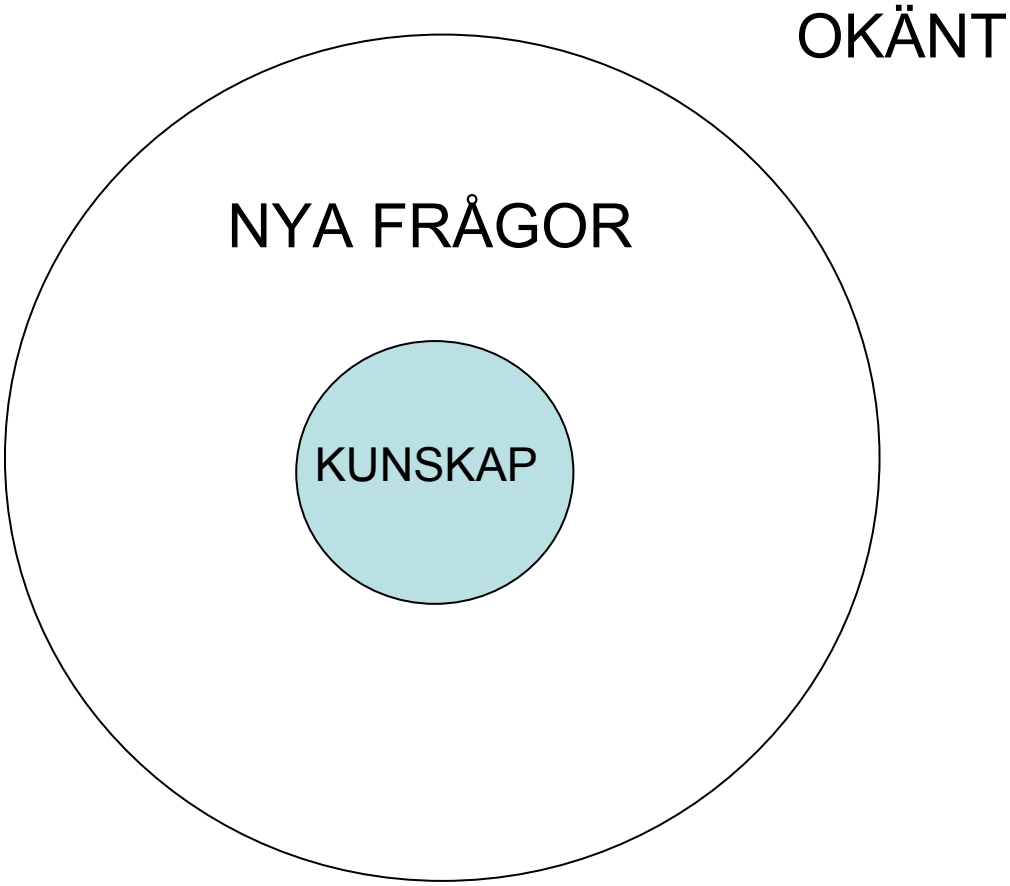
Shannons entropimått anger hur många bitar som i medeltal krävs för att beskriva en situation. Woodward införde motsvarande mått för enstaka händelser, t ex efter en mätning med en sensor. Information skingrar osäkerhet och definieras därför som skillnaden mellan entropi före och efter en mätning. Denna definition är användbar utanför sannolikhetsteorin och ger en åskådlig bild av de problem ett spaningssystem ska kunna lösa.

Figur 2 visar schematisk att det kan finnas situationer där osäkerheten växer snabbare än kunskapen; det inträffar bland annat om mätsystemet inte hinner uppdatera mätningarna tillräckligt ofta och t ex förlorar följning. Bilden understryker att behovet av kunskap måste vägas mot osäkerheten. Det är en väsentlig skillnad mellan att inte kunna mäta det som låter sig mätas och det som är okänt. Ett typiskt exempel är radiovågorna före 1850 – ett verkligt fenomen som ännu låg utanför erfarenheten. Kända och okända osäkerheter påverkar båda beräkningarna, men bedömningarna blir olika – återigen ett exempel på att en beräkning kan innehålla subjektiva element.

Den allmänna slutsatsen blir att det är viktigt att väga kunskap mot osäkerheter i ett spaningssystem. För enstaka sensorer (monostatisk radar) finns ett enkelt samband mellan signalen och mängden information. I sammansatta system blir sambanden snabbt komplicerade. I sådana spaningssituationer är det ofta lika viktigt att ta ställning till vad som saknas (blinda områden) som vad man ser. För enstaka radarstationer är blinda områden lätta att överblicka men i ett nätverk förändras situationen helt.

Det uppkommer dessutom *tvetydigheter* i tolkningen som beror på att en komplicerad verklighet beskrivs med radarns begränsade resurser. Informationsteorin är av stort värde när det gäller att beskriva sådana situationer i allmänna termer. Ofta spiller man krut på att noggrant bestämma parametrar som ligger inom räckhåll för sensorerna och försummar

obekanta eller mer svårbestämda faktorer. Detta problem kan undvikas med en systematisk formalism som beskrivs nedan och även har diskuterats tidigare (Falk och Hyberg, 2003).



Figur 2.
Schematisk beskrivning av förhållandet mellan kunskap och osäkerhet inför beslut. Frågan om uppgiften kan lösas beror på hur kunskapen växer i förhållande till det som återstår att utforska.

8.3 Exempel på osäkerhet

Följande exempel har använts i en tidigare rapport (Falk 2002), men kompletteras här med en utvidgning som visar att sannolikheten är en subjektiv kvantitet, även om situationen verkar vara objektiv.

En person deltar i ett TV-program och får veta att bakom tre stängda dörrar står en lyxbil och två getter (Figur 3). Han får peka ut en dörr, varpå programledaren öppnar en annan dörr och visar att bakom den står en get. Den tävlande får chansen att byta till den tredje dörren eller stå fast vid sitt ursprungliga val.

Figur 3.
Problemet med tre dörrar. Bakom en av dörrarna står en värdefull bil.

Trots sin enkelhet brukar detta problem vålla häftig debatt. Många experter vill inte erkänna att problemet handlar om subjektiva sannolikheten som beror på deltagarens kunskap och bedömningar. Somliga anser att sannolikheten för att hitta bilen inte kan påverkas av en handling som inte direkt berör den dörr bakom vilken bilen står. Så är naturligtvis inte fallet: programledaren ger indirekt information om var bilen står genom att visa var den inte finns. Man kan lätt visa att chansen att vinna bilen fördubblas om man byter dörr, men samma beslut kan utan beräkningar härledas ur den allmänna princip som diskuterades ovan:

Man kan i genomsnitt inte vinna fördelar genom att avstå från tillgänglig information.

Annorlunda uttryckt: Man får aldrig kasta bort information inför ett beslut, innan man förvissat sig om att den är ovidkommande. I problemet med tre dörrar finns det bara ett sätt att utnyttja informationen. Den som håller fast vid sitt val har liksom tidigare chansen 1/3. Den som vill utnyttja den information programledaren ger deltagarna måste alltså eliminera ett alternativ. I det aktuella fallet kan det bara ske genom att byta dörr. Eftersom det är den enda möjligheten att ändra sitt beslut kan man beräkna den återstående sannolikheten till vinst genom att subtrahera det andra alternativet och finner att chansen är 1- 1/3 = 2/3, d v s en fördubbling av sannolikheten.

Liknande fall uppkommer i sensorsystem där man försöker utnyttja sin kunskap. Data från sensorerna måste på rätt sätt kombineras med vad man vet om situationen. Om en av dörrarna öppnas av en slump, t ex genom ett konstruktionsfel, uppstår ett nytt problem, även när det inte står någon bil bakom dörren. Detta är en nämligen helt annan situation, trots att situationerna objektivt sett tycks vara lika (MacKay 2003).

Skillnaden återspeglas i det faktum att sannolikheten att finna bilen bakom de återstående dörrarna blir olika i de två fallen. Uppenbarligen är chansen att vinna en bil i det senare fallet ½, eftersom programledarens kunskap inte påverkar beslutet. Man väljer helt enkelt mellan två likvärdiga alternativ. Liknande fenomen uppstår om någon har anledning att misstro programledaren, som t ex kan fuska för att spara pengar eller öka intresset genom att skapa flera vinnare. Det är vår uppfattning om programledarens avsikter som styr beräkningen, d v s det rör sig om en subjektiv bedömning.

Liknande frågor uppstår i strid, i synnerhet vid avancerat telekrig, eftersom det finns tid för både planering och vilseledning. Man måste i sådana fall avgöra om ett misstänkt mål är äkta eller bara ett skenmål skapat med hjälp av UAV:er eller elektroniska metoder. Sådana beräkningar kan formaliseras i termer av sannolikhet som Bayes visade i mitten på 1700-talet.

8.4 Bayes formel

Bayes studerade hur många gånger man måste kasta ett mynt för att avgöra om det är äkta eller falskt. Liknande frågor uppkommer bland läkare och läkemedelstillverkare, som är intresserade av att göra sina försöksserier så korta som möjligt. Frågan uppkommer också när sensorer ser ett fluktuerande mål i klotter och brus. Hur länge behöver man mäta för att upptäcka ett mål av given storlek i fluktuerande klotter?

(1,1)	(1,2)	(1,3)		
(2,1)		(i,k)		
(3,1)				(m,n)

Figur 4.
Härledning av Bayes' formel: sannolikheter för utfall som beror på två parametrar.

För att härleda Bayes' formel kan man tänka sig sannolikheten som en mängd (1 kg) sand i en sandlåda. Sanden är utspridd i lådan, som är indelad i ett rutnät enligt figuren med *m* rader och *n* kolumner. Uppgiften är att välja mellan alternativ, som i detta fall definieras av två parametrar. Fördelen med Bayes' formel är att den klart skiljer mellan den matematiska beräkningen och den intellektuella uppgiften att definiera lämpliga alternativ. Detta måste ske först och är människans uppgift. I ett nätverk av sensorer har valet vanligen redan gjorts av tillverkaren, men det finns kvar ett val om vilken sensor som ska användas.

Mängden sand (sannolikheten) i varje ruta kan beräknas på två olika sätt: antingen ser man efter hur mycket sand som finns i rad *(i)* och anger hur stor andel som finns i kolumn *(k)* förutsatt att man står i rad *(i)*. Alternativet är att man ser efter hur mycket sand som finns i kolumn *(k)* och anger hur stor andel som finns i rutan med radnummer *(i)* om man står i kolumn *(k)*.

Matematiskt sett är detta en definition av de betingade sannolikheterna $p(i \mid k)$ och $p(k \mid i)$, som kan knytas till varandra genom att mängden sand i varje ruta *(i,k)* (sannolikheten p_{ik}) kan skrivas på två olika sätt.

$$p_{ik} = p(i \mid k)\, p(k) = p(k \mid i)\, p(i).$$

Detta är Bayes' formel under bivillkoret att den totala sannolikheten är 1,

$\Sigma p_{ik} = 1$

Bayes' formel betraktas ofta som en definition av betingad sannolikhet. Om raden *(i)* är opåverkad av kolumnen *(k)* bör tydligen gälla,

$p(i \mid k) = p(i)$

Bayes' formel stämmer med vår uppfattning om sannolikheten för oberoende händelser. Om *(i)* är opåverkad av *(k)* ska inte heller *(k)* vara påverkad av *(i)*. Bayes' formel ger

$p_{ik} = p(i \mid k)\, p(k) = p(k \mid i)\, p(i)$

Faktorn $p(i \mid k) = p(i)$ faller bort och som väntat finner vi

$p(k \mid i) = p(k)$.

Kärnan i all slutledningskonst är att beskriva sambandet mellan olika variabler. I vårt fall väljer vi att jämföra utfallet av olika försök med hypoteser. Bayes formel visar då att trovärdigheten för en hypotes kan studeras på experimentell väg. Sannolikheten blir ett mått på vad vi tror om hypotesen.

Det ansågs länge ovetenskapligt att förknippa hypoteser med ”subjektiva sannolikheter”, men exemplet ovan visar att subjektiva bedömningar ofta kommer med vid beräkning av sannolikheter. Numera accepterar de flesta att mänskliga bedömningar måste bygga på både ”objektiva” och ”subjektiva” omdömen som kommer från sensorer resp. experter. I militära bedömningar ingår dessutom ofta att bedöma motsidans avsikter och förmåga.

Hypoteser och utfall kan behandlas som andra variabler om man låter *(i)* beteckna hypotesen H_i och *(k)* utfallet x_k av ett försök. Bayes' formel ger

$p(H_i \mid x_k)\, p(x_k) = p(x_k \mid H_i)\, p(H_i)$

Formeln ger ett mått på hur mycket sannolikheten av (tron på) en hypotes H_i ändras genom ett mätresultat x_k,

$p(H_i \mid x_k) = p(x_k \mid H_i)\, p(H_i) \,/\, p(x_k)$

Bayes' formel värderar all information lika oavsett i vilken ordning data presenteras. Den skiljer sig i det avseendet från mänskliga bedömare som har en tendens att värdera den första faktor som väcker uppmärksamhet högt. Senare information tolkas lätt i ljuset av denna om man inte genom systematisk träning har lärt sig att övervinna denna bias.

Amerikanska försök visar tydligt denna effekt. Luftvärnspersonal fick fatta beslut om hur man skulle bemöta flygplan som kom nära eller flög in över ett skyddat område. Flygplanen kunde uppträda med eller utan transpondersvar och andra former av identifiering. Personalen använde sig nästan uteslutande av den första indikator de observerade och byggde sina slutsatser på den. Liknande försök har rapporterats i andra beslutssituationer (Sefaty, Entin och Tenney (1989)).

Personal som är beroende av en saklig bedömning kan systematiskt träna sig i att sortera om fakta för att motverka denna effekt. Det är alltså möjligt för människan att genom övning närma sig en objektiv bedömning. Människans andra svaghet är oförmågan att hantera sannolikheter av varierande storleksordningar, vilket lätt får beslutsfattare och operatörer att försumma osannolika händelser. Även denna svaghet kan man i viss mån öva bort genom att jämföra sina beslut med resultat grundade på maximal information.

Människans sätt att bedöma information är en anpassning till en värld, där det gällde att snabbt komma till enkla praktiska beslut. Denna begränsning blir en svaghet i komplicerade system, där förmågan att hantera stora mängder data är avgörande. Människan tenderar att överskatta sin förmåga till intuitiva beslut (Sefaty, Entin och Tenney (1989)). Bäst lyckas experter med stor erfarenhet av systemen, fast även de kan ha svårt att uttrycka sitt kunnande i explicita termer (Klein 1998).

Människans begränsningar hänger samman med att den metodik som beskrivits ovan är svår att använda. Formalismen är enkel så länge sannolikheterna är enstaka tal, p_i, men i allmänhet är de fördelningar över en eller flera parametrar, $p(x_i)$. Det är bara i undantagsfall man kan genomföra en fullständig beräkning, men det är också sällan nödvändigt.

8.5 Information a priori

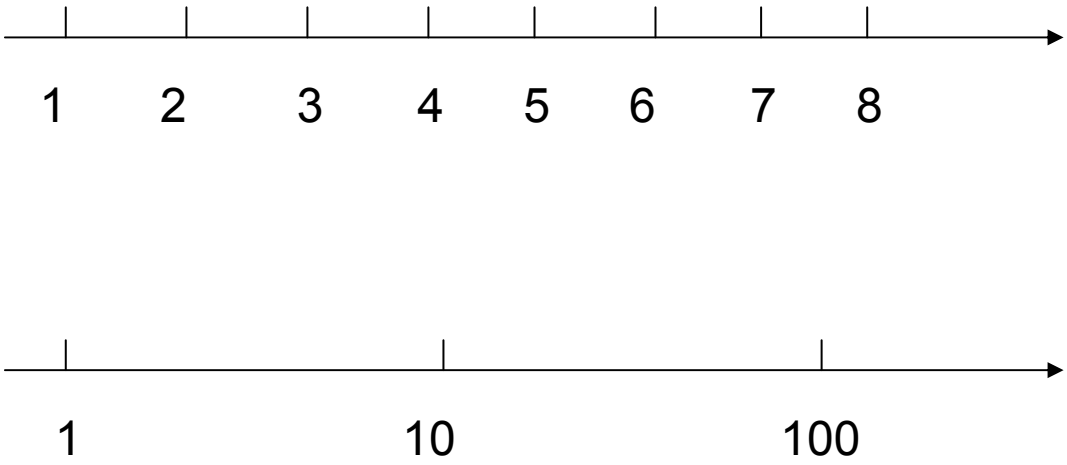
Bayes' formel används för att uppgradera omdömen med hjälp av nya data, men man måste börja någonstans. De ursprungliga osäkerheterna kallas sannolikheter *a priori* (engelskans "priors"), medan de nya osäkerheterna är sannolikheter *a posteriori*.

Valet av ursprungliga sannolikheter vållar sällan problem i radar eller andra militära system. Man använder tidigare erfarenhet om sensorsystemet för att sätta sannolikheter *a priori*. Värdena på sannolikheterna hämtas ur verkligheten och är inte teoretiska konstruktioner. Sannolikheterna *a priori* kan betraktas som resultat av tidigare mätningar som redan använts i Bayes' formel (Jaynes 2003). I praktiken är sannolikheterna *a priori* sällan något problem, eftersom mätdata snabbt korrigerar för dåliga antaganden.

Det är en utbredd missuppfattning att alla möjligheter *a priori* skulle anses vara lika troliga. En sådan åsikt leder till filosofiska problem, eftersom man inte kan veta vilka hypoteser som ska formuleras eller ens hur många de bör vara. Missuppfattningen bygger på ett felaktigt antagande. Man saknar nämligen aldrig kunskap om mätdata i ett system för praktiskt bruk.

Upplösning och maximalt utslag på instrumentet har valts redan vid konstruktionen och alla händelser, även oförutsedda, tolkas inom denna ram. Av detta argument framgår att osäkerheter sällan är lika *a priori*, trots alla påståenden i den riktningen. Det krävs betydligt subtilare resonemang för att korrekt uttrycka brist på kunskap och osäkerhet i en given situation (Jeffreys 1939).

Ett åskådligt exempel är Benfords lag som upptäcktes på 1930-talet. Benford fann att den första siffran i många data ligger nära 1, medan siffran 9 är ovanlig. En liknande observation hade gjorts av den amerikanska astronomen Simon Newcomb, som noterade att observatoriets logaritmtabeller slets olika. De sidor där talet började på 1 var mer nötta än andra.



Figur 5.
Information a priori i godtyckligt valda tal ges av Benfords lag, som säger att kvantiteter med sort ofta beskrivs av en logaritmisk fördelning.

Varken Benford eller Newcomb insåg orsaken till snedfördelningen. Heltalen är skapade för att beskriva addition och är jämnt fördelade på tallinjen. De passar inte för att beskriva kvantiteter med sort, t ex storleken på sjöar, länder och städer, som jämförs genom division.

Sådana tal uttrycks naturligt genom logaritmer, som gör skalan linjär. Tal som börjar med siffran 1 hamnar mellan log 2 - log 1 = 0.3, medan intervallets totala längd är log 10 - log 1 = 1. Sannolikheten att ett tal med sort ska börja med 1 är alltså 30%, medan sannolikheten att talet ska börja med 9 blir mindre än 5%. Effekten är så påtaglig att den kan användas för att avslöja förfalskad bokföring. Den som försöker hitta på ”godtyckliga” siffror måste veta vilken slags data han försöker förfalska. Befolkningen i städer mäts inte i godtyckliga enheter, men siffrorna följer ändå Benfords lag, eftersom de sträcker sig över flera dekader.

Jeffrey visade detta resultat i allmän form genom att notera att alla data med sort måste ha en fördelning som inte beror på enheten. Sannolikheten *p(x)* ska alltså vara proportionell mot

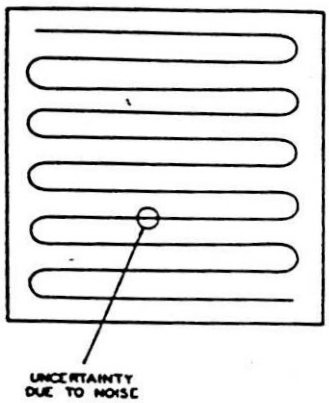
dx/x, vilket ger *p(x) = log(x)* efter integration (Jeffrey 1939). Benfords lag är ett specialfall av Jeffreys fördelning.

En betydligt viktigare fördelning ges av Jaynes' princip för maximal entropi, som används för att finna en opartisk fördelning vid analys av komplicerade system (Jaynes 2003). Ett uppfriskande inslag i denna analys är att man inte slipper kravet att fundera över sin egen kunskap, vilket är ett viktigt krav vid varje bayesiansk beskrivning av en spaningssituationen (Falk och Hyberg 2003). Man måste både veta vad man vet och vad man inte vet.

8.6 Tvetydigheter

Det faktum att Bayes' formel inte beskriver kunskap utan osäkerhet är betydelsefullt vid avancerad tolkning. Tvetydigheter är typiska för alla mätningar med sensorer. Tvetydigheter är välkända för enstaka radarstationer i form av andragångsekon och osäkerheter i avstånd vid höga pulsfrekvenser. I ett nätverk består sensorsystemen av flera sensorer i samverkan. Den extra information som samlas in genom samverkan minskar visserligen osäkerheten (entropin), men vållar ändå problem vid tolkningen.

Sensordata ger en reducerad bild av verkligheten, vilket gör att en radarstation fungerar bäst mot enstaka punktmål. Där finns ett entydigt samband mellan radarsignalen och målets avstånd, fart och riktning, men en så enkel tolkning är bara möjlig om sändning och mottagning sker från samma plats. Om radarn fångar in reflexer från terrängen räcker de uppmätta parametrarna inte till för att beskriva verkligheten och radarklotter uppstår. Klotter är en stokastisk process som skapas genom att signalen inte förmår avbilda verkligheten utan ger en starkt reducerad bild av terrängen. Shannon beskrev processen i följande klassiska bild.



Figur 6.
Effekten av att data reduceras till lägre dimensioner. Data som på ett naturligt sätt beskrivs i högre dimensioner (två i detta fall) kan reduceras till lägre dimensioner, men till priset av att punkter som ligger åtskilda kommer nära varanda och lätt blandas ihop i närvaro av brus. I mer komplicerade fall skär ytorna alltid varandra så att tvetydigheter uppstår (Shannon 1949).

Kompression av data medför stora risker om signalen inte kodas. I radar är detta svårt att göra och reduktion av data ger ofta upphov till tvetydigheter. Detta sätt att tolka tvetydigheter visar hur effektiv informationsteorin är vid analys av sensorsystem. Variation av parametrar och ett nätverk av sensorer kan användas för att skapa klarhet vid tvetydighet, men det fordras noggranna beräkningar för att välja rätt uppsättning parametrar. Med rätt val av sensordata kan man reducera osäkerheten till en nivå där det är möjligt att fatta beslut.

8.7 Uppgift och beslut

Informationsteorin ger en naturlig koppling till sannolikhetsteorin via satsen att man inte kan vinna fördelar genom att avstå från tillgänglig information. Bedömningar och beslut blir först optimala genom en bayesiansk beräkning. Det innebär att nätverkets uppgift vid spaning kan beskrivas på följande sätt.

UPPGIFT	→	BEHOV AV INFORMATION	→	VAL AV SENSORER
↕				↓
BESLUT	←	SANNOLIKHETER	←	MÄTDATA

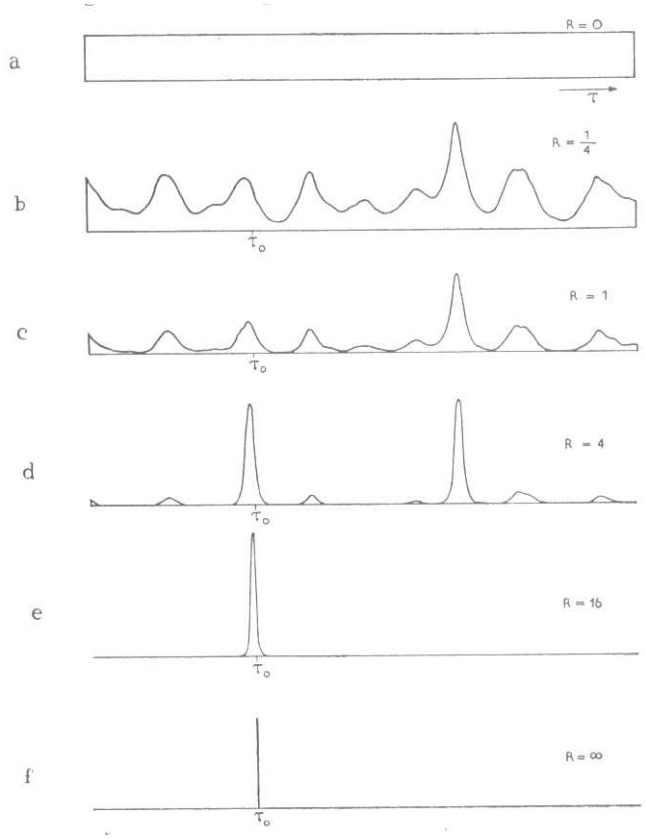
Sedan man kommit fram till en bedömning, som tillsammans med en värdering av alternativ leder till beslut, bör man jämföra bedömningen med uppgiften, för att se om sensorsystemet förmår lösa den. Informationsteorin gör att denna process kan formuleras i allmänna termer och på sikt även automatiseras. I existerande radarsystem styrs de tekniska lagren redan av algoritmer, som rätt nära följer det bayesianska schemat men med förenklade beräkningar.

Det abstrakta schemat motsvarar steg för steg den traditionella beskrivningen av ett radarsystem. Ett typexempel är spaning efter flygplan med radarkedjor. Den traditionella beskrivningen motsvarar steg för steg det abstrakta schemat uttryckt i radartermer.

MÄTOMRÅDE	→	MÅLSTORLEK	→	RADARTYP, VÅGFORM
↕				↓
BESLUT	←	SNR	←	AVSTÅND, RIKTNING, DOPPLER

Den största skillnaden är valet av sannolikheter som radarterminologin förvandlas till trösklar och SNR (signal-till-brus-förhållande). I traditionella system är man låst vid det som händer på skärmen. Numera övergår man alltmer till att lagra sannolikhetsfördelningarna för att uppnå en optimal bedömning. Ett typiskt exempel är *track-before-detect*, där följning påbörjas redan innan målet kommit över tröskeln för detektering.

De tvetydigheter som uppstår vid dessa processer analyserades redan av Woodward, men det dröjde innan hans metoder fick genomslag. Genombrottet skedde på 1980-talet när datorerna kunde genomföra de komplicerade beräkningarna. Woodward illustrerade i början på 1950-talet det endimensionella fallet på följande sätt (Woodward 1953).



Figur 7.
Upptäckt av mål vid successiv integration av flera pulser.

I bilden illustreras alla de fenomen som uppstår vid uppgiften att söka efter mål.

a) Fullständig okunskap om läget *a priori*.

b) Brus när mottagen energi är otillräcklig.

c) Mål börjar synas, men osäkerheten är stor.

d) Flera tänkbara mål börjar synas.

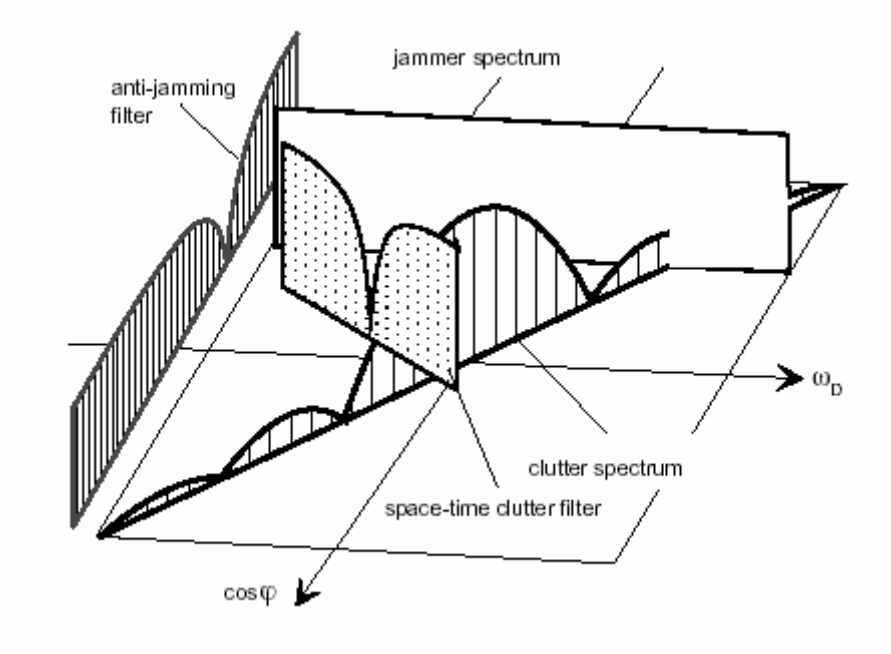
e) Ett mål upptäcks och övriga elimineras.

f) Målets läge mäts in som svar på en ny fråga: avstånd till målet?

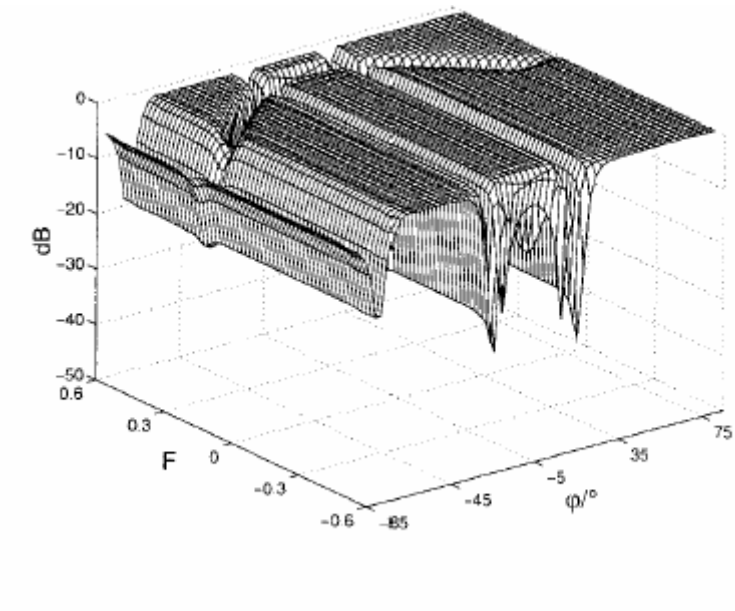
Analysen visar att man hela tiden måste hålla ögon på uppgiften. Om uppgiften ändras (”mät in läget!”) måste i princip hela beslutskedjan räknas om för att uppnå en optimal process. Woodwards analys visar hur viktig operatörens kunskap är vid lösandet av en uppgift. Det gäller särskilt vid tvetydigheter, som i princip alltid uppträder i radarfallet. En radar är begränsad till sitt instrumenterade avstånd: allt utanför denna ram tolkas in i radarbilden. Tvetydigheterna kan bara lösas upp genom att variera mätningen eller tillföra ny information, gärna i form av mänsklig kunskap som Woodward påpekade. ”First, however, a definite assumption has to be made about the prior distribution because ambiguity is a phenomenon which very definitely depends on the extent of prior knowledge.” (Woodward (1953)

I ett nätverk av sensorer växer problemen snabbt jämfört med det enkla radarfallet. Ett typiskt exempel är en modern radarmätning från flygplan filtrerad med hjälp av mänsklig kunskap. En flygburen radar söker efter mål i klotter som skapas av omgivande terräng. Radarn är utsatt för brusstörning från störsändare. Digitala filter kan dämpa störenergi med en faktor över 1000 och klottret med en faktor omkring 100 (Klemm 2002).

Konstruktionen av filtret bygger på kunskap om terrängen och om flygplanets uppträdande. Klottret har varierande radiell hastighet i förhållande till flygplanet beroende på siktvinkeln, vilket leder till olika dopplerskift. Störsändarna är punktkällor, vilket motsvarar bestämda riktningar och raka linjer i figuren. Filtrets prestanda ligger nära ett bayesianskt optimum och det vore svårt att tillföra ytterligare kunskap. Redan i två dimensioner (radiell fart och siktvinkel) blir beräkningarna oerhört komplicerade. I ett nätverk av sensorer växer svårigheterna snabbt på grund av oundvikliga tvetydigheter.



Figur 8.
Exempel på kunskapsbaserad filtrering. Punktstörare (rektangulärt spektrum) och markklotter (diagonal dämpad sinuskurva) dämpas ut med numerisk filtrering under en radarmätning.



Figur 9.
Dämpning av punktstörare (raka linjer) och markklotter (böjd linje) med numerisk filtrering enligt föregående schema. Radarmätning från flygplan utrustat med tre mottagarantenner.

9. Telekrig mot nätverk

De föregående resultaten kan tillämpas på informationsflödet i ett nätverk i närvaro av störning. Teorin visar att goda beslut bara är möjliga om all information utnyttjas på ett systematiskt sätt. Man kan (i medeltal) inte försämra sina beslut genom att ta med all information i bedömningen.

Ett villkor för denna slutsats är att databehandlingen sker så snabbt att fördröjningar i nätverket inte påverkar processen. Uppgiften och läget måste vara så stationära att information kan bearbetas och hinner påverka besluten. I ett modernt nätverk är snabb kommunikation inget problem, men sändningen måste begränsas av risk för upptäckt. I äldre system finns det länkar med begränsad kapacitet som inte får överbelastas.

Sedan dessa begränsningar beaktats består processen i att uppdatera sannolikheterna genom att tillföra nya sensordata. Ingen information försvinner i princip under denna process och Bayes' formel garanterar att data behandlas optimalt i förhållande till uppgiften. Kunskap *a priori* kan tas med genom att subjektiva sannolikheter beskriver personalens förmåga. En sådan beskrivning innebär begränsningar jämfört med verkligheten, men de kan redovisas och diskuteras och korrigeras under analysens gång.

9.1 Beslut nära tröskeln

Exakta beräkningar i ett sensornätverk kan av tidsskäl inte alltid genomföras. Mestadels låter man sig nöja med deterministiska slutsatser, t ex när en radar söker ett ensamt mål i luften med stort signal-till-brus-förhållande. Den bayesianska teorin är särskilt användbar i komplicerade fall, t ex ett mål nära tröskeln för upptäckt. I denna situation kan mänsklig information på ett avgörande sätt bidra till att man fattar rätt beslut.

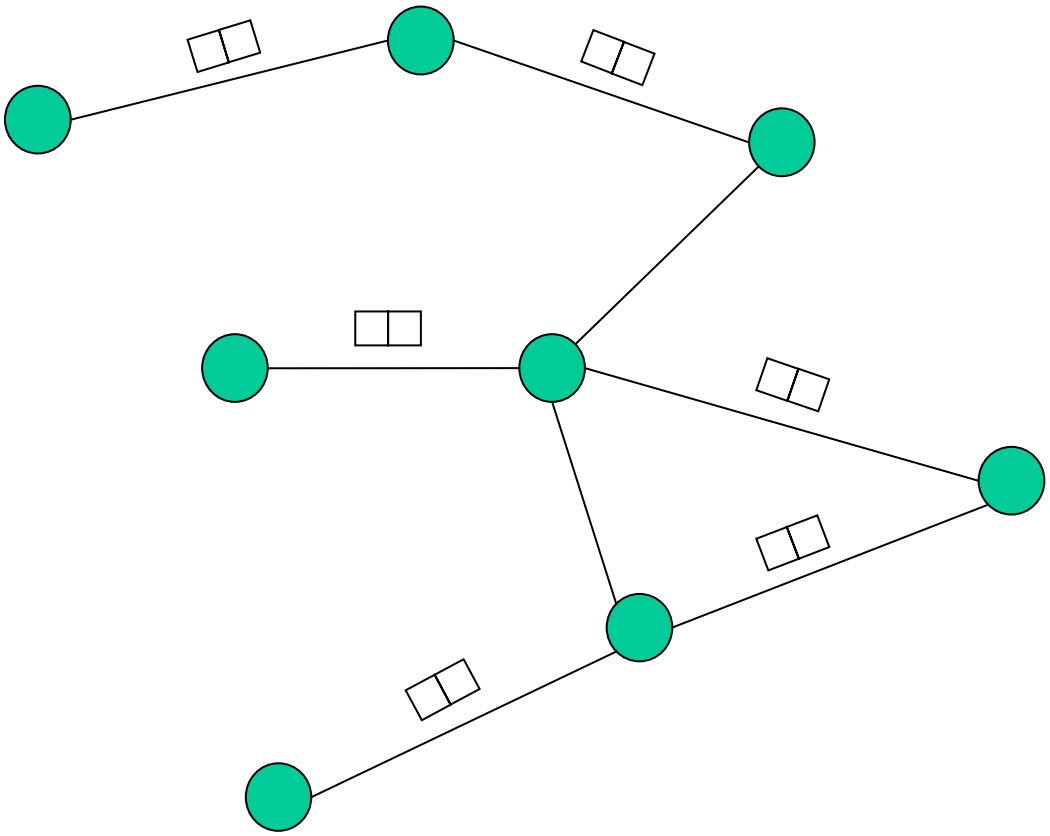
Beslut nära tröskeln har speciellt intresse, eftersom syftet med telekrig är att sätta in en störinsats som nätt och jämt blockerar upptäckt och beslut. Typiska tröskeleffekter är upptäckt av mål nära känslighetströskeln och identifiering av mål. Två sådana exempel diskuteras här för att illustrera svårigheterna med att skapa en systematisk beslutsprocess byggd på sannolikheter.

Ett välkänt fall är sökandet efter den sjunkna ubåten Scorpion 1969 (Sontag 1999; Falk 2002). Under sökandet måste man kombinera några få, exakta hydrofonmätningar med allmän kunskap om hur en ubåt uppför sig i krissituationer. Den senare informationen är svår att beskriva: den samlades in genom intervjuer med experter som fick sätta sannolikheter för de alternativ som användes för bayesiansk analys under utredningens gång.

Vid identifiering av okända mål spelar mänsklig kunskap en stor roll. Den bidrar inte med många bitar information, men kan vara avgörande för valet mellan olika alternativ. Den mänskliga kunskap som tillförs vid identifiering av mål bör vara ortogonal mot den tekniska informationen för att tjäna som ett tillskott och inte upprepa kända resultat.

Svårigheterna med identifiering är lika stora när det gäller egna farkoster. De terrorister som kapade flygplanen den 11 september 2001 slog genast av transpondersystem, eftersom de visste att flygplanen skulle bli osynliga för den civila luftbevakningen. Flygplanen upptäcktes inte med radarn därför att man sedan länge förlitar sig på transponderfunktionen.

Många situationer är svåra att förutse. Ett brittiskt Tornadoplan sköts 2003 ner av ett amerikanskt Patriot-batteri. Missförståndet berodde enligt uppgift på att reflexer av signaler från andra radarstationer misstolkades som en radarsökande robot (Postol 2004). IK-transpondern svarade inte, möjligen beroende på ett kraftbortfall som besättningen inte kunde observera. I sådana situationer finns ofta mer information om målet än vad som nämns i reglementet, men det krävs god utbildning för att tolka den. I det nämnda fallet valde personalen i batteriet att följa reglementets instruktioner.



Figur 10.
I ett framtida automatiserat nätverk kommer informationsflödet att bestå av datapaket som överför information och underrättelsebehov för varje given uppgift.

9.2 Skenmål

I framtida system kan uppdrag och data från sensorerna distribueras parallellt som datapaket enligt figuren (Falk och Hyberg, 2003). Genom kodning försäkrar man sig om att data kommer fram med hög tillförlitlighet. Ur telekrigssynpunkt är problemet det omvända: hur ska information stoppas och vilka noder och länkar ska man angripa för att hindra beslut?

Kodning och redundans är ett effektivt sätt att bemöta telekrig mot länkarna med tanke på att vanlig störning slår planlöst. Ren brusstörning döljer egna företag men leder till att uppmärksamheten riktas mot dem. En bättre lösning är att slå mot beslutsfunktionerna i den mån de kan identifieras. För ett sensorsystem sker det bäst genom att man överlastar sensorerna med falska mål som är tillräckligt trovärdiga för att passera yttre filterfunktioner.

Sådana skenmål kan genereras mot radarstationer med hjälp av DRFM (digitala radiofrekventa minnen). Överflödig information blockerar linjerna och tynger ner beräkningarna, så att processorn inte kommer till beslut. Systemet behöver inte ens upptäcka att det är stört utan kan vara fullt sysselsatt med att rensa bort fel.

Det är uppenbart att insatser som riktas mot beslutsprocessen kan ge goda resultat även mot nätverk. Militära beslut är vanligen hårt centraliserade och standardiserade. Den formalism som beskrivits i denna rapport ger kvantitativa upplysningar om var gränsen för effektiv störning går och kan användas för att uppskatta vilken störning som krävs för att störa ut nätverk. Telekrig mot beslutsfattaren är effektivt. Ett viktigt syfte med det fortsatta arbetet är att undersöka var gränsen går i praktiskt existerande system.

Nätverk är effektiva mot traditionell störning, där man försöker dölja enstaka mål genom att överrösta radarekon från ett givet område. I sådana fall blir nätverket varnat och kan välja andra sensorer, men förblir känsligt för angrepp mot beslutsfunktionen. Slutsatsen är att vilseledning är överlägsen brusstörning vid bekämpning av ett utbyggt nätverk av sensorer.

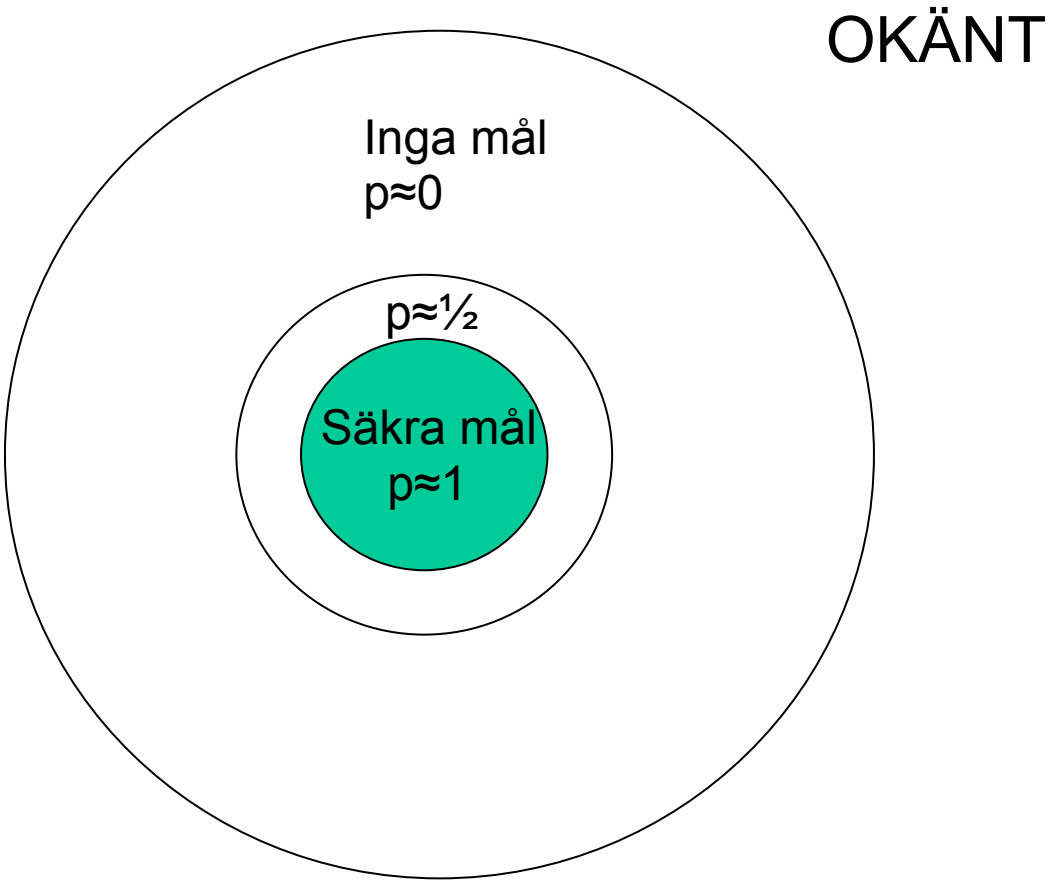
9.3 Vilseledning

Vilseledning har använts vid många av världshistoriens mest berömda militära segrar. Resultatet blir ofta spektakulärt som vid Hannibals segrar över romarna. De vanns genom intensiv spaning och hård disciplin hos trupperna. Bakhållet vid Trasimenus och inringningen vid Cannae omges av ett legendariskt skimmer, eftersom romarna krossades av numerärt underlägsna styrkor.

Lika ryktbara är den sovjetiska inringningen vid Stalingrad och invasionen i Normandie. Båda dessa operationer föregicks av långvarig och omsorgsfull planering där man i detalj studerade motståndarens avsikter och kunskapsläge. Hannibal lärde känna den romerska taktiken innan han utnyttjade den genom sina exakta manövrer vid Cannae. De sovjetiska styrkorna vid Stalingrad tog dagligen fångar för att lära känna läget (Beevor 2001). Segrarna byggde på ett övertag i kunskap som tog lång tid att bygga upp.

Vilseledning på högre nivå kräver ofta mindre resurser. Det kan röra sig om propaganda som riktas mot andan i en nation eller armé, d v s i princip mot förmågan att fatta och genomföra beslut (Taylor 1995). Systematisk vilseledning betraktades tidigare som en spektakulär men mycket ovanlig möjlighet att vinna slag, eftersom man sällan nådde fram till

beslutsfunktionen. Genomförandet krävde kunskap, disciplin och långa förberedelser. Vid elektronisk krigföring är läget ett annat. Det är lätt att generera skenmål och vilseledning kan inledas snabbt sedan man kartlagt nätverket av sensorer. Uppgiften är väldefinierade och det är jämförelsevis lätt att rikta vilseledningen mot beslutsfunktionen.



Figur 11.
Ett nätverk avsett för spaning, på marken eller i luften, hanterar vanligen bara ett måttligt antal mål inom sökvolymen, d v s förhållandet mellan antalet radarluckor med ett respektive inga säkra mål är litet. Filtren hanterar de luckor som innehåller osäkra mål (p=½), men skenmålen kan påverka beslutsfunktionen och överbelasta hela processen.

En viktig slutsats är att målen inte behöver vara många. De måste främst vara trovärdiga för att nå fram till beslutsfunktionen. Det är lätt att uppskatta hur olika störmetoder fungerar mot ett nätverk. I spaningsfallet förutsätter systemet vanligen att volymen hos det (logiska) rum som är fritt från mål (p=0) är mycket större än andelen upptäckta mål (p=1). Det är alltså fördelaktigt att generera falska mål som passerar filtren och belastar beslutsfunktionen. Dessa

mål bör vara så normala som möjligt för att försena beslut om att förkasta dem. Detaljerade analyser av detta problem kommer att publiceras i ett följande arbete.

10. Sammanfattning

Analysen visar att funktion och tålighet hos militära nätverk kan beskrivas effektivt med hjälp av informationsflödet i systemet. En sådan beskrivning kräver stora resurser och fordrar kunskap om osäkerheter i form av objektiva och subjektiva sannolikheter. Fördelen är att metoden kan användas för att analysera nätverkens prestanda även vid telekrig och andra former av yttre bekämpning som sällan modelleras i verkliga försök. Den viktigaste slutsatsen är att en sannolikhetsbeskrivning måste omfatta både sensorer och observatörer för att vara effektiv. Vilseledning med hjälp av skenmål visar sig vara en mycket effektiv form av bekämpning, eftersom den når ända fram till beslutsprocessen. Det är lätt att uppskatta hur nätverkets filter fungerar mot olika typer av skenmål. Analysen ger på detta sätt ett mått på vilken nivå övningar och verkliga anfall ska läggas för att vara effektiva. Dessa frågor kommer att studeras experimentellt vid försök tillsammans med Försvarsmakten.

Erkännande

Olle Malm, Mikael Nordström och Michael Herre vid StrilS i Uppsala har bidragit med en rad värdefulla synpunkter på funktionen hos sensorsystem i nätverk. Ett speciellt tack vill författaren rikta till Philip M. Woodward i Malvern, England, som i samtal beskrivit sitt arbete med denna analysmetod under radarns första tid. Författaren är tacksam mot Per Hyberg, FOI Försvarsanalys, för en rad diskussioner kring detta arbete.

Referenser

A.-L. Barabasi and E. Bonabeau: Scale-free networks. Scientific American, May 2003, pp. 50-59.

A. Beevor: Stalingrad (Historiska media 2001).

Christian Carling och Henrik Carlsen: ”Inte bara Internet”, Framsyn nr 4, 2003.

Carl von Clausewitz: Om kriget. Översättning och granskning av Hjalmar Mårtensson, Klaus-Richard Böhme och Alf W. Johansson (Bonniers 1991).

Chris Craig: Eldunderstöd. Sjöstriderna under Falklands- och Gulfkriget (Marinlitteraturföreningen nr 86, 2000).

Lars Falk.: "Information flow in radar”, Invited paper. RadioVetenskap och Kommunikation 2002. RVK-02, Stockholm, 10 – 13 June 2002. (FOI-S--0466--SE)

Lars Falk: "Informationsflödet i nätverksbaserat försvar", FOI rapport FOI-R—0658--SE, november 2002.

Lars Falk: "Information Flow in an Air Defence System", Föredrag på Dstl, Farnborough, 6 maj 2004.

Lars Falk: "Information in radar – a tribute to P. M. Woodward", Waveform Diversity and Design Conference, Edinburgh, November 2004. Conference CD.

Lars Falk och Per Hyberg: "Telekrig och information i nätverk", FOI Memo 03-2283, oktober 2003.

H. D. Griffiths: "Knowledge-based solutions as they apply to the general radar problem (RTO Lecture Series 233, 2003).

Per Hyberg: "Informationshantering i sensorberoende luftförsvarssystem", FOI-R--0466—SE, september 2002.

Per Hyberg: "Omvärldsuppfattning i sensorbaserade luftförsvarssystem" FOI-R--1392—SE FOI, november 2004.

E. T. Jaynes: Probability theory: The logic of science (Cambridge University Press, Cambridge 2003).

D. J. King: An Information Map for Electronic Warfare, Dstl/CR09861/1.0, April 2004.

J. Kjellgren: "A simple study of the information requirements for missile guidance", Acquisition, tracking and pointing XVII, M K Masten, L A Stockum, Editors, Proceedings of SPIE Vol. 5082 (2003), p 77-86.

Gary Klein: Sources of power. How people make decisions (The MIT Press 1998).

R. Klemm: Principles of Space-Time Adaptive Processing (IEE 2002)

S. Kullback: Information theory and statistics (John Wiley and Sons 1959).

David MacKay: Information Theory, Inference & Learning Algorithms (Cambridge University Press, 2003).

James Moffat: Complexity Theory and Network Centric Warfare (CCRP Publication Series 2003).

P. M. Morse and G. E. Klein: Methods of operations research (The MIT Technology Press 1950).

J. Pearl: Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference (Morgan Kaufmann Publishers 1997).

T. A. Postol: An informed guess about why Patriot fired upon friendly aircraft and saw numerous false missile targets during Operation Iraqi Freedom (MIT Report 2004).

Sherry Sontag and Christopher Drew: Blind Man's Bluff (Harper Paperbacks 1999).

D. Sefaty, E. E. Entin and R. R. Tenney: “Planning with Uncertain and Conflicting Information”, in Science of Command and Control, Vol. 2 (ed. S. E. Johnson and A. H. Levis, AFCEA International Press 1989).

C. E. Shannon: A mathematical theory of information. Bell Sys. Tech. Jour. vol. 27, p. 379, 1948.

P. M. Taylor: Munitions of the Mind: A History of Propaganda (Manchester University Press, 1995).

P.M.Woodward: Probability and information theory with applications to radar (Pergamon Press, London 1953).

S. Woodward: Ett hundra dagar. Striden om Falklandsöarna. (Marinlitteraturföreningen nr 77, 1994).