Telekrig mot NBF, resultatöversikt: Teori och metoder

LARS FALK

FOI
Totalförsvarets forskningsinstitut
Försvarsanalys
164 90 Stockholm

Tel: 08-555 030 00
Fax: 08-555 031 00

www.foi.se

FOI-R--1803--SE
ISSN 1650-1942

Underlagsrapport
December 2005

Försvarsanalys

Lars Falk

Telekrig mot NBF, resultatöversikt:

Teori och metoder

FOI-R--1803--SE
ISSN 1650-1942

Försvarsanalys
Underlagsrapport

December 2005

Utgivare FOI - Totalförsvarets forskningsinstitut Försvarsanalys 164 90 Stockholm	**Rapportnummer, ISRN** FOI-R--1803--SE	**Klassificering** Underlagsrapport
	Forskningsområde 6. Telekrig och vilseledning	
	Månad, år December 2005	**Projektnummer** E1421
	Delområde 61 Telekrigföring med EM-vapen och skydd	
	Delområde 2	
Författare/redaktör Lars Falk	**Projektledare** Roland Heickerö	
	Godkänd av E. Anders Eriksson	
	Uppdragsgivare/kundbeteckning	
	Tekniskt och/eller vetenskapligt ansvarig	

Rapportens titel

Telekrig mot NBF, resultatöversikt: Teori och metoder

Sammanfattning

Nätverksbaserat försvar (NBF) är avsett att ge Försvarsmaktens personal en snabb och säker omvärldsuppfattning inför beslut. Nätverk är flexibla och robusta strukturer som uthärdar förlusten av enstaka noder och därmed är mindre känsliga för traditionella former av telekrig mot sensorer och kommunikationslänkar. Inom projektet ”Telekrig mot NBF” studeras nya former av telekrig som kan användas mot nätverksbaserat försvar. Analysen visar att det är fördelaktigt att angripa beslutsfunktionen direkt genom mättning och vilseledning av systemet. Dessa åtgärder är billiga och kan sättas in snabbt. För att analysera verkan beskrivs en teori för telekrig som tillämpas på olika fall. Teorin beskriver både data från sensorer och operatörernas kunskaper i temer av sannolikhet genom att representera dem som alternativ som påverkas av ny information. Denna beskrivning av systemets omvärldsuppfattning leder till en klassificering av olika former av telekrig som gör det möjligt att uppskatta och jämföra deras effekt. Vilseledning visar sig vara en särskilt effektiv åtgärd som kan sättas in redan på taktisk nivå.

Nyckelord

telekrig, NBF, NCW, NEC, störning, informationsteori, sannolikhet, omvärldsuppfattning

Övriga bibliografiska uppgifter	**Språk** Svenska
ISSN 1650-1942	**Antal sidor:** 35 s.
Distribution enligt missiv	**Pris: Enligt prislista**

Issuing organization	Report number, ISRN	Report type
FOI – Swedish Defence Research Agency Defence Analysis SE-164 90 Stockholm	FOI-R--1803--SE	Base data report
	Programme Areas 6. Electronic Warfare and deceptive measures	
	Month year December 2005	**Project no.** E1421
	Subcategories 61 Electronic Warfare including Electromagnetic Weapons and Protection	
	Subcategories 2	

Author/s (editor/s)	Project manager
Lars Falk	Roland Heickerö
	Approved by E. Anders Eriksson
	Sponsoring agency
	Scientifically and technically responsible

Report title (In translation)

Electronic warfare against NCW/NEC, overview of results: Theory and methods

Abstract

Network Based Defence (NBF) has been introduced in Sweden to provide military personell with rapid and reliable Situational Awareness. Networks are flexible and robust structures that can function even if some nodes are lost. This property makes the network less sensitive to traditional forms of electronic warfare, which are directed at individual sensors and communication links. The project “Electronic warfare against NBF” was initiated to study new forms of electronic warfare that may be used against Network Based Defence. The analysis shows that it is advantageous to attack the decision process by flooding the system and applying deception. These methods are cheap to use and can be initiated at short notice. The effect of electronic warfare is analysed by developing a theory which is applied to several different cases. The theory describes the data obtained from sensors and the knowledge of operators by representing them as choices and assigning probabilities in terms of information. This view of Situational Awareness can be used to classify various forms of electronic warfare and assess their effectiveness. Deception is shown to be a particularly effectiv method and can be applied even at the tactical level.

Keywords

electronic warfare, NBF, NCW, NEC, jamming, information theory, probability, situational awareness

Further bibliographic information	Language Swedish
ISSN 1650-1942	**Pages** 35 p.
	Price acc. To pricelist

1. INLEDNING

Militära ledningssystem ska kunna agera snabbt och effektivt på ofullständig information. Inför viktiga beslut är det nödvändigt att ledningen kan överblicka riskerna och alla de osäkerheter som är förknippade med ett beslut.

Försvarsmakten prövar för närvarande det nätverksbaserade försvaret (NBF) som är avsett att ge personalen snabb och säker omvärldsuppfattning. Nätverk är flexibla och robusta strukturer, där kommunikationslänkarna kan flyttas och utslagna noder ersättas med nya. Nätverk är mindre känsliga för störningar än hierarkiska organisationer och det gör de traditionella formerna av telekrig mindre verkningsfulla. Det gäller särskilt de metoder som bygger på bekämpning av enstaka länkar och sensorer.

Nätverk har fördelen att de är rika på information. Data samlas in från många oberoende sensorer och kunskapen kan distribueras bland flera användare. Det gör bearbetningen mindre känslig än i äldre system, där informationen analyseras centralt i några få staber. Det nätverksbaserade försvaret är en intressant utmaning för framtida telekrig med tanke på att informationsflödet är elektroniskt och fördelat över ett större system utan klara angreppspunkter.

2. SYFTE

Inom projektet ”Värdering av telekrig i NBF” studeras de nya former av telekrig som kan användas mot nätverk. Syftet med rapporten är att ge en översikt av de teorier och metoder för telekrig som utvecklats under projektets gång. De nya metoderna har prövats i praktiska försök och visat sig vara framgångsrika. Det är viktigt att denna försöksverksamhet fortsätter, eftersom Försvarsmakten har goda resurser för att simulera telekrig mot nätverk.

Simuleringar gör det möjligt att effektivt upplysa personalen om nya former av telekrig. Den pedagogiska uppgiften är stimulerande och har varit ett viktigt delmål för arbetet enligt projektbeskrivningen för ”Värdering av telekrig i NBF”: ”Denna verksamhet kommer att leverera en konsekvensbeskrivning av hur telekrig påverkar ett modernt spanings- och ledningssystem inklusive beslutsfattarnivån. Ett viktigt syfte med verksamheten är att skapa ett pedagogiskt instrument för att beskriva och utveckla nya (okända) system.”

En viktig slutsats av arbetet är att framtida angrepp med fördel kan riktas mot beslutsfunktionerna snarare än sensorerna. Det nätverksbaserade försvaret är tåligt för bekämpning av enstaka sensorer och länkar. Den effektivaste formen av telekrig är därför att rikta insatserna mot tilltron till nätverket. Det visar sig vara särskilt effektivt att angripa beslutsfunktionen genom mättning och vilseledning. Denna slutsats har prövats på både teoretisk och experimentell väg inom projektet.

3. METOD

I denna rapport ges en översikt av de begrepp som införts och prövats inom projektet ”Värdering av telekrig i NBF” under åren 2003-2005. Många resultat har publicerats som rapporter och internationella konferensbidrag för att sprida kunskapen inom Försvarsmakten (Falk 2005).

Avsikten var ursprungligen att analysera informationsflödet i sensorer och länkar för att undersöka hur nätverkets struktur påverkar förloppet. Denna del av arbetet har sammanfattats av Per Hyberg i en parallell rapport, som också beskriver hur personalens reaktioner kan modelleras i ett informationsteoretiskt perspektiv (Hyberg 2005).

I föreliggande rapport analyseras informationsflödet med hjälp av en ny metod som både beskriver dataflödet från sensorerna och personalens uppfattning om läget (Falk 2005). Under de senaste åren har gränsen mellan människa och maskin förskjutits. Datorerna har tagit över många av de uppgifter som operatörerna haft tidigare. Människan behövs främst för att tillföra erfarenhet och hålla kontakt med utomstående organisationer.

En gemensam beskrivning av människa och maskin är nödvändig, i synnerhet när det gäller svåra uppgifter som identifiering och bedömning av målens avsikter. Den generella modell som beskrivs i denna rapport ger en överskådlig bild av hur ett nätverk fungerar och gör det möjligt att dra allmänna slutsatser om hur telekrig mot nätverk bör utformas. Det är inte nödvändigt att räkna genom varje fall i detalj för att jämföra effekten av olika former av telekrig. Analysen visar att det finns flera sätt att föra telekrig mot nätverk. Den metod som rapporteras gör det möjligt att jämföra deras effektivitet i kvantitativa termer med hjälp av enkla uppskattningar.

4. ARBETETS UPPLÄGGNING

Idén att studera informationsflödet i sensorer och länkar för att få ett mått på deras effektivitet har sitt ursprung i den undervisning i radar och telekrig som författaren och Per Hyberg i flera år bedrivit på FHS. Det har visat sig fördelaktigt att diskutera nyttan av olika former av telekrig i termer av osäkerhet. I teknisk mening kan osäkerheten uttryckas med hjälp av Shannons entropi, som är ett mått på den mängd information som krävs för att skapa en tillräckligt fullständig omvärldsuppfattning för att lösa en förelagd uppgift (Hyberg 2003).

En användbar beskrivning av osäkerheten kräver att entropin relateras till användarens avsikt, som kan bero både på objektiva och subjektiva kvantiteter (Falk 2004). En fullständig lösning av problemet är besvärlig, men det är fullt möjligt att dra allmänna slutsatser om hur telekrig mot nätverk bör genomföras utan att ge sig in på stora beräkningar (Falk 2005).

De teoretiska analyserna leder fram till ett behov av att utföra motsvarande försök i en simuleringsanläggning. På StriC i Uppsala finns en utmärkt simulator för ändamålet. Försöken är hemliga och kan bara beskrivas kortfattat här, men det är viktigt att notera att metoderna växte fram i dialog med personalen som vet hur systemet är organiserat och vilka sensorer man kan lita på (Hyberg, Falk och Malm, 2005; Hyberg 2005).

5. RAPPORTENS STRUKTUR

I rapportens första del ges en allmän beskrivning av hur militära nätverk fungerar för att förklara varför Stril valdes som exempel. Avsikten är att gå vidare till nya försök med andra former av nätverksbaserat försvar. Flygspaning är ett representativt exempel, eftersom radarsensorerna är pålitliga och operatörerna ofta erfarna. Det innebär att försök på Stril ger resultat som inte snedvrids av osäkerheter och brister i systemet.

I nästa avsnitt förklaras varför nätverk måste beskrivas med sannolikheter, trots att det medför många komplikationer. Som exempel används Skagerackslaget 1916, som är väl beskrivet i litteraturen men också representativt, eftersom flera former av osäkerhet påverkade besluten. Marina exempel är givande, eftersom lägesbilden innehåller mycket information och felaktiga beslut snabbt leder till svåra följder.

Liknande överväganden kommer att göras under framtida svenska insatser i utlandet. Nordic Battle Group (NBG) kommer att ha god tillgång till sensorer, men mycket låg acceptans för förluster. Det gör att alla risker måste beskrivas i termer av sannolikheter, om man ska komma till riktiga beslut. En sådan detaljerad beskrivning leder till den intressanta frågan hur omvärldsuppfattningen växer fram i moderna sensorsystem. Analysen visar vilka metoder för telekrig som är lämpliga att använda mot nätverk. Vilseledning visar sig vara speciellt användbar, eftersom metoden riktar sig mot beslutsfunktionen i systemet.

Avslutningsvis analyseras begreppet militär vilseledning och illustreras med flera exempel. Vilseledning har tidigare mest använts på operativa nivåer och högre upp (Smedberg 2001). Analysen visar att metoden i framtiden också kan komma att användas på taktisk nivå, där kampen förs mellan elektroniska system med god omvärldsuppfattning och snabba reaktioner. Slutligen visas ett exempel på farorna med att förlita sig enbart på nätverk av sensorer.

6. NÄTVERK AV SENSOR

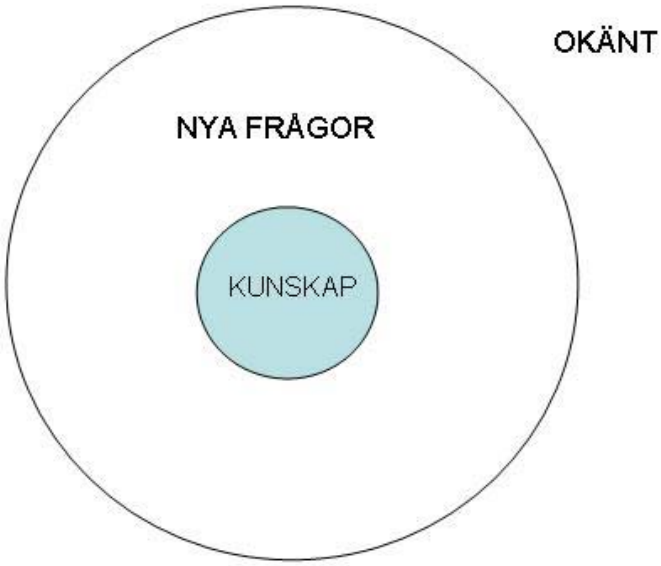
6.1 Omvärldsuppfattning

Grundvalen för en analys av nätverk är en beskrivning av hur sensorer och operatörer gemensamt bygger upp sin omvärldsuppfattning (Situational Awareness, SA).

Den analysmetod som beskrivs i rapporten utvecklades ursprungligen för att undersöka vilken innebörd begreppet ”information” har i termen ”informationskrig”. Ordet ”information” har en teknisk innebörd som motsvarar det militära behovet av att skapa en klar och tydlig omvärldsuppfattning. Begreppet ”informationskrig” används många gånger okritiskt och det är angeläget att undersöka om termen kan ges en teknisk definition (Falk och Hyberg, 2002).

Information i teknisk mening är en kvantitet som används för att lösa upp osäkerhet. För att beskrivningen ska vara relevant måste man veta vilka uppgifter som ska lösas och vilka frågor som ska besvaras. Det innebär att det tekniska begreppet ”osäkerhet” är nära relaterat till det militära begreppet ”omvärldsuppfattning”. Omvärldsuppfattningen blir fullständig för ett givet ändamål i samma ögonblick som all osäkerhet försvinner.

Fullständig omvärldsuppfattningen beskrivs ofta som ett mål för framtida militära operationer. Detta ideal skiljer sig radikalt från den dimma och friktion som enligt Clausewitz utmärker ett klassiskt slagfält. Den stora svårigheten med att skapa en pålitlig omvärldsuppfattning är inte att samla in data utan att definiera de konceptuella ramar inom vilka osäkerheten ska beräknas. Detta förhållande är välkänt för alla utredare: jurister, försäkringsmän och underrättelsepersonal bygger sina slutsatser på spaning och vet att verksamheten bygger på att man vet vad man *inte vet*, lika mycket som man kan tala om vad man vet. Detta förhållande illustreras i följande figur.



Figur 1. Kunskapen i ett nätverk av sensorer måste vägas mot vilka frågor som ännu inte besvarats. Dessutom finns det frågor som är oåtkomliga för systemet, men som kan vara betydelsefulla för beslut. Modellen omfattar också operatörernas kunskaper, men geometrin kan vara mer komplicerad än bilden antyder.

Goda chefer utmärker sig ofta genom denna insikt. Det är inte lätt att medge sin okunnighet, men när hertigen av Wellington någon gång råkade i fara brukade det bero på att han gett sig ut på egna spaningsföretag för att finna kunskap som saknades. Han underströk ofta att man måste skaffa sig kännedom om det som är okänt snarare än det som är välbekant.

"All the business of war, and indeed all the business of life, is to endeavour to find out what you don't know from what you do; that's what I called 'guessing what was on the other side of the hill."(Croker Papers, vol. 3)

6.2 Nätverksbaserat försvar

Verksamheten i ett nätverk av sensorer ska ge underlag för beslut genom att skapa en pålitlig omvärldsuppfattning. Teorin visar att det krävs klar blick för avsikten och riskerna om man ska kunna formuleras en sådan modell. Det är naturligt att det ställs formella krav med tanke på att så få dödsfall och skador numera tolereras vid militära insatser. Det innebär att alla data och kunskaper måste beskrivas i sannolikheter för att kunna användas i riskbedömningar.

Inom Försvarsmakten finns redan flera nätverk med beslutsfattare och kommunikationscentra utrustade med effektiva sensorer och vapenbärare. Typiska exempel är Stril och FV 2000. Det pågår dessutom en utveckling mot det nätverksbaserade försvaret, NBF, som förutsätter att nya plattformar kan lösa flera uppgifter och vid behov ersätta varandra. Ett sådant nätverk kan bli ytterst flexibelt och uthärdar många former av traditionellt telekrig.

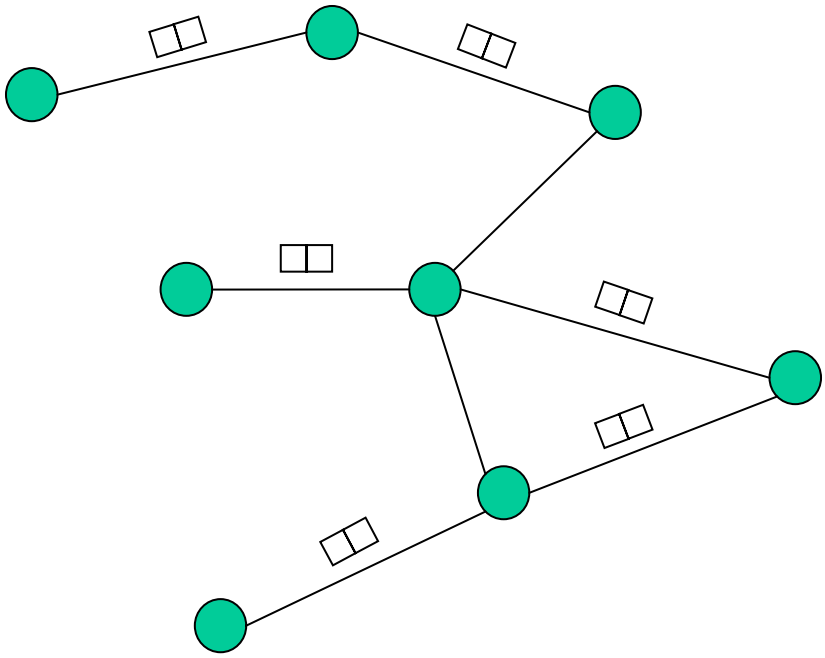
Nätverksprincipen har använts länge för att konstruera tekniska system, men inom den militära världen var det något av en revolution när motsvarande principer började tillämpas. Termen ”Revolution in Military Affairs” (RMA) användes under 1990-talet för att beskriva det nya läget. De traditionella hierarkierna förväntades på sikt lösas upp, så att detaljerade föreskrifter kunde ersättas med en friare organisation som kan agera snabbt och självständigt på tillgänglig information.

Projektet ”Värdering av telekrig i NBF” syftar till att öka förståelsen för hur telekrig kan störa ett nätverksbaserat försvar. För att undersöka dessa frågor måste man i första hand studera egenskaperna hos ett nätverk byggt för militära ändamål.

Ett nätverk ska samla in och bearbeta information och förmedla data i lämplig form till beslutsfattarna. Nätverket ska också kunna samordna information från olika enheter och skapa en fullständig omvärldsuppfattning under förutsättning att sensorerna är tillräckligt effektiva. Traditionellt samordnas informationen i staber och ledningscentraler, men moderna nätverk överför data snabbt och precist och analysen kan fördelas över hela systemet.

Mängden snabbt tillgänglig information har revolutionerat den militära tekniken. Datorerna erbjuder nya möjligheter att bearbeta data och det har väckt förhoppningar om att man ska kunna skapa insyn i motståndarens verksamhet och på så sätt skaffa sig full kontroll över läget.

Erfarenheterna från krigen i Kuwait 1991 och Irak 2003 har visat att det i vissa fall är möjligt att uppnå total överlägsenhet på informationsarenan. Å andra sidan finns det exempel från Kosovo och Irak som tyder på att även enkla åtgärder kan hindra insyn. Frågan är om ett välplanerat telekrig skulle kunna rubba tilltron till ett nätverk, t ex genom att man lyckas föra in falsk information i systemet för att vilseleda motståndaren. Tillit är kittet i alla nätverk och om trovärdigheten försvinner bryter analysen samman.



Figur 2. Ett nätverk är flexibelt genom att länkarnas och nodernas placeringar kan varieras. Nätverket är också robust mot förlust av enstaka noder, eftersom det är rikt på överlappande information. Data från sensorer och annan information förmedlas som datapaket inom nätverket med modern kommunikationsteknik.

6.3 Val av exempel

Nätverkets förmåga beror lika mycket på sensorernas egenskaper som systemets förmåga att förmedla och analysera data. För att studien ska bli effektiv måste man undersöka ett nätverk med kraftfulla sensorer, som i ostört tillstånd kan lösa alla uppgifter av betydelse. Under projektet visade sig ett utmärkt exempel finnas tillgängligt i form av simuleringsutrustningen på Flygvapnets anläggning StriC i Uppsala.

Ett nätverk av sensorer är rikt på information och bildar dessutom en flexibel och robust struktur. Risken är att tillförlitligheten skapar överdriven tilltro till systemet. Kunskapen är ofta anonym och det öppnar möjligheter att föra in falsk information i nätverket. Hög tilltron och bristande insikt hos användarna är goda utgångspunkter för telekrig. För att finna lämpliga angreppspunkter måste man undersöka en generell struktur som innehåller väl utvecklade sensorer och kraftfulla system för datafusion och analys.

Den naturliga kandidaten är spaningsradar. Det finns gott om automatiserade system som samordnar information från många olika radarenheter. Operatörerna är ofta väl utbildade och uppgiften att bevaka luftrummet är entydigt definierad. Systemet är särskilt instruktivt genom att det är enkelt att upptäcka mål, men svårt att tillföra mänsklig kunskap för att lösa de besvärliga uppgifterna att identifiera flygföretag och bedöma deras avsikter.

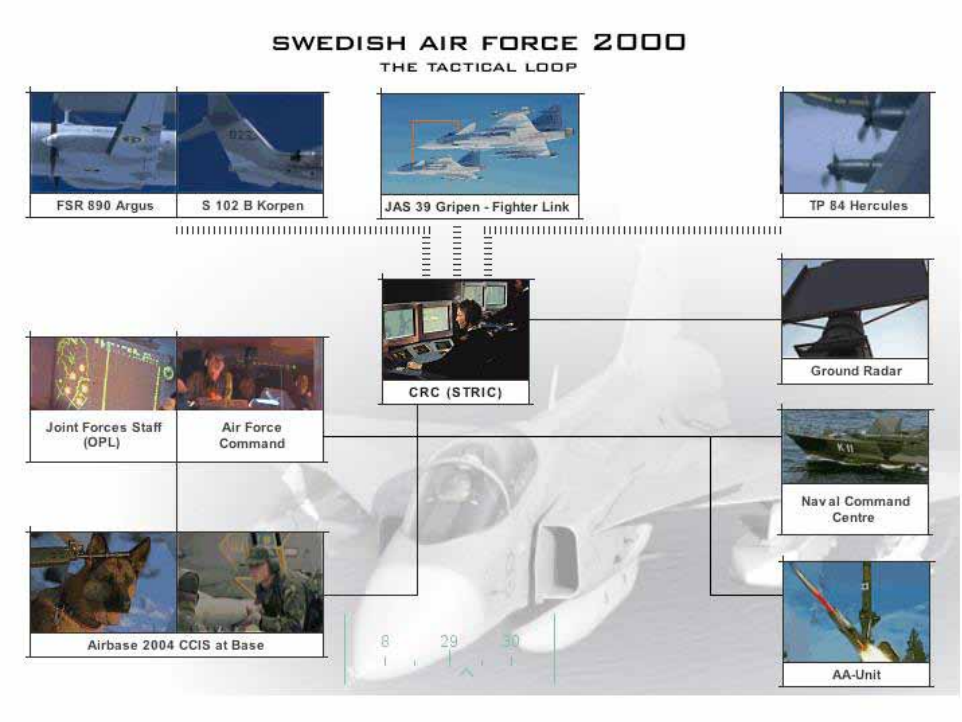
Figur 3. Det första exemplet på att radarstationer samordnades i ett nätverk var Chain Home. Bilden visar ett 110 m högt torn i Essex. Radarn använde låga frekvenser (30 MHz) och antennerna var känsliga för fysiska angrepp, en möjlighet som tyskarna försummade att utnyttja. Data förmedlades till sambandscentraler via telefon.

6.4 Exempel på radarnätverk

Redan i radarns barndom bildades det första nätverket av radarsensorer, Chain Home. Britterna byggde före andra världskriget upp detta system inför väntade bombanfall mot storstäderna. Som de flesta sensornätverk innehöll det flera olika typer av sensorer. Förutom radar ingick optiska observatörer och sambandscentraler. Radarsystemet var uppdelat i två system, Chain Home med lång räckvidd och Chain Home Low med ytterst begränsad räckvidd men kapacitet att upptäcka flygplan på låg höjd.

Radardata behöver vanligen kompletteras med annan information för att utnyttjas effektivt. Långt efter kriget avslöjade engelsmännen att de kunde läsa en del meddelanden som skrevs med den tyska chiffermaskinen Enigma. Sådana meddelanden sändes via radio och snappades upp av signalspaningen. Resultatet av analysen blev sällan tillgängligt så snabbt att det gav förvarning om förestående flyganfall, men den tyska rapporteringen om förluster och förstärkningar var ovärderlig (Winterbotham 1977). Chain Home kan mycket väl ha avgjort ”The Battle of Britain” 1940, då RAF kämpade på gränsen för sina resurser. Jaktplanen hann möta bombarna i tid och de tyska bombplanen tvingades så småningom övergå till nattliga anfall med minskad precision för att undvika jakt.

Liknande radarkedjor byggdes upp i flera länder efter kriget. Det svenska systemet, Stril, började anläggas på 1950-talet. Det var redan från början samordnat med flygvapnet och anläggningen har moderniserats i flera steg. Det utgör f n en del av Flygvapen 2000.



Figur 4. Flygvapen 2000 är ett exempel på ett modernt militärt nätverk med radarsensorer, ledningscentraler, flygplan förenade av ett effektivt kommunikationssystem. I de telekrigförsök som utförts inom projektet ingick bl. a. StriC, ATK, FSR 890 Argus samt markradar.

Skälen till att välja luftbevakningsradar som exempel på sensorer i nätverk är många.

1. Det finns utbildad personal som kan samordna informationen.
2. Det svenska systemet Stril är väl utbyggt och har under senare år genomgått en omfattande revision.
3. I samband med denna revision infördes en simulator som ger goda möjligheter att prova telekrig i samverkan med utbildad personal.
4. Ett nätverk måste ha effektiva sensorer för att kunna ge användbar information. Radar har nästan fullständig täckning om analysen begränsas till luftmål.

Den varierande räckvidden och upplösningen hos radarstationer gör att de nästan alltid ingår i nätverk med flera olika system (Falk 2002). Två typiska fall är luftspaningsradar och luftvärnsradar som alltid innehåller flera typer av samverkande radarsensorer.

Spaningsradar

Spaningsradar för luftmål utnyttjar flera radarstationer med varierande räckvidd. Systemet består vanligen av ett radarkedja utplacerad längs nationsgränserna. Ett välkänt exempel är svenska Stril, där radarstationerna enklast ordnas efter avtagande räckvidd: PS 66, PS 860 och PS 870. Den flygburna PS 890 har egenskaper liknande PS 860 men är ytterst mobil och adaptiv till sin funktion.

PS 860 är utplacerad på centrala punkter i landet från norr till söder. PS 870 har låghöjdstäckning och är utplacerade i en kedja längs kusten, medan den flygburna PS 890 rör sig längs kusten ett stycke in i landet. Tillsamman bildar dessa radarstationer ett nätverk som täcker allt svenskt territorium och vars information analyseras i Stril.

Figur 5. Spaningsradar bildar ofta ett naturligt nätverk på grund av radarstationernas varierande räckvidd och täckning. Flera olika typer av sensorer används för att skapa en sammanhängande bild. Denna bild från flygutställningen i Moskva 2003 visar flera olika typer spaningsradar med varierande räckvidd och upplösning. Antennen i mitten använder metervågor och har flera hundra km räckvidd. Den omges av två antenner avsedda för kortare avstånd och med kapacitet för höjdmätning. Till vänster en spaningsradar för medelavstånd (cirka 50 km). I bakgrunden radar och avskjutningsramper för långdistansrobotar. (Foto: Lars Falk, FOI).

Luftvärn

Det viktigaste problemet för ett luftvärnssystem är att snabbt bestämma skjutriktningen. Radarstationerna bildar ett nätverk över ytan, där information från olika sensorer samordnas. Spaningsradarn lokaliserar inflygande mål och överlämnar avstånd och riktning till eldledningsradarn som följer målet till skott eller överlämnar målet till skyttar med optiska riktmedel.

Både vid radarspaning och luftvärn samverkar flera olika sensorer för att skapa en trolig omvärldsuppfattningen. Liknande mätningar kan utförss med optiska sensorer som har bättre upplösning än radar och överför mera data. Å andra sidan är informationen svårare att samordna på grund av rikedomen på detaljer. Det är lätt att maskera militär utrustning mot optisk insyn och det gör det naturligt att välja radar som ett inledande exempel på sensornätverk.

Figur 6. Inom luftvärnet kan information från olika sensorer i ett nätverk samordnas för att snabbt upptäcka inflygande mål från olika riktningar. Spaningsradarn till vänster mäter in mål, ofta efter anvisning från system med längre räckvidd. På några tiotals km avstånd överlämnas koordinaterna till eldledningsradarn till höger via kommunikationsantennerna. (Flygutställningen i Moskva 2003. Foto: Lars Falk, FOI).

I framtiden kommer de militära nätverken att bli alltmer omfattande. Improviserade nätverk skapas ofta under internationella uppdrag, men det är svårt att samordna den information som kommer från olika länders sensorer, vilket måste beaktas i analysen.

Den höga tillförlitligheten hos radar gör att ett nätverk av radarstationer lämpar sig väl för analys av hur moderna system påverkas av störning. StriC valdes som exempel, därför att nätverket utvecklats under många år och nyligen genomgått en omfattande revision. Bland annat har StriC fått god simulatorkapacitet som utnyttjades i praktiska försök.

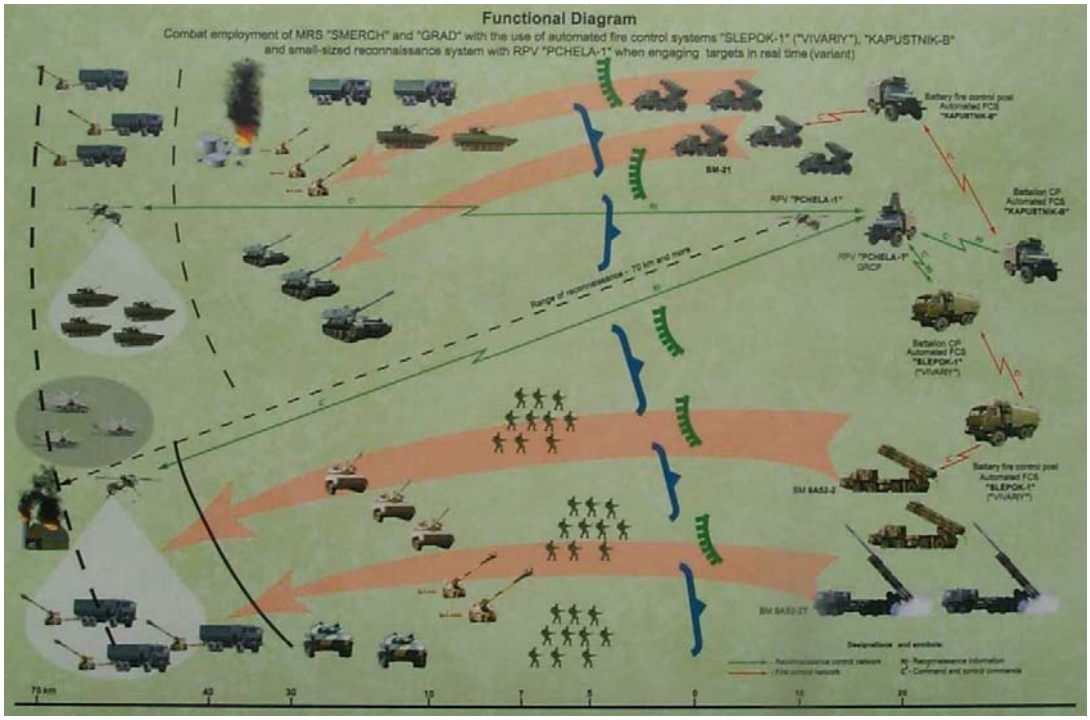
6.5 Nätverksbaserat försvar: NWC, NEC, NBF

Information från sensorerna samlas in av ett nätverk som måste kunna analysera och agera medan informationen är aktuell. Det ställer stora krav på organisationen och har lett till många diskussioner om hur doktriner för nätverksbaserat försvar bör formuleras.

Den svenska termen nätverksbaserat försvar (NBF) motsvaras i USA av Network Centric Warfare (NCW). I UK heter motsvarande koncept Network Enabling Capability (NEC). Terminologin varierar något i olika länder. Termen NCW används genomgående i USA,

medan NEC föredras i Europa, där man ofta uppgraderar befintliga system. Genom att tillföra datorer och pålitlig kommunikation kan man göra snabba vinster i effektivitet.

Termen nätverksbaserat försvar är nästan okänd i Ryssland, men det hindrar inte ryska militärer från att bygga om sina system på liknande sätt. Figuren visas ett artillerisystem utrustat med kontrollsystemet Kapustnik-B. Systemet ingår i ett nätverk med artillerilokaliseringsradar, optisk UAV, stabsfordon, chefsfordon och salvpjäser. Tiden till skott uppges ha reducerats med 90% med hjälp av nya datorer och kommunikation. Trots denna förbättring känner ryska militärer knappast till begreppet nätverksbaserat försvar, som författaren fann genom att fråga ut ett antal officerare under flygutställningen i Moskva 2005.



Figur 7. Ryskt artillerisystem med optisk UAV, artillerlokaliseringsradar, datainsamling och stabsfordon som samordnar den information som förmedlas till salvpjäserna. (Flygutställningen i Moskva 2003. Foto: Lars Falk, FOI).

Figur 8. Detaljer ur det ryska artillerisystemet i figur 7: UAV, stabsfordon och i bakgrunden en salvpjäs. UAV ”Pchela” är ett optiskt system utrustat med en TV-kamera vars data länkas till fordon. (Flygutställningen i Moskva 2003. Foto: Lars Falk, FOI).

7. OMVÄRLDSUPPFATTNING

Den som vill studera hur telekrig påverkar nätverksbaserat försvar måste i första hand undersöka hur ett modernt spanings- och ledningssystem fungerar under störda förhållande. Nätverk anses vara robusta och uthärdar olika former av störning, men för att undersöka problemet på ett realistiskt sätt måste man kartlägga egenskaperna hos ett militärt nätverk som innehåller både människor och sensorer.

Den tekniska informationen kan alltid beskrivas i matematiska termer. Många system automatiseras numera och gränsen mellan människa och maskin förskjuts högre uppåt i kedjan. Många uppgifter som tidigare sköttes av operatörer kan formuleras i tekniska termer och utföras av datorer med överlägsen precision och uthållighet. En typisk uppgift är att upptäcka mål, men det är svårare att beskriva den följande processen där målen identifieras och ofta utnyttjar man både människor och maskiner.

7.1 Mänsklig information

Militära användare utnyttjar nätverksbaserat försvar (NBF) för att bygga upp en tillförlitlig omvärldsuppfattning som är räcker för att lösa en given uppgift. Frågan är om man med telekrig kan påverka omvärldsuppfattningen så att besluten blir felaktiga eller omöjliga att genomföra.

Svaret beror på flera olika faktorer. De viktigaste är motståndarens avsikt, stridsteknik och informationsbehov, sensorernas prestanda och nätverkets struktur. Lyckligtvis kan man dra vissa allmänna slutsatser om vilka metoder som lämpar sig bäst för telekrig. Tidigare har man ofta använt energi i breda frekvensband för att dränka sensorerna i brus. Numera försöker man utnyttja energin för riktade angrepp mot specifika funktioner.

Det är fullt möjligt att formulera en teori för hur informationsflödet påverkar ett nätverk som består av människor och sensorer, fast mänskliga reaktioner är svåra att kartlägga (Klein 1998). Praktiska försök i befintliga system utförs i regel utan telekrig och det innebär att det är svårt att dra slutsatser ur experiment. För att kartlägga framtida hot är det bättre att utnyttja allmänna metoder och analysera nätverkets uppgift. Denna metod leder till en teori som kan användas för att överblicka tänkbara metoder och värdera deras effektivitet inbördes.

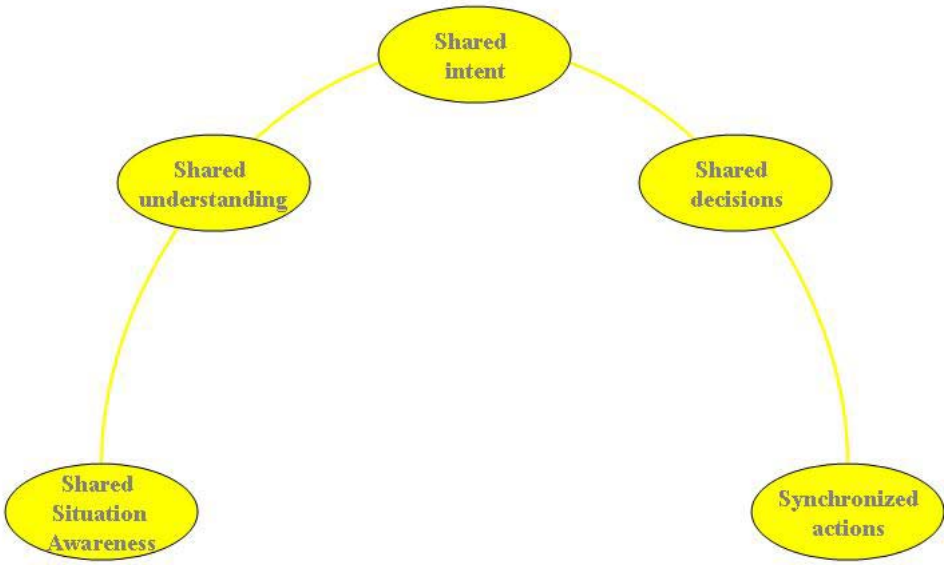
Teorin visar att all information, inklusive mänsklig kunskap, måste beskrivas i termer av sannolikhet. Det är en verklig utmaning att beskriva mänskliga operatörer i sådana begrepp med tanke på hur stor del av kunskapen som inte är explicit utan s k ”tyst kunskap”, som först demonstreras vid användning. Beteendevetarna har lagt ner stor möda på att beskriva mänsklig kunskap och jämföra den med representationer i datorer (Klein 1998, Essens 2003).

Det må vara svårt att sätta siffror på mänsklig kunskap, men problemet är lätt att beskriva. Dilemmat består i att kunskapen finns i två olika världar som i vardagslag beskrivs och analyseras med skilda språk. Interoperabilitet handlar inte längre om hur maskiner ska fungera tillsammans, utan om hur människor ska förstå varandra om begreppen inte kan samordnas.

Personalens uppgift är inte bara att skaffa sig en *gemensam lägesuppfattning* med hjälp av data från nätverket. Man ska också försöka komma fram till en *gemensam förståelse, en gemensam avsikt och gemensamma beslut*. Allt detta bör helst ske genom *synkroniserade insatser*, där det inte krävs explicita order för varje steg (Essens 2003).

För att skapa en gemensam utgångspunkt måste man använda begreppet sannolikhet, som kan användas för att beskriva kunskap hos både människor och maskiner (Jaynes 2003). Det återstår många steg innan en sådan beskrivning blir fullständig, men svårigheten är inte praktisk utan logisk. För att beräkna sannolikheter måste man först definiera ett rum av begrepp. Denna uppgift är inte särskilt besvärlig i ett radarnätverk, där det finns entydiga samband mellan sensordata och verkligheten med undantag för vissa tvetydigheter.

I andra fall är problemet svårare, t ex vid bildanalys och utfrågning av människor, där geometrin i det logiska rummet blir komplicerad. Sensorerna kan sällan leverera alla data som krävs för en fullständig bild på grund av logiska problem eller otillräcklig kapacitet (Kullback 1959, Jaynes 2003). De flesta sensorer ger mångtydiga data. Det innebär att användaren måste tolka de bilder han får av omvärlden. I den följande analysen förbigår vi sådana komplikationer och förutsätter att mängden data är tillräcklig för att definiera en entydig och korrekt omvärldsuppfattning, d v s nätverket är tillräckligt för sitt ändamål.



Figur 9. En sammanställning av de kognitiva funktioner som måste samordnas i ett nätverk av människor om de som grupp ska nå framgång. Det räcker inte att skapa en gemensam omvärldsuppfattning: man måste också uppnå gemensam förståelse och gemensamma avsikter för att komma till gemensamma beslut. Hela processen ska helst utformas genom synkroniserade insatser som inte kräver explicita order (Essens 2003).

7.2 Sannolikhet och risker

Det räcker inte att skapa gemensam uppfattning och synkroniserade insatser för att ett nätverk ska fungera framgångsrikt. Personalen måste också ha en gemensam uppfattning om vad som är möjligt att göra och vilka risker som är kopplade till olika alternativ. Detta faktum förbises i de analyser där man enbart inriktar sig på att skapa god omvärldsuppfattning.

Följande faktorer måste minst ingå i analysen.

1. Situationsuppfattning
2. Kunskapsläge
3. Handlingsplan
4. Strategiska mål

Ett historiskt exempel visar hur dessa faktorer kan spela in i en militär analys.

7.3 Skagerackslaget 1916

Första världskriget framstår ofta som oundvikligt på grund av rivaliteten mellan stormakterna, allianssystemet och den militära upprustningen kring sekelskiftet. Upprustningen var mest framträdande inom marinen och många hade väntat att kriget skulle avgöras till sjöss.

I själva verket utkämpades ett enda större slag till sjöss. Kriget avgjordes på de platser där det gavs tillfälle till utnötning. I skyttegravarna var förlusterna så förutsägbara att man nästan deterministiskt kunde beräkna hur stora förluster skulle bli för given insats. U-båtskriget fick en liknande karaktär och var ytterst framgångsrikt, eftersom det var riskabelt att strida på ytan.

Skeppsartilleriet och torpederna hade blivit så effektiva att flottorna undvek öppen strid, liksom rovdjur och kärnvapenmakter brukar göra. Man nöjde sig med att bevaka varandra, en taktik som används även i insatser med lägre intensitet. Om man inte av politiska skäl kan acceptera förluster måste man begränsa riskerna, trots att sannolikheten är liten.

Dessa överväganden visar att man måste tänka i termer av *sannolikhet* för att analysera utgången i sådana fall. Eftersom det inte finns ett klart definierat utfall måste man räkna igenom alla möjligheter. Detta var välkänt inom marinen långt före första världskriget. Den ryska östersjöflottan hade förintats på några timmar vid Tsushima-sundet. Fartygen var hotade av skeppsartilleri och torpeder, eftersom sikten var fri ända till horisonten. Fartygen var dessutom utrustade radio och optisk signalering för effektiv kommunikation. Många av de faktorer som kännetecknar moderna nätverk fanns alltså i stormaktsflottorna redan för hundra år sedan.

De tekniska framstegen tvingade fram nya typer av fartyg och man analyserade ingående duellen mellan pansar och artilleri. Besättningarna var väl övade i konsten att sänka fartyg, sedan stormakterna tagit lärdom av de fiaskon som noterats under det spansk-amerikanska kriget 1898 (Hughes 1986).

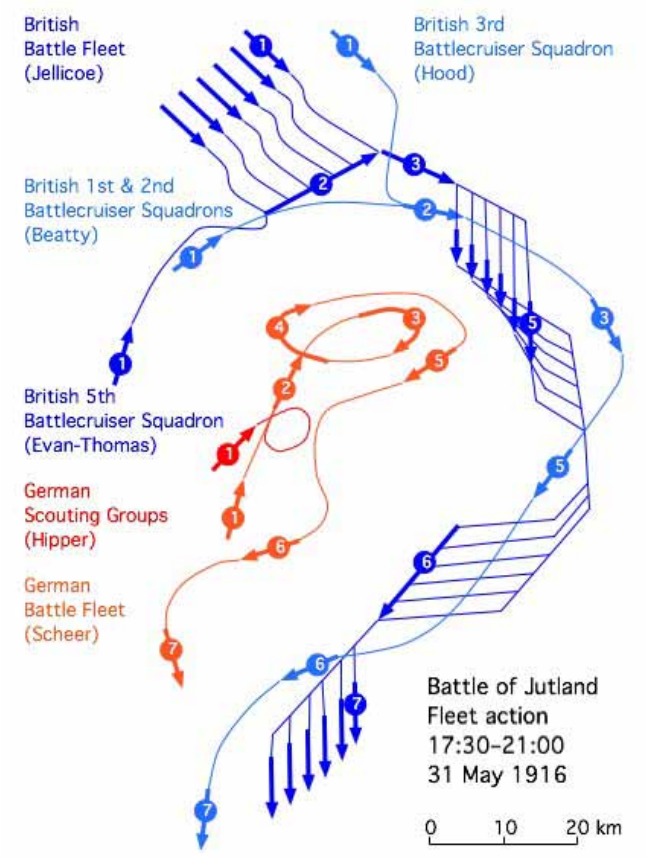
Dessa insikter ledde paradoxalt nog till att ett enda större sjöslaget utkämpades under första världskriget. Det inträffade den 31 maj 1916 och kallas Skagerackslaget eller ”The Battle of Jutland”. Krigshistorikerna brukar påstå att slaget slutade oavgjort, men båda sidor led enorma förluster. Under en enda dags strider förlorade tyskarna elva större fartyg och engelsmännen femton, vilket var cirka 10% av numerären, eftersom den engelska flottan var 50% större.

Ingendera parten kunde uthärda sådana förluster under någon längre tid. Även om tyskarna firade utgången som en seger tvingades den tyske befälhavaren von Scheer återvända till Wilhelmshafen, där Hochseeflotte förblev liggande under krigets slut. I England var besvikelsen stor över att slaget inte blivit ett nytt Trafalgar. Den brittiska flottan antogs vara överlägsen alla andra nationers (”We’ve got the ships, we’ve got the men, we’ve got the money too”), men inom marinen visste man hur riskabel sjöstrid är. Den brittiske befälhavaren Jellicoe fick utstå mycket kritik och ersattes av Beatty, men åsikterna har gradvis förändrats. Jellicoes bedömning beskrivs i Svensk Uppslagsbok (1950) som motiverad och numera anser de flesta handböcker att han handlade rätt (Hughes 1986).

Hur kan man förklara så stora skillnader? Tidiga bedömare insåg inte betydelsen av sensorer och kommunikation utan såg enbart till eldkraften, men en sådan analys blir tvivelaktig om man försummar den statistiska aspekten. Det kunde räcka med en träff för att sänka ett fartyg. Alla officerarna visste att ett övertag i fartyg och eldkraft snabbt gav utslag till sjöss och just detta faktum tycks ha bromsat Jellicoe att döma av hans egen rapport.

”At 9 p.m. the enemy was entirely out of sight, and the threat of torpedo-boat destroyer attacks during the rapidly approaching darkness made it necessary for me to dispose the fleet for the night, with a view to its safety from such attacks, whilst providing for a renewal of action at daylight.”

Den engelska marinen hade via signalspaningen fått förvarning om att den tyska flottan var på väg ut och lade sig i bakhåll med hela huvudstyrkan i Scapa Flow. I sista stund lyckades von Hipper genom ett spektakulärt anfall med sina jagare hejda den engelska huvudstyrkan från att skära av reträtten. Den tyska huvudstyrkan kunde slutligen föras i hamn i skydd av rök och mörker.



Figur 10. Skagerackslaget 1916. Den engelska huvudstyrkan under Jellicoe anlände sent på eftermiddagen efter en inledande strid mellan Beattys och von Hippers jagare. Jellicoe hotade att ta sig runt den tyska flottan och blockera vägen tillbaka till Wilhelmshafen. I detta läge gick von Hippers jagare till angrepp och lyckades hejda rörelsen så att von Scheer i skydd av mörkret kunde föra den tyska huvudstyrkan i hamn.

Det räcker att studera den information Jellicoe hade till sitt förfogande för att förstå vilka bedömanden som avgjorde att han inte gav sig in i striden. Alla dessa faktorer innehåller någon form av risk och visar tydligt betydelsen av sannolikheter vid en samlad bedömning. Lägg märke till att det lägre befälet var mindre intresserade av flottans strategiska uppgift och förordade anfall under de oklara förutsättningar som rådde på kvällen den 31 maj 1916.

Situationsuppfattning: Jellicoe hade tillgång till radio och optisk signalering, men informationen var bristfällig. Stora mängder rök uppstod när fartyg efter fartyg exploderade. Beskjutningen mellan fartyg började på 15 km avstånd och kunde ge snabbt resultat. En viktig faktor visade sig vara om motståndaren syntes i väster mot den nedgående solen.

Kunskapsläge: Jellicoe visste efter tidigare skärmytslingar att de tyska fartygen och besättningarna var minst jämbördiga med de engelska, men han kunde inte medge det officiellt. Det rådde stor osäkerhet om hur flottornas artilleri och pansar skulle hävda sig i en duell. Under striden visade sig de engelska fartygen ha en fatal svaghet: ammunitionen lagrades ofta nära kanonerna och det kunde räcka med en träff för att sänka ett fartyg.

Handlingsplan: Båda flottorna var välträna de och beskjutningen effektiv. De övergick i strid till linjeformering som traditionen krävde. Det visade sig senare att denna formering var känslig för massanfall med torpeder som amerikanarna fick erfara under striderna i Stilla havet 1941-42 (Hughes 1986).

Strategiska mål: Tyskland hade byggt upp sin flotta för att kunna konkurrera med England på världshaven. Englands mål var att alltid behålla ett övertag mot Tyskland.

Den sista faktorn var förmodligen avgörande för Jellicoes beslut jämte insikten om hur osäker hans omvärldsuppfattning var. Om den engelska flottan gick under var kriget förlorat. Tyskland ville gärna bryta blockaden, men kunde trots allt föra strid i Frankrike. Resultatet var att flottan blev liggande overksam i Wilhelmshafen till krigets slut 1918.

Jellicoe kan inte ha bedömt dessa sannolikheter exakt, men han insåg utan tvivel att det fanns en risk att hela flottan skulle gå under, trots sitt numerära övertag. Det kunde räcka med en fluktuation någonstans ute på havet för att tyskarna skulle få ett övertag och slå ut sina motståndare. Flera episoder under striden visade hur snabbt det gick att sänka en motståndare om man tillfälligt kom i överläge.

Efter slaget påpekade Churchill att Jellicoe "was the only man who could have lost the war in an afternoon." Churchill hade som marinminister samarbetat med Jellicoe och var äl medveten om de strategiska och politiska målen. Hans eget fall vållades av invasionen på Gallipoli 1915 och han visste hur ofta militära och politiska frågor styrs av slumpen. Churchill sammanfattade på ett utmärkt sätt sin insikt om hur viktigt det är att tillämpa sannolikhetens lagar på den information som finns tillgänglig i osäker form.

"True genius resides in the capacity for the evaluation of uncertain, hazardous, and conflicting information." (W. S. Churchill)

7.4 Sannolikheter

Föregående exempel leder till en viktig slutsats. Utgången av en konflikt styrs av de sannolikheter som representerar omvärldsuppfattningen men också av de sannolikheter som representerar vapeninsatsen. Teorin visar att dessa faktorer bara kan skiljas tydligt åt i sannolikhetsteorin. Detta faktum upptäckte bland annat Wald, när han härledde reglerna för beslutsteori omkring 1950 (Jaynes 2003).

Sannolikhetsteorin har fördelen att den skapar en tydlig uppdelning mellan uppgiften att producera en omvärldsuppfattning och att bestämma hur resurser och kunskaper ska utnyttjas. Omvärldsuppfattningen kan bara utformas separat om alla parametrar beskrivs med sannolikheter. Det är alltså nödvändigt att värdera sensorinformation och mänsklig kunskap tillsammans. Det är en besvärlig uppgift i många situationer, men relativt lätt för radarsensorer, som genererar få och tämligen entydiga parametrar som avstånd, riktning och radiell hastighet.

Den teori som används måste uppfylla två krav, som beskriver vår grundläggande syn på information som en tillgång som ska användas rationellt och inte får kastas bort.

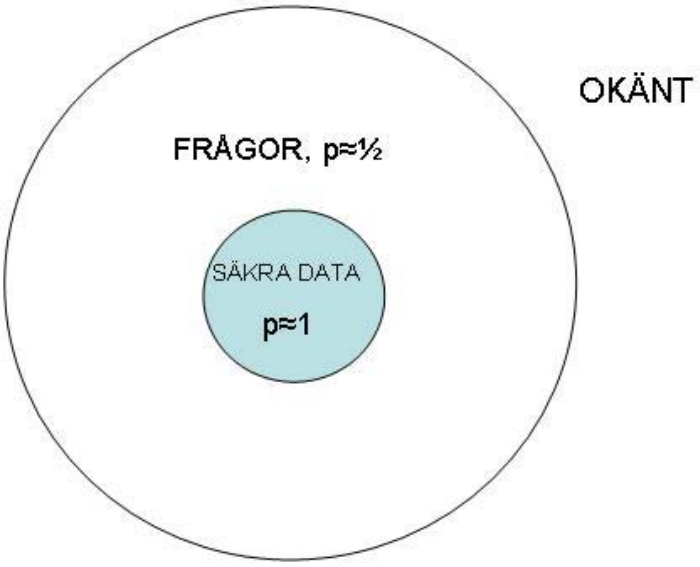
1) Information får bara användas en gång;
2) Argument ska kunna presenteras i godtycklig ordning.

Dessa båda krav leder till en formalism som genererar optimala slutsatser ur tillgänglig information (Falk 2004). Teorin avgränsar också vad som menas med ”information” och denna definition stämmer med Shannons beskrivning av teknisk information. Det är en definition som kan vara svår att tillämpa, men garanterar en optimal omvärldsuppfattning om all sensorinformation och mänsklig kunskap utnyttjas rätt (Jaynes 2003).

Denna beskrivning har stora teoretiska fördelar men är rätt komplicerad. Framför allt kräver teorin att alla beskrivningar är logiskt konsistenta. Det ställer stora krav på den analys som ska leda fram till en korrekt omvärldsuppfattning. Det finns givetvis approximationer som förenklar beräkningarna och leder till snabba insikter. I denna rapport används modellen främst för att dra allmänna slutsatser om hur telekrig mot nätverk bör utformas. För det ändamålet räcker det att visa hur informationen utnyttjas i ett nätverk av sensorer.

8. TELEKRIG MOT SENSORNÄTVERK

Den sannolikhetsmodell som beskrivits ovan ger en konceptuell bild av hur kunskap registreras i ett nätverk av sensorer. Figur 11 ger en schematisk bild av hur kunskapen samlas in, men kan inte återge den komplexitet i geometrin som kännetecknar data om man tar hänsyn till inbördes relationer (Kullback 1958). Radar är ett enkelt exempel, därför att det finns en nästan entydig koppling mellan data och verklighet frånsett vissa kända tvetydigheter. Andra typer av sensorer är mycket svårare att tolka, t ex optiska bilder.



Figur 11. En allmän beskrivning av kunskap i ett nätverk där kommunikation mellan noderna inte utgör en väsentlig begränsning. Vissa frågor har fått säkra svar (sannolikhet nära 1), medan andra är obesvarade (sannolikhet omkring 0.5). Utanför systemet finns okända fakta som tillgängliga sensorer inte kommer åt.

Detta sätt att åskådliggöra ett nätverk beskriver rätt väl moderna radarsystem. Datorerna sköter tröskelsättningen och det finns logik som sorterar målen om de kommer nära varandra (Griffiths 2003). Ett registrerat mål visas på skärmen först när sannolikheten för upptäckt närmar sig 100%. Identifiering kräver tillskott av mänsklig kunskap. I dessa processer får begreppen ”anpassat filter” och ”tröskelsättning” en ny innebörd och blandar information från människor och maskiner i samma språkbruk (Hyberg 2005).

De olika metoderna för telekrig mot nätverk kan klassificeras efter hur stor förmåga nätverket har att samla in och bearbeta information. Alla sensorer och beslutsfattare är utrustade med filter som sorterar bort felaktiga signaler. En radar är utrustad med filter som är anpassade till radarns egen signal. Ett sådant anpassat filter (matched filter) släpper igenom mest energi när den ser radarns utsända puls .

Härledningen av formeln för ett anpassat filter kräver stort utrymme i många radarböcker. Det är ett bevis för styrkan i informationsteorin att motsvarande uttryck kan härledas på några rader om man börjar från informationsteorin (Jaynes 2003). Mänsklig kunskap behöver inte beskrivas med sannolikheter i detta fall, eftersom människan uppträder separat efter maskinen och löser sin egen uppgift. Ett falskt mål blir trovärdigt först då det registrerats och accepterats både av maskiner och människor.

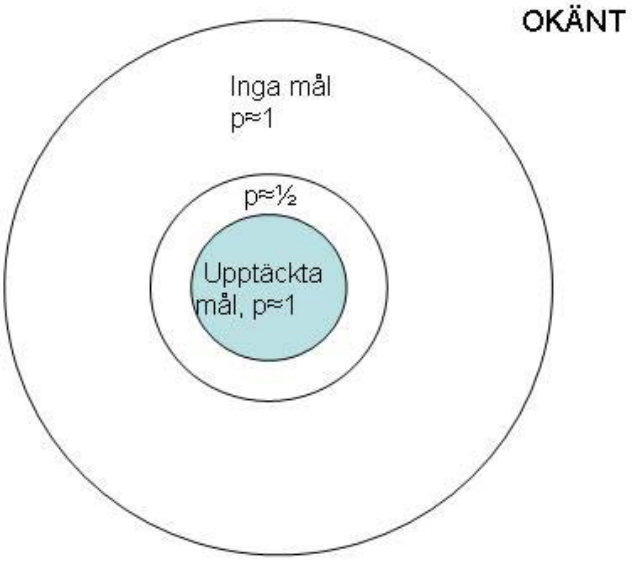
8.1Skenmål

Det anpassade filtret anger hur ett falskt mål måste se ut för att accepteras av sensorn och bli ett trovärdigt *skenmål*. En viktig slutsats är att falska mål bör presenteras för de sensorer som är mest trovärdiga för att påverka systemet. Denna slutsats kan kvantifieras och tillämpades i försöken på StriC (Hyberg, Falk och Malm, 2005).

Följande bild visar schematiskt hur sannolikheten är fördelad i ett nätverk av radarsensorer avsett för spaning. Nätverket är vanligen organiserat så att det täcker en stor volym kring radarn, men analysen förutsätter att nästan alla celler är tomma. Systemet kan hantera ett stort antal upptäckta och identifierade mål som visas upp för operatörerna, men klarar bara av ett litet antal oklara företag som sysselsätter nästan hela personalen i pressade situationer.

Detta förhållande öppnar intressanta möjligheter för telekrig. Informationsrummet är uppdelat i volymer av helt olika storlek. Figuren avbildar geometrin på ett schematiskt sätt eftersom det bara är volymerna som är viktiga. Följande siffror är typiska för de mål som kan hanteras.

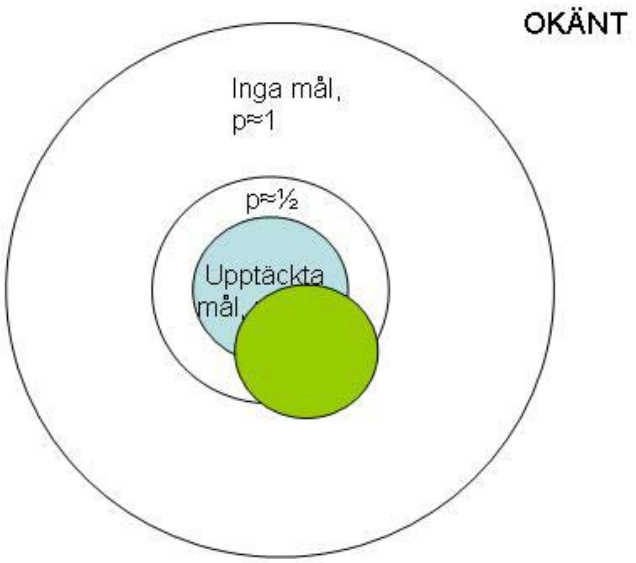
Luckor/svep: >1 000 000
Antal accepterade mål: <10 000
Mål som kan analyseras: <100



Figur 12. En allmän beskrivning av kunskap i ett system för bevakning av luftrum. I de flesta upplösningsceller finns inga mål, medan ett måttligt antal mål kan noteras som identifierade med säkerhet. Ett litet antal mål är tveksamma eller oidentifierade och sysselsätter nästan hela personalen.

8.2 Brusstörning

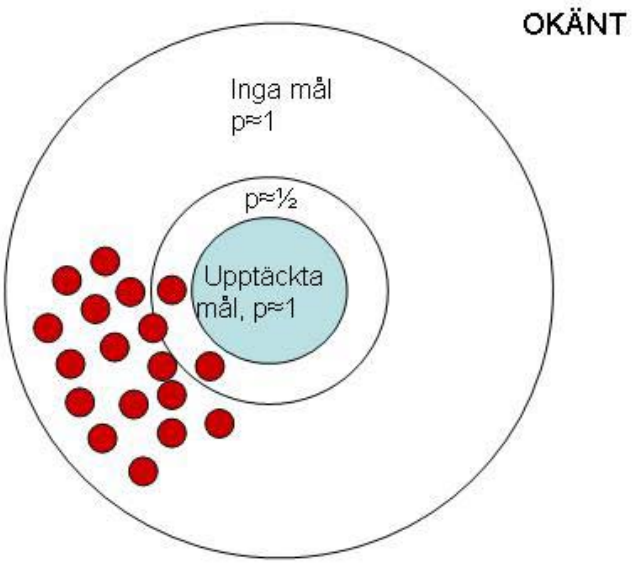
Med utgångspunkt från denna bild av aktiviteten i ett radarnätverk kan man klassificera olika metoder för telekrig beroende på hur informationsflödet påverkas. Den traditionella metoden är att tillföra brus och remsor för att blockera insyn i ett område där egna flygplan uppträder. Metoden har nackdelen att den röjer att ett företag är på väg och den är kostsam, om man som USA stöder alla flyganfall med bakgrundsstörare på stora avstånd bakom attackflygplanen.



Figur 13. Den traditionella metoden för att störa bevakning av luftrum. Ett visst antal mål är upptäckta men identifiering och följning i detta område hindras genom att man blockerar sensorerna med remsor och brus. Nackdelen är att det syns att ett företag är på väg. Insatsen bör helst kompletteras med skeninsatser på annat håll för att öka osäkerheten om vad som sker.

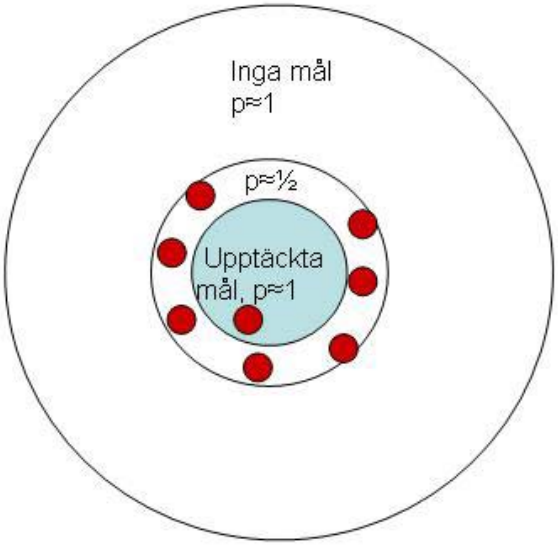
8.3 Mättning med falska mål

Diagrammen visar att det är mer lönande att agera mot de stora områden som nätverket anser vara fria från mål. Det sker genom att man skapar skenmål som antingen mättar sensorerna eller länkarna från radarstationerna. För detta ändamål räcker det att skenmålen passerar det anpassade filtret i radarmottagaren. Det är lätt att producera tusentals trovärdig mål genom att repetera radarns egen signal som alltid passerar det anpassade filtret. På detta sätt kan man mätta sensorn eller ledningen till gruppcentraler.



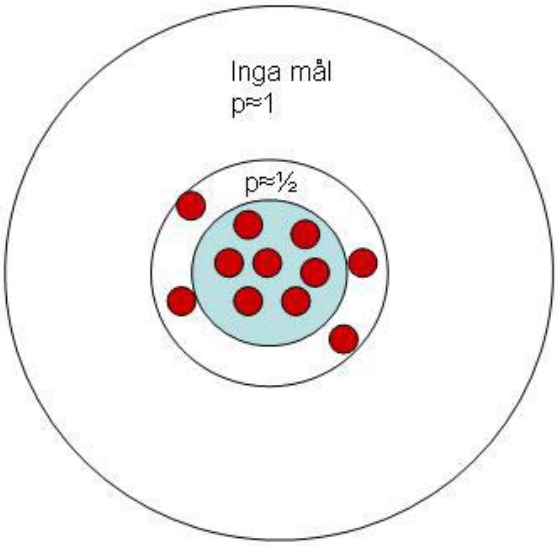
Figur 14. En modern metod för att störa luftbevakningssystem är att lägga ut skenmål som mättar sensorerna. Insatsen döljer inte egna företag men fördröjer upptäckten.

Tidigare var länkarna en flaskhals i militära nätverk, men de håller på att ersättas med bredbandiga länkar. Det kan vara bättre att angripa beslutsfunktionen direkt i stället för sensorerna om deras data kompletteras med andra sensorer i nätverket. Figur 15 visar hur det kan gå till. Man skapar skenmål som sysselsätter beslutsprocessen genom att åstadkomma signaler som passerar radarns anpassade filter och är tillräckligt trovärdiga för att försena operatörerna. Det är möjligt att producera hundratals skenmål som mättar beslutsprocessen. Dessa mål ska vara trovärdiga men samtidigt tvinga operatörerna till ständigt nya insatser. Antalet mål bestäms av operatörernas utbildning och kapacitet.



Figur 15. För att störa luftbevakningen kan man i framtiden lägga ut skenmål som registreras av personalen och mättar beslutsprocessen. Insatsen gör att upptäckt av andra företag fördröjs.

Ett intressant alternativ till mättning är att vilseleda militära nätverk med skenmål som passerar beslutsprocessen. Signalerna måste passera alla anpassade filter inklusive människan och alltså vara tillräckligt trovärdiga för att under viss tid accepteras av mänskliga operatörer. Vilseledningen skapar en falsk omvärldsuppfattning som leder till felaktiga beslut. Vilseledning är en mycket omskriven metod i krigshistorien, men har inte praktiserats så ofta som det ibland påstås, eftersom metoden kräver kunskap om motståndarens vetande (Falk 2005).



Figur 16. Vilseledning av nätverk för luftbevakning kan ske genom att man lägger ut skenmål som accepteras av personalen och försvårar beslutsprocessen.

9. VILSELEDNING

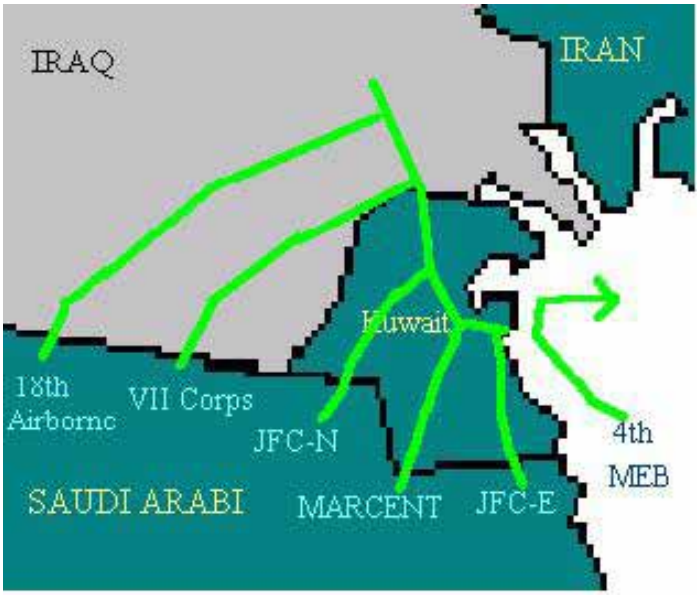
"Allt krig bygger på vilseledning" skriver Sun Tzu. Vilseledningen är en högt skattad metod i Orienten, men ställer stora krav på en exakt insats. Metoden fordrar god insyn i motståndarens tankesätt. I väst har man satsat mer på stridssätt som bygger på koncentration av trupper och kräver mindre detaljerad kunskap om motståndaren (Falk 2004).

Vilseledning är intressant därför att metoden tvingar båda parter att jämföra och värdera sina omvärldsuppfattningar. Analysen visar att vilseledning är särskilt effektiv om nätverkens omvärldsuppfattning anses pålitlig.

Vilseledning går ut på att skapa trovärdiga alternativ. Med telekrig kan man skapa kaos och generera en osäker omvärldsuppfattning, men det är bättre att låsa motståndaren vid felaktiga alternativ genom vilseledning. Metoden fungerar bäst under en lång uppladdning, där man kan inrikta all information på en sådan uppgift. Vilseledning används därför helst i militära operationer där det är gott om tid. Metoden är kostnadseffektiv men fordrar omsorgsfulla förberedelser. Traditionellt har vilseledning använts mest vid överraskande anfall och efter långa förberedelser i ett låst läge (Ulfving 2000; Falk 2005).

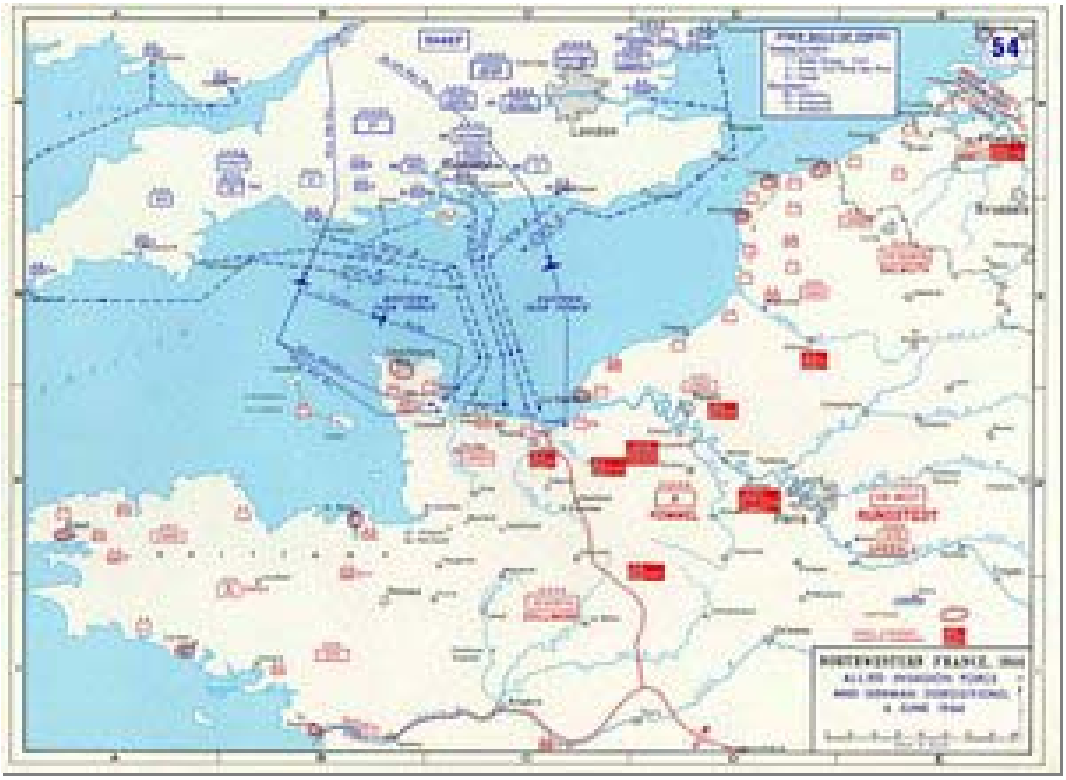
Den 24 februari 1991 avgjordes Gulfkriget genom ett anfall mot Kuwait och Irak. Kriget var över på några dagar med obetydliga förluster. Till denna utgång bidrog en vilseledande

manöver som utfördes av amerikanska marinkåren i Persiska viken. Ett skenanfall inleddes mot kusten och band tio irakiska divisioner till försvaret trots att någon landstigning aldrig ägde rum. Det var prövande för marinkåren att stå utanför striderna, men operationen väckte allmän beundran. Fientlig trupp bands till låga kostnader vid uppgifter som aldrig förverkligades.



Figur 17. Angreppet mot Kuwait den 24 februari 1991 innefattade en vilseledande manöver av marinkåren från Persiska Viken som band tio irakiska divisioner till försvaret.

Det mest berömda exempel på vilseledning är fortfarande D-dagen, den 6 juni 1944. Tyskarna trodde i det längsta att invasionen skulle äga rum över Engelska kanalen vid Calais. Genom att på olika sätt bekräfta denna teori lyckades de allierade fördröja den tyska motoffensiven. En tysk pansardivision blev stående overksam nära Paris under landstigningen i Normandie. Bland vilseledningsåtgärderna märktes hundratals fartyg med radarreflektorer som gick ut i Engelska kanalen och skapade intryck av en invasion. Rykten spreds ut om att en ny armékår bildats i England med general Patton som befälhavare. Dechiffreringen av meddelanden från chiffermaskinen Enigma var viktig för att verifiera att vilseledningen fungerade (Winterbotham 1977).



Figur 18. Invasionen i Normandie den 6 juni 1944 föregicks av flera vilseledande åtgärder som band tyskarna vid försvaret av Calais som i det längsta ansågs vara huvudmåletet.

Effekten av en lyckad vilseledning är så spektakulär att dess betydelse ofta övervärderas. Det finns i själva verket få fall av lyckade vilseledningar i krigshistorien beroende på att kraven på ledning är så höga (Falk 2005).

I moderna termer är vilseledning ett sätt att förändra motståndarens omvärldsuppfattning, så att ett falskt alternativ bedöms som verkligt. Det är viktigt att verifiera att denna form av vilseledning lyckas. Detta är lättast under statiska förhållanden, t ex i början av ett krig som vid Pearl Harbour eller efter långvariga förberedelser med ständig kontroll av motståndarens omvärldsuppfattning som vid Stalingrad och inför D-dagen.

Vilseledning kräver noggranna förberedelser, men det krävs också god kontroll över egen trupp för att genomföra vilseledningen och kunna utnyttja förvirringen. Det innebär att en rad villkor måste vara uppfyllda för att vilseledning ska lyckas.

1. God disciplin
2. Kunskap om motståndarens taktik
3. God underrättelsetjänst
4. Noggrann planering och kvantitativ utvärdering av effekten
5. Möjlighet att verifiera effekten

Slutsatsen blir att klassisk vilseledning fungerar bäst på politisk, strategisk och operativ nivå och det bekräftas av den krigshistoriska erfarenheten (Ulfving 2000). Men slutsatsen modifieras på ett väsentligt sätt i framtida telekrig (Falk 2005).

Orsakerna är flera:

1. Fientliga signaler har blivit lättare att mäta.
2. Kostnaden är måttlig och därmed minskar risken.
3. Motståndarens reaktion kan testas genom signalspaning och skenanfall.

Slutsatsen blir att elektronisk vilseledning är en lovande metod för telekrig när nätverk står för omvärldsuppfattningen. Vilseledning kan sättas in på taktisk nivå, där man av tradition bara använder elektronisk vilseledning i rena duellsituationer, som är högst automatiserade processer (de Arcangelis 1985; Woodward 1994).

Med datoriserade nätverk av sensorer är det fullt möjligt att snabbt genomföra elektronisk vilseledning om man har bättre omvärldsuppfattning än motståndaren. Snabbheten och precisionen i moderna nätverk är den egenskap som gör att vilseledning kan föras in på taktisk nivå (Falk 2005).

Elektroniska signaler är lätta att kontrollera jämfört med de metoder som tidigare använts för militär vilseledning (Ulfing 2000). I en elektronisk värld kan man ofta av signalernas karaktär avgöra om vilseledningen lyckats. Operationen i Beqaadalen 1982 är ett klassiskt exempel (de Arcangelis 1985). Ett stort antal syriska luftvärnssystem och mängder med jaktflygplan slogs ut, sedan de syriska radarstationerna lockats att belysa skenmål och röja sina positioner. Därpå följde flera vågor av samordnade angrepp mot radarstationer och luftvärn och mot de jaktflygplan som ingrep. Operationen blev särskilt effektivt genom att man kartlagt beslutsprocesserna hos de syriska trupperna som följde det sovjetiska reglementet.

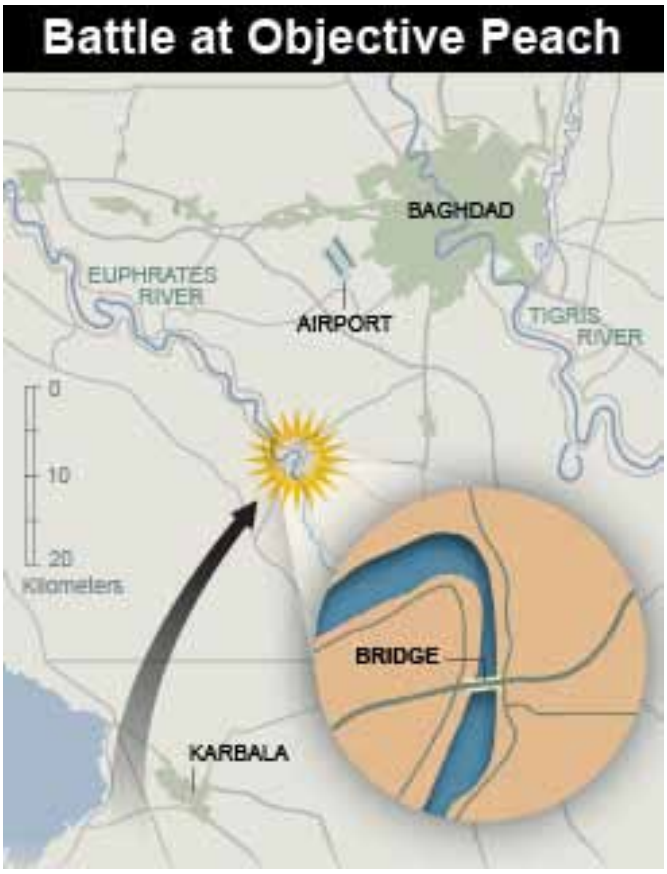
Operationen i Beqaadalen krävde lång planering. Den föregående analysen visar att moderna nätverk kan värdera lägen snabbt och effektivt, så att tiden är mogen för elektronisk vilseledning på taktisk nivå. Analysen visar att det kan ske i form av snabba elektroniska attacker riktade mot beslutsprocesserna i ett nätverk av sensorer.

10. NÄTVERKENS BEGRÄNSNINGAR

Ett varningens ord är på sin plats när det gäller nätverk. Det är farligt att övervärdera den information som sensorerna i ett nätverk erbjuder. Resultatet beror trots allt på sensorernas kvalitet och man måste alltid försöka beakta vad man *inte vet* om läget.

Den 3 mars 2003 anföll amerikanska styrkor en bro över Eufrat nära Bagdads flygplats, ”Objective Peach”. Det borde ha funnits en irakisk försvarsstyrka på plats, men trots upprepade frågor blev svaret att det inte fanns någon trupp i närheten. I själva verket missade de optiska sensorerna 8 000 irakiska soldater och över 70 stridsfordon i en by i närheten.

Den följande striden avgjordes genom de amerikanska stridsvagnarnas överlägsenhet, men det följde en förbittrad diskussion om kvaliteten på sensorerna och analysen i nätverket. En bidragande orsak till förvirringen var överdriven tilltro till systemet. Nätverket gav exakta upplysningar om egna fordons positioner (”blue force tracking”) och det skapade föreställningen att det fanns liknande kunskap om irakiska fordon. De stod i många fall gömda under kamouflage och visade sig svåra att hitta med optiska metoder så att man kunde forma en gemensam helhetsbild.



Figur 19. Striden vid Objetive Peach den 3 mars 2003 blev en obehaglig överraskning för amerikanerna, sedan de luftburna sensorerna missat den irakiska styrkan nära bron.

11. SLUTSATSER

Analysen leder fram till några allmänna slutsatser om hur telekrig mot NBF bör bedrivas.

1. Sannolikheter ger en användbar modell av nätverk av sensorer och människor.
2. Nya metoder för telekrig bör riktas mot beslutsfunktionen genom repeterstörning, mättning och vilseledning.
3. Elektronisk vilseledning kan i framtiden användas också på taktisk nivå.
4. Bästa skyddet mot telekrig är en god teori och systematisk träning av operatörerna.

Försöken på StriC utnyttjade den sensor som personalen för ögonblicket litade mest på (Hyber, Falk och Malm, 2005). Det är viktigt att försöken fortsätter för att man ska vinna erfarenhet av hur simuleringar bör genomföras för att bli ett pedagogiskt hjälpmedel. Liknande försök bör utföras under NBF-försöken vid LedSystM.

12. ERKÄNNANDE

Per Hyberg har bidragit med inspirerande diskussioner. Vi vill båda tacka Olle Malm, Mikael Nordström och Michael Herre vid StriC i Uppsala för värdefulla synpunkter på hur simuleringar av telekrig kan genomföras.

13. REFERENSER

[1.] Mario de Arcangelis: Electronic warfare. From the battle of Tsushima to the Falklands and Lebanon conflicts (Blandford, Poole 1985).

[2.] Peter Essens, Ad Vogelaar, Erlan Tanercan, Donna Winslow: The Human in Command (2003).

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

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

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

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

[7.] Lars Falk: "Kvantitativa beslut i nätverksbaserat försvar", FOI-R--1390, november 2004.

[8.] Lars Falk: "The Benefits of Deception", MilTech 2 Conference, Stockholm 25-26 October 2005, pp.101-108. (FOI-S--1838--SE)

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

[10.] Lars Falk and Per Hyberg: "Electronic warfare against a network of sensors." RadioVetenskap och Kommunikation, RVK 05, Linköping, juni 2005, sid. 515-520.

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

[12.] Wayne P. Hughes: Fleet tactics: Theory and Practice. (Naval Institute Press, 1986).

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

[14.] Per Hyberg, "Shannon and Centric Network, Stockholm 1st Conference on Military Technology, Stockholm 2003.

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

[16.] Per Hyberg: "Vilseledning av beslutsfunktioner baserade på sekundärradar", FOI-R—1722-SE, september 2005.

[17.] Per Hyberg: "Telekrig mot NBF, resultatöversikt: Informationsteoretisk grund med luftförsvarsexempel", FOI-R—1802-SE, december 2005.

[18.] Per Hyberg: "Network Centric Warfare and Information Theory", Journal of Electronic Defense, Vol. 28, No 12, December 2005

[19.] Per Hyberg, Lars Falk, Olle Malm: "Försök med störning av beslutsfunktioner baserade på sekundär Stril-radar", FOI-RH—0471-SE, december 2005.

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

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

[22.] S. Kullback: Information theory and statistics (John Wiley and Sons 1959).
[23.] Lars Ulfving: Den stora maskeraden – Sovjetrysk militär vilseledning (Försvarshögskolan, Stockholm, 2000).
[24.] F. W. Winterbotham: Operation Ultra (Prisma 1977).
[25.] S. Woodward: Ett hundra dagar. Striden om Falklandsöarna. (Marinlitteraturföreningen nr 77, 1994).