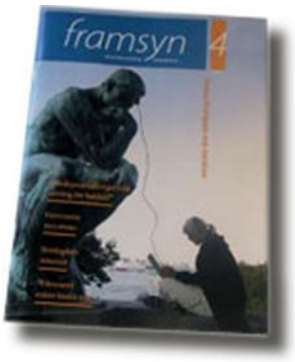
Framsyn Nr 4 2004



Nr 4 Kampen om tanken

”Skapa förvirring i fiendens huvuden”

Katten leker med musen. Katten släpper musen som tror att den är fri. Så fångas musen in gång på gång och när inget annat återstår spelar musen död i hopp om att katten är mer uttråkad än hungrig.

I naturen och i krig har detta spel alltid pågått. Lejonet ryter för att injaga skräck. Fältherren luras genom att visa sig svagare än vad han är och få motståndaren att gå i en fälla. Eller han kan ge sken av att ha en styrka som han inte har i hopp om att undvika strid.

”För att vinna måste vi sluta fiendens ögon och öron och göra honom blind och döv. Vi ska skapa förvirring i huvudena på fiendens befälhavare och driva dem till vansinne.” Så beskrev Mao Zedong vägen till seger 1938.

Ytterst handlar det om att få en mottagare att ta till sig ett budskap och agera på det sätt som sändaren vill. Det kan vara musen som försöker lura katten, generalen på slagfältet eller reklammakaren som vill sälja en vara. Det kan göras på olika sätt bara. Det viktiga är att budskapet går hem. Mottagaren måste känna igen budskapet. Katten vet hur tråkigt det är när musen dör. Då är leken slut.

Det är inget konstigt med det här, säger Håkan Gustafsson vid Högkvarteret som arbetar med vad som idag kallas informationsoperationer. Området har länge varit snårigt. Flygblad har blandats med telekrig och hackers. Nu håller försvaret på att reda ut begreppen och ska gå vidare på den fjärde arenan - informationsarenan. På denna arena används mjuka och hårda verktyg och det är kombinationen som ger förstärkningen. Under den första Irakkriget blandades flygblad med bombmattor och det fick irakierna att ge upp i massor.

I den nya världen kan angreppet komma på informationsarenan. En gång skulle vi försvara oss mot storinvasionen. Hur bra är vårt försvar mot det nya hotet? Mats Ekdahl, mångårig publicist i ledande befattningar och nu chef för Styrelsen för psykologiskt försvar, skriver att ”ur en totalförsvarsaspekt är det moderna mediasamhället den perfekta terrängen för informationspsykologiska bakhåll”. Det är till stor del media som ger oss en bild av verkligheten. Mats Ekdahl påpekar att om allt fler människors verklighetsbild formas av krafter från underhållning, lobbying och propaganda så blir det brister i den medborgerliga kunskaps- och idébildningen.

Kampen om tanken förs nu med nya och effektivare medel. Informationssamhällets genombrott gör att nya opinioner sprids blixtsnabbt över hela jorden. Amatörbilderna från det amerikanska fängelset i Irak fick ett omedelbart genomslag. Tekniken gjorde att bilderna skadade USA mer än många bilbomber tillsammans.

I detta nummer av Framsyn gör vi ett försök att visa både de mjuka och hårda metoderna. Reklammannen Greger Stenström talar om trovärdighet i budskapet. Detsamma gör Fredrik Konnander vid Försvarshögskolan. Fast då handlar det om psylogiska operationer, psyops, som är den militära motsvarigheten till marknadsföring.

Informationsarenan består till stor del av det som vardagligt kallas nätet. Vilka faror lurar därute? FOI:s experter på IT-säkerhet kan visa att det bara tar någon minut innan en oskyddad dator anfalls. I en annan FOI-studie varnas för tilllfälliga brottsplatser på internet. När brottet är utfört sopas spåren undan.

Kampen om tanken gäller också vår förmåga att ändra synsätt. Det kan gälla Försvarsmaktens inriktning. Eller att byta kalla krigets syn på NBC-skydd till något som är anpassat till informationssamhället och nya hotbilder.

IT-professorn Bo Dahlbom varnar dock för att försvaret slänger ut kreatörerna när man nalkas informationsamhället. Det finns en risk för att vi får ett centralstyrt försvar helt i motsats till grundtanken i ett insatsinriktat försvar.

Jan-Ivar Askelin är redaktör för Framsyn

Innehåll

Informationskriget styr vår verklighet

Informationskriget pågår ständigt och människor påverkas allt mer av reklam, underhållning och propaganda. Ju mer tidningar, tv och internet styr vår bild av världen, desto viktigare blir också makten över medierna.

Den snabba IT-utvecklingen ger dessutom nya möjligheter för den som vill manipulera sin omvärld.

Av Mats Ekdahl, Göran Lindmark och Göran Stütz

Vad är det som påverkar och övertalar oss till ett visst synsätt, en attityd eller ett visst beteende?

Förmodligen en hel del men det omedelbara svaret är förstås det vi ser, hör och på andra sätt direkt erfar. I den processen blir massmedierna och då speciellt nyhetsmedierna centrala eftersom det huvudsakligen är genom dem som vi navigerar i vår omvärld. Fast bilden är forskningsmässigt komplex. Hur relationen medieinnehåll-mediekonsumtion egentligen ser ut är en svår fråga och än svårare att studera är medieinnehållets effekt på våra åsikter, attityder och, i förlängningen, på till exempel skilda opinionslägen i samhället. Att nyhetsmedierna, som genom sitt innehåll anger det som är aktuellt för dagen, det vill säga bestämmer agendan, påverkar våra attityder och förhållningssätt torde dock vara oomtvistat. Mediemångfald, fri åsikts- och opinionsbildning är viktiga förutsättningar för det demokratiska samhällets existens.

Stark psykologisk kraft

Massmedierna är en stark - den starkaste - psykologiska kraften i samhället i egenskap av alla sina möjligheter och samhällsvärden: som nyhetsförmedlare, opinionsbildare, debattforum, idéspridare, belysare av andra folk, teknologipådrivare, samhällsgranskare, minoriteternas röst, underhållare, utbildare, social kontakt, effektiviserare av handel och affärsliv och som sammanhållande kraft för samhällets kommunikationsströmmar.

Handeln med nyheter och underhållning är en av de få salufördа saker i det moderna samhället som kan förändra, förstärka eller försämra en samhällskänsla. I en mycket allmän mening handlar kommunikation via massmedierna alltid om en transformation där något yttre blir till något inre, eller om något inre som blir till något yttre. Materia och energi i form av texter, bilder, föremål, rörelser, elektriska signaler, ljud och ljus-vågor ges mening, ett mentalt innehåll - ett medvetandeinnehåll.

Här utkristalliserar sig några viktiga begrepp som hör hemma på området ”kampen om tanken”. De är självklara ingredienser i varje psykologiskt försvar och har länge varit föremål för intresse från det svenska psykologiska försvarets sida. Påverkan och försök till påverkan är två sådana ingredienser. De verksamheter, såväl i fred som i krig, som vi idag övergripande kallar informationsoperationer (IO), diverse mjuka insatser, bland annat psykologisk krigföring, avsiktlig vilseledning, perception management och något som lite oegentligt kallas desinformation, men också ”hårda” attacker där man försöker skaffa sig kontroll över mottagarens/motståndarsidans informationssystem, har som mål att påverka mottagarens/målets registrering av omvärlden i en för aktören/avsändaren gynnsam riktning.

Vi utsätts dagligen för försök till opinionsbildning och annan styrning av vår verklighetsuppfattning, alltifrån enkla reklambudskap till lobbying och mer avancerad öppen eller dold propagandaverksamhet. Fast alla sådana aktiviteter kan knappast kallas informationsoperationer. Att försöka påverka är helt legalt och behöver varken vara lagstridigt eller illasinnat. Att ljuga är inte i lag förbjudet.

Ett annat lika centralt begrepp är förtroende. Förtroende - eller bristen på detsamma - finns som en självklar ingrediens i våra liv utan att vi närmare funderar på saken. För att ett samhälle ska fungera måste det finnas ett visst mått av förtroende männi-skor emellan och för samhället i vid mening, annars lär ett sådant knappast kunna existera. Åtminstone inte av det slag vi vill ha.

Rätten till information

I sammanhanget är förstås begrepp som information och kommunikation viktiga. Utan dessa komplexa företeelser kan samhället av flera skäl knappast fungera. Människors rätt till information är, tillsammans med yttrandefriheten, grundlagsfäst i vårt land och gäller oberoende av situation. På det förhållandet baserades det tidigare psykologiska försvaret och en betydande del av verksamheten gick ut på att på olika sätt verka för att samhället kunde leva upp till de informations- och kommunikationsmässiga

kraven. Inte minst gäller detta i samband med samhällsstörningar där mängden av och kraven på information och kommunikation ökar, och under sådana betingelser inte bara är verktyg för att rädda liv och egendom utan också sätt att vidmakthålla medborgarnas förtroende för samhället och dess institutioner.

Massmedierna är emellertid inte bara en ”normal”, daglig fatabur för vår omvärldsbevakning och kompassnål för vår orientering, för det fria ordet, för opinionsbildning. De har också en annan funktion, egentligen flera i ett demokratiskt samhälle, men i detta sammanhang att som den viktigaste kanalen gentemot medborgarna ingå i samhällets varnings-, larm- och informationssystem. De bägge funktionerna kan till synes vara olika men tjänar i slutändan samma demokratiska syfte.

Människan har alltid varit omgiven av fysiska risker och hot av olika slag. Många av dessa har varit väntade och synliga och har därmed också i varierande grad kunnat åtgärdas. Vad som kännetecknar samhället av idag är att många risker och hot är obekanta, osynliga, oförutsägbara och därmed också opåverkbara för den enskilde själv. Ofta äger han eller hon inte kunskaper för att på egen hand hantera situationen och ha kontroll på de risker och hot utvecklingen lett till, och därmed har ansvaret för människors väl och ve allt mer lagts i händerna på andra (experter, politiker, kommentatorer med flera). Samhällets förmåga att kommunicera prövas speciellt i samband med samhällsstörningar då behovet av och kraven på information och kommunikation växer.

Information/kommunikation, påverkan och förtroende är förstås centrala också i denna del. Att som sändare i alla lägen effektivt ”nå ut”, att ha något relevant att säga, att mottagarna har förtroende för avsändaren samt att informationskanalerna upplevs som trovärdiga är ett måste om försök till former av påverkan ska krönas med framgång. Detta gäller under normala förhållanden men speciellt vid samhällsstörningar när upplevda hot och risker, som i sin tur kan leda till oro och ängslan, kanske panik, måste ersättas med adekvat kunskap, råd och anvisningar.

Massmediernas beredskap
Ett område inom vilket det psykologiska försvaret har att verka är massmediernas beredskap. Massmediernas beredskap generellt, men speciellt i störda situationer, ses här som en delmängd i - men inte en funktion av - samhällets informationsberedskap. Att försöka sammanblanda dem vore utsiktslöst, och i praktiken omöjligt. Den medierade informationen om hotet eller riskens orsaker och om krishanteringen i sig, kan vara av avgörande betydelse för krishanteringens effektivitet i ett senare skede. I ett akut skede är medierna effektivare genom sin snabbhet och spridning än andra kända informationskanaler. Den upplevda legitimiteten som förmedlare av information, tillförlitligheten, hos medierna är här av central betydelse.

I detta uppdrag framträder medierna tydligt som en av det demokratiska samhällets grundbultar emedan åtminstone två av deras roller sammanfaller, dels som en resurs i samhällets informations-, larm- och varningssystem, dels för upprätthållandet av en fri och oberoende nyhetsförmedling och opinionsbildning. Här möts de nämnda begreppen var för sig men framför allt i kombination. Såväl i termer av ett samhälleligt beredskaps- och sårbarhetstänkande som i våra enskilda, normala, dagliga liv är dessa kanske viktigare och mer aktuella idag än någonsin tidigare.

Målet i denna del av Styrelsens för psykologiskt försvar (SPF) verksamhet är att kunna ge råd och vägledning om massmedieföretagens beredskapsplanering, att efter samråd med företag inom tidnings-, nyhetsbyrå- samt radio- och tv-områdena följa och analysera utvecklingen i mediernas beredskapsplanering, att utarbeta underlag för regeringens beslut om beredskapen för massmedieområdet, samt att hålla sig informerad om utvecklingen inom massmedieområdet.

Att försöka förvanska verkligheten
Försök att påverka system och människor för att skaffa sig fördelar har förekommit i alla tider. Formerna och verktygen för sådana försök har förändrats under historiens gång. Tidigare upprätthöll man en gräns mellan krigstid och fredstida verksamheter. Idag är den gränsen diffus. Försök till påverkan behöver som sagt inte vara fientlig, kriminell eller ens skadlig utan är en del av vårt normala liv. Det slags påverkan som här primärt avses har som syfte att målet för aktionen (mottagaren) inte uppfattar en förvanskad verklighet, vilket på kort eller lång sikt medför konsekvenser till men för mottagaren.

Väpnade konflikter, som exempel, förs idag med både militära och mediala medel. Att nyhetsmedierna har betydelse som instrument för opinionspåverkan är helt klart. Försök att styra och forma och att även manipulera opinioner är närmast en självklarhet för den stats- och krigsledning som har makt och kontroll över nyhetsmedierna. Propagandamakarens möjligheter att nå ut inte bara till hemma-opinionen och fiendesidan utan också till en större omvärld är idag bättre än någonsin genom den medietekniska utvecklingen. Propagandainslag utformas ofta som en naturlig del i nyhetsförmedlingen vilket vi sett många exempel på från konflikternas Balkan och dagens Irak.

Nya tekniska vägar
På medieområdet medför den snabba teknikutvecklingen att informationsflödet och mängden av stimuli från en outtömlig medievärld bara växer och växer. Nya tekniska vägar öppnas ständigt till nya verkligheter, fakta och underhållning. Sorteringsproblemen och våra begrepp om vilka mediernas uppgiftslämnare egentligen är blir allt svårare att hantera. I det växande flödet av nyheter, reklam och underhållning blir gränsen mellan självständig journalistisk rapportering och subtilt styrda budskap svår att se. Inte minst i en tid när hantverksmässig journalistik rationaliseras bort till förmån för industrialiserad nyhetsproduktion. Det moderna mediesamhället är utifrån en totalförsvarsaspekt den perfekta terrängen för informationspsykologiska bakhåll. Ju viktigare medierna blir för vår bild av världen desto viktigare blir också medielandskapet för aktörer inom PR,
lobbying och informationsoperationer av olika slag, har publicisten och debattören Göran Rosenberg konstaterat. Det våld-samma informations- och underhållningsflödet gör att det finns mycket att gömma sig bakom eller förklä sig till.

En definition som skulle kunna vara generellt giltig inom området massmediernas beredskap kan vara att informationsoperationer är ”sätt för en aktör att via en avsiktlig teknisk och/eller kognitiv påverkan via massmedierna uppnå ett kalkylerat inflytande över ett system eller annan aktör som medför effekter för dettas/dennes förmåga att återge eller registrera verkligheten. Avsikten är att på kort eller lång sikt skapa egna fördelar”.

En angelägen uppgift för medieberedskapen är att på olika sätt förebygga och minska sårbarheten i viktiga mediers produktion och distribution genom att skapa en sådan säkerhets- och krishanteringsförmåga, att samhällets krav på information säkras och kan fungera i alla situationer och inte minst vid samhällsstörningar.

Sverige har i dag en försvarspolitik som på en rad punkter skiljer sig från den som rådde för ett antal år sedan. Visionen på den civila sidan är enkelt uttryckt en förberedd, robust och decentraliserad civil kris- eller katastrofberedskap, huvudsakligen i bruk i fredstid men med kapacitet till anpassning för kris- och krigsliknande tillstånd. Ansvaret för beredskapsplaneringen har decentraliserats till berörda lokala och regionala organisationer, myndigheter och i samverkan med näringslivet. Detta bör på sikt också gälla på massmediesidan.

Rapporteringssäkerhet
Vårt svenska samhälle sägs under de senaste årtiondena efterhand ha övergått från ett industrisamhälle till ett informationssamhälle/nätverkssamhälle. Det moderna samhället är i ljuset av detta i betydligt högre grad än tidigare samhällen just informationsberoende, ”informationstätt”, i såväl tekniskt som kognitivt avseende. Möjligheterna att sammanställa och använda information av allehanda slag påverkar både den enskildes vardag och samhället i stort. Denna strukturomvandling medför konsekvenser för myndigheter, näringsliv, beslutsfattare och medborgare - samt för massmedierna som sådana och samhällets mediestruktur i stort.

Utvecklingen är i många avseenden positiv men vi kan inte blunda för de hot och risker denna utveckling fört med sig, de sårbarheter i samhället och för enskilda som kan identifieras och de konsekvenser dessa kan få för samhället i stort och i smått. Den snabba utvecklingen på IT-området, digitalisering, nya medier, sammansmältning av flera informationskanaler och tillväxten av såväl utbud som efterfrågan på ”information” gör det angeläget att till exempel ta sig an de nya problem, såväl tekniska som källkritiska, och sårbarheter som denna utveckling medfört. Nya tekniker öppnar nya möjligheter, tillsammans med traditionella informationsspridningskanaler, för den som vill manipulera sin omvärld.

När det gäller massmedierna dominerar två hotbilder som inte är varandra uteslutande eller oberoende - snarare tvärtom. Den ena är av teknisk karaktär och gäller kollaps inom större eller mindre delar av mediestrukturen, som i sin tur påverkar mediernas möjligheter att producera och distribuera, medan den andra är av kognitiv, ”mjuk” karaktär, det vill säga i vilken utsträckning massmedierna kan och låter sig bli instrument för eller redskap i aktioner med vilseledande syften av det slag som angetts ovan.

Till detta ska förstås läggas andra trender i dagens massmedielandskap. Globaliseringen har inneburit förändrade villkor för såväl medie- som nyhetsverksamheten vilket bland annat har genomgripande betydelse för journalistikens form och innehåll. Globala mediekonglomerat växer upp och lägger under sig många och skilda medier. Medielogiken styr rapporteringen. Gamla publicistiska ideal verkar få stå tillbaka för målsättningar av annat slag. Vem är det i dag - medierna, medborgarna, mediekonglomeraten - som avgör vad som är av ett ”oavvisligt allmänintresse”? Infotainment är härvidlag ett aktuellt begrepp.

Vi har idag för lite kunskap om de redaktionella processer och nya arbetssätt som är en följd dels av den nya tekniken, dels av ett hårdnande ekonomiskt klimat. Den moderna ”redaktörsrollen” i vid mening är därför en demokratisk nyckelroll. ”Redaktören” står som yttrandefrihetens förvaltare i den offentliga

opinionsbildningen. Han eller hon står i spänningsfältet mellan demokrati och marknad och kan därför liknas vid en portvakt för det offentliga samtalet. Redaktörsrollen blir också allt svårare att upprätthålla i en tid präglad av mediers sammansmältning och i en expansion av nya kommunikationsredskap som inte är massmedier i traditionell mening.

Förr var det i hög grad ägarna till medierna och deras närmaste nätverk som bestämde vem och vilka åsikter som skulle komma till tals. Idag är det en blandning av journalistnätverk, medielogik, ägarkoncentration och corporate speech (de stora snackar samma språk) som bestämmer. De nya medieteknologierna och det hårdnande ekonomiska trycket skapar väldiga gap som hela tiden ska fyllas med nytt stoff. Detta gör de nya medieimperierna, ofta styrda av aggressiva företagare, betydligt mer sårbara än de gamla mediehusen vilka byggdes upp av generationer av entreprenörer som utan brådska konsoliderade sina verksamheters ekonomi och opinionerna om dem.

Påträngande tidstjuvar

Foto Martin Nauclér (Bilden är manipulerad.)

Massmedierna stjäl tid och samtalsresurser från oss människor. De hör alltså till människans största och mest påträngande tidstjuvar. Därför är det naturligtvis väsentligt vilken verklighetsbild, människosyn och samhällssyn de framställer genom sina uttrycksformer, bildval, ämnesval och värderingar. Massmedierna präntar bildligt talat in sina vitt skilda mentaliteter i samhällssjälen varje dag. Människors mottaglighet för propaganda och lobbying och människors förmåga att genomskåda propaganda och lobbying är en ödesfråga för det civiliserade samhällets utveckling. Det gäller bland annat frågan om hur attityder, moraliska värderingar och beteenden påverkas, förändras och utvecklas över tiden - och vilka konsekvenser sådana förändringar i männi-skors synsätt får på samhället och samhällsstrukturen, antingen i uppbyggande eller i negativt urholkande mening. Om allt fler människors verklighetsbild formas av krafter från reklam, underhållning, propaganda och lobbying, är det uppenbart att det blir brister i den medborgerliga kunskaps- och idébildningen. Naturligtvis har detta betydelse för samhällsklimatet och samhällsberedskapen, men också för samhällshälsan i vid mening.

Mot den bakgrunden kan man ställa sig frågan vilka möjligheter dagens mediesamhälle ger den som på ett avsiktligt tekniskt och/eller innehållsmässigt sätt via massmedierna önskar påverka eller manipulera sin omgivning, i någon mening, menliga syften? Vem, vilka eller vad som ligger bakom sådan påverkan kan variera från enskilda individer till hela stater eller grupperingar inom dessa; företag, terrorgrupper etcetera. Ur ett beredskapsperspektiv kan konstateras att dagens hotbilder uppvisar stor variation och artrikedom. Det gäller att skaffa sig förhållningssätt gentemot och kunskaper kring hot och risker som ligger utanför den traditionella säkerhetspolitiken, främst icke-militära hot. Oberoende av utgångspunkter måste hoten identifieras och effekterna diskuteras:

Vad är input, vad är output, hur och varför kommer massmedierna in som en ”svart låda” däremellan?

På massmediesidan ska public service-företagen under normala betingelser ”stå i allmänhetens tjänst”, men också enligt avtalen med staten ha beredskap att kunna verka så normalt som möjligt även under

störda förhållanden. De privata medierna har utöver sina kommersiella mål även samhällsviktiga skäl att verka även under så kallade svåra förhållanden. Det synes väsentligt att för den privata och offentliga mediesektorn försöka skapa en gemensam syn på behovet av säkerhet, beredskap, krishanteringsförmåga och samverkan. Gemensamma kunskaper om hot, risker, sårbarheter samt möjligheter att bistå varandra är nödvändiga förutsättningar för att under störda förhållanden - samhällsstörningar, kriser, katastrofer; ytterst krig - kunna agera adekvat, snabbt och effektivt.

Här kan det nya begreppet rapporteringssäkerhet föras in i bilden. Med det kan avses ett eller flera robusta system på olika nivåer i samhället för säker distribution av allehanda information och kommunikation - nyheter, krisinformation, varning. Säkerheten avser robusthet såväl i tekniskt avseende som innehållsmässigt, och detta oberoende av situation.

Gällande civila försvarsdoktrin bygger i väsentliga delar på ett ”partnerskap” innebärande ett (ökat) samarbete i totalförsvars- och beredskapsfrågor mellan stat och näringsliv. Vad gäller massmediernas beredskap är det viktigt att samverkan kommer till stånd mellan berörda myndigheter och medieföretag för att på så sätt ”säkra” mediernas roll som oberoende - i meningen från staten skilda - och trovärdiga förmedlare av information och kommunikation också i kris och under höjd beredskap.

Genom informationsoperationer antas någon aktör kunna utnyttja och/eller påverka mediers och mediesystemens - mediemarknadens - strukturella egenskaper varvid leveransproblem uppstår då leveranssäkerheten rubbas. I förlängningen kan medierna upplevas som mindre tillförlitliga och på sikt finns det risk för att medborgarnas förtroende och tillit urholkas inte bara för medierna utan för samhället i stort.

Forsknings- och utredningsprojekt
Utgångspunkten för en av de på området ”massmediernas beredskap” pågående studierna är att förtroende och tillit för samhället påverkas av strukturella egenskaper hos medierna och mediesystemen. Studien syftar till att belysa åtgärder för att på sikt åstadkomma robusta informationssystem omfattande såväl public service-företagen som de kommersiella medierna. Studien inleds med en hotbildsanalys. I ljuset av denna identifieras övergripande strukturella egenskaper hos medierna och i mediestrukturen. Målet är att definiera ett antal för gällande hotbilder relevanta nyckelindikatorer. Den sista fasen i studien blir en analys av och diskussion om hur identifierade aktörer skulle kunna manipulera medierna via nyckelindikatorerna för bestämda syften. En diskussion av vilka beredskapsmässiga krav som borde ställas på dessa egenskaper avslutar projektet.

SPF:s roll i sammanhanget
Massmedierna - ”mediemarknaden” - är bemannade av människor som tror sig kunna tjäna på dem, främst pengar. Att förmedla nyheter, att uppträda som samhällets och allmänhetens ombud, ”tredje statsmakten” etcetera är alltså ingen filantropisk verksamhet och ska inte heller vara det i ett samhälle av det slag vi önskar. Beredskapstänkande är följaktligen föga överraskande inte någon första ledstjärna för de kommersiella eller privata medierna. Bilden är förstås i det avseendet annorlunda på public service-sidan.

Medierådet är en central del i SPF:s arbete med frågor som rör medieberedskap. Rådets verksamhet syftar till att för den privata och offentliga sektorn skapa en gemensam syn på behov av säkerhet, beredskap, krishanteringsförmåga och samverkan inom massmedieområdet. I medierådet finns representanter för Radioutgivareföreningen (den privata radiobranschens organisation), Sveriges Radio, Sveriges Television, Teracom, Tidningarnas Telegrambyrå, Tidningsutgivarna, TV4, Post- och telestyrelsen, Krisberedskapsmyn-digheten och Räddningsverket.

De upparbetade kontakter som i dag finns i medierådet är av avgörande betydelse vid kriser av olika slag emedan ledamöterna inte har några självklara kontaktytor i det dagliga arbetet. Gemensamma kunskaper om hot, risker, sårbarheter samt möjligheten att bistå varandra är nödvändiga förutsättningar för att vid kriser kunna agera adekvat, snabbt och effektivt. En av rådets viktigaste uppgifter är att verka för att det finns ett ömsesidigt förtroende och en respekt mellan aktörer och beslutsfattare.

Mats Ekdahl är generaldirektör vid Styrelsen för psykologiskt försvar (SPF) med bakgrund bland annat som chefredaktör för tidningarna Vi, Resumé, Läkartidningen och Arbetet.
Göran Lindmark är informationschef vid SPF och ställföreträdande chef för myndigheten.
Göran Stütz är senior rådgivare och laborator samt tidigare forskningschef vid SPF.

Nyttig kunskap för massmedier

Styrelsen för psykologiskt försvar (SPF) är en myndighet som i huvudsak arbetar med medie-beredskap, totalförsvarsinformation och opinionsstudier. SPF:s roll inom området massmedieberedskap har förändrats i det nya krishanteringssystemet. SPF ska ge råd och vägledning om massmedieföretagens planering för höjd beredskap (krig) och för svåra påfrestningar på samhället i fred. SPF ska även utarbeta underlag för regeringens beslut om beredskap för massmedieföretagen inför krig och vid svåra påfrestningar i fred samt hålla sig informerad om den framtida utvecklingen inom massmedieområdet. Detta är omfattande och viktiga uppgifter.

SPF:s roll fokuseras på att vara samtalspart och kunskapsförmedlare till massmedieföretagen inte minst när det gäller verksamhet under störda förhållanden.

Nyckelordet är dialog. SPF:s verksamhet ska vara till direkt nytta för massmedieföretagen och den ska stödja dessa inom områden som de själva - av olika skäl - inte kan bevaka fullt ut, och som enkelt uttryckt handlar om att anlägga ett samhällsperspektiv på informationens betydelse under störda förhållanden. Medborgarnas rätt till information är ju grundlagsfäst i vårt land och nyhetsmedierna är de viktigaste förmedlarna av händelser i samhället.

Människan, mediemångfalden och det öppna samhället

Bok av Mats Ekdahl
ISBN 91-87260-99-9

Den som vill tränga djupare in i ovanstående artikels resonemang kan läsa Mats Ekdahls bok som utlovas vara ”historien om massmediernas pluralism och dess labyrintiska processer”. Boken har tillkommit på initiativ av kulturminister Marita Ulvskog som tyckte att det saknas en bok om mediemångfalden. Boken sägs kräva koncentration, men ger belöning. Och det kan nog stämma.

Författarens ambition har varit att lyfta ut frågan om mediernas mångfald från den plats där den brukar debatteras - på akademikernas och experternas arena - till ett mer vardagligt plan där den vanlige läsaren kan känna sig hemma.

Mediemångfald är ju ingen lätt fråga. Mer mångfald ger inte mer poäng. Det viktiga är att se vad som utgör mångfalden. Vi har tv dygnet runt i ett otal kanaler och ändå debatteras ständigt frågan om att tv blivit sämre.

Drygt 70 procent av befolkningen läser regelbundet en morgontidning. Det kan tyckas som mycket. Men för 20 år sedan var siffran 80 procent. Dagspressen tappar stadigt och sakta i upplaga.


Foto: Martin Nauclér

Vad sådana saker beror på, vilka konsekvenser de kan få och vad man möjligtvis kan göra för att rädda situationen handlar denna bok om.

Marknadsföringens egen gerillakrigare

Att vara trovärdig, tänka utifrån och in och att kommunicera ett budskap i taget är tre hållpunkter för den som vill nå ut med sitt budskap. Det menar reklammakaren Greger Stenström som ser sin egen yrkeskår som marknadsföringens gerillakrigare.

Av Jan-Ivar Askelin

Det finns de som lever på att vi ska tänka om. Byta från ett tandkrämsmärke till ett annat. Eller byta politiskt parti. Går allting att sälja med reklam?

- Nej, säger Greger Stenström, grundare av Stenström & Co Annonsbyrå i Stockholm, numera Stenström Red Cell. Reklamen måste som all kommunikation vara ärlig. Vår uppgift är att tala om att det finns en viss produkt på marknaden och att hitta rätt köpare till produkten. Den som säljer vill inte ha missnöjda kunder. Kruxet för oss är att ingen egentligen vill lyssna på oss. Journalisten har sin publik. Vi måste erövra vår varenda gång.

Greger Stenström kallar reklammakarna för marknadsföringens gerillakrigare. Man måste överraska för att fånga intresset. Styrelsen för psykologiskt försvar (SPF) har anlitat reklamfolk just av det skälet. För att kunna få ut budskapet på ett icketraditionellt sätt och på lite olika vägar.

- Det kanske man måste kunna när fienden står i landet.

Först några grunder:
- Information är en envägskommunikation. Det är ett ensidigt framförande av ett budskap. Kommunikation är när det uppstår en dialog mellan sändare och mottagare. Många företag har nu insett att det inte är så stor skillnad mellan information och marknadsföring och i stället för informationsavdelningar skaffar man sig kommunikationsavdelningar. Och det tycker jag är rätt. Det finns ingen större motsättning i detta.

- Det som saknas i Sverige, säger Greger Stenström, är en kommunikationsutbildning.

- Vi har skolor för journalister, informatörer och reklammakare, men inte för kommunikatörer. Och ändå är det ju samma mekanismer man använder.

I väntan på den skolan så kan Framsyn erbjuda Greger Stenströms snabbkurs. Den som klarar den har kommit en bra bit på vägen. Man ska tänka på att:

- Tänka utifrån och in. Inte inifrån och ut.
- Vara sparsam med antalet budskap. Helst ett. Högst tre.
- Vara trovärdig.
- Alltid fråga sig ”vem är jag till för?”

- Utifrån och in innebär att du lyssnar av vad de som du vänder till dig är intresserade av att du talar om. Utifrån det måste du forma din kommunikation för att nå ut med ditt budskap. Många företag, även stora, har svårt för det här. De utgår från sin fabrik och ser vilka produkter som kan göras. Sedan frågar man om någon är intresserad på utsidan. I stället ska man fråga sina tänkbara kunder om de vill att vi ska ändra vår produkt på något sätt. Så kallad samhällsinformation har svårt för det här. Det blir gärna ett ensidigt budskap och därmed ingen kommunikation med dem som man riktar budskapet till.

Få budskap
- Man bör ha ett huvudbudskap och upprepa det. Två budskap kan funka. Tre i nödfall, säger Greger Stenström.

På frågan om en försvarsmakt som har fyra huvuduppgifter har en eller ett par för mycket säger han att man i så fall bör kommunicera en i taget.

En särskild avdelning här är de politiska partierna. Inför varje val investeras miljoner i att få ut budskapet. I soffan i valstudion sitter sedan några dystra och beklagar sig att de inte fick ut budskapet. Ett särfall var väl Anders Björck som i senaste valet beklagade sig att partiet fick ut sitt budskap.

- Politiska partier är svåra att jobba med för en reklamare därför att de är så inställda på ensidig kommunikation. Partierna har sina ideologier och hjärtefrågor. Egentligen borde man fråga väljarna vilka frågor de tycker är intressantast och sedan gå till sitt parti och se om det finns något där att erbjuda. Men det budskapet kanske ligger för långt från partiets själ.

Trots att det talas om otrogna väljare så är människor betydligt trognare i valet av attityder än i valet av varumärken. Där är vi notoriskt otrogna, säger Greger Stenström.

Trovärdigheten avgörande
Trovärdigheten är kanske det svåraste problemet i reklambranschen, menar Greger Stenström. För de fyra borgerliga partierna är trovärdigheten just nu nummer ett.

- De satsar på ett budskap, maktskifte. Det är bra. Nu hänger trovärdigheten på att partierna inte pratar mer för sig själva än den gemensamma saken. För det är trovärdigheten hos avsändaren som avgör om budskapet ska gå hem. Det lönar sig inte så mycket att man slår sig för bröstet och talar om sin produkts förträfflighet eftersom alla vet att man talar i sin egen sak.

Greger Stenström tar varningen för rökningens faror som exempel.

- Det mest trovärdiga är att den som tillverkar produkten också varnar för den. Det är ju så man gör också, även om tobaksbolagen tvingats till det. Men vi tänker nog som så att om rökningen inte ökar risken för cancer så skulle aldrig bolagen gå med på kraven.

En klassiker är ju Socialstyrelsens uppmaning att vi skulle äta bröd.

- De flesta trodde ju att det verkligen var myndigheten som stod bakom. Man såg inte att avsändaren var Brödinstitutet.

Vem är jag till för?
- Frågan om vem man är till för bör man ställa sig då och då, oavsett vad man pysslar med. Om svaret inte blir annat ”än sig själv” så har det ju blivit lite väl smalt, säger Greger Stenström och tar upp fenomenet omorganisation.

- ”Nu går det för dåligt. Nu ska vi omorganisera och ha en plattare organisation”. Men väldigt sällan funderar man på syftet. För vem finns vi till?

Med dessa visdomsord avslutas grundkursen. Nu kan vi studera branschen lite närmare och titta på kunder, hur man vinner kundens hjärta, produkter och varumärken.

Reklamens uppgift är enligt Greger Stenström att tydliggöra erbjudandet. Så här ser vår vara ut som finns på marknaden.

- Vi vill inte att du ska göra fel val. Då är du förlorad och kommer inte tillbaka och företaget måste ersätta missnöjda kunder med nya kunder. Företaget vill ha goda ambassadörer och därför måste man vara tydlig i sitt budskap. Företagen är livrädda för missnöjda kunder. Men lyssnar man på en missnöjd kund kan man få en bra ambassadör.

Vilket följande historia ska visa.

Ett varuhus var känt för att alltid ge missnöjda kunder pengarna tillbaka. En dag kom det in en kund och klagade på sina nyinköpta snökedjor. Inget kvitto hade han. Men arg var han. Försäljaren tog snökedjorna, bad om ursäkt och lämnade tillbaka pengarna. Hans kamrat som såg på blev mer och mer förvånad och sa:

”Men vi säljer ju inte snökedjor”. Och svaret blev: ”Nej, men han kommer säkert tillbaka och köper något”.

- Det är maximal kundservice. Längre än så kan man nog inte komma i att lyssna på kunden.

Hur når man då in i huvudet på kunden? Hur ser kampen om tanken ut?

- Om vi vill sälja resor frågar vi oss vad som rör sig i knoppen på den som står i begrepp att köpa en resa: Vilka beslutskriterier är de viktigaste? Priset, kompisarnas råd, katalogen, sol på resmålet? Då kollar vi om just det här resföretaget är bra på att möta något av dessa krav. Och så jobbar vi med det. Det kanske innebär att vi måste ändra lite på produkten.

Produkten måste vara bra
En av Red Cells stora kunder sedan länge är Bregott. I mitten av 1990-talet bestod produkten av 80 procent smör och 20 procent sojaolja. Då var det väldigt intressant med en helsvensk produkt och den importerade sojaoljan byttes därför ut mot nyttig svensk rapsolja.

- Då flyttade vi ut till landet, till Bregottland. Där hittade vi korna och så småningom kom vi på att detta var vår fabrik, Bregottfabriken. I motsats till margarinfabriken där det rök ur skorstenarna.

- Produkten måste vara bra. Annars funkar det inte. En braskande reklam kan slå ihjäl en halvbra produkt, säger Greger Stenström och erinrar sig hur en ny tidning aldrig fick chansen.

- Reklambyrån jobbade med en stor kampanj och redaktionen jobbade med den nya tidningen. När kampanjen kulminerade kom den nya tidningen ut. Perfekt? Nej, det trista var att det första numret inte var bra. Och dessvärre hade för många köpt tidningen. Att sedan tidningen efter några nummer var riktigt bra hjälpte inte. Reklamen hade lockat för många att köpa det första numret.

Bregott lär vara känt av 98 procent. Hur många känner till Hammarbys fotbollslag? Rimligtvis är det mer känt än Bregott.

- Men det räcker inte med ett känt varumärke, säger Greger Stenström. Vad är Hammarby känt för? Att man inte gör mål? Spelar tråkig fotboll? Ett av de mest kända märkena är Trygg-Hansas livboj. Bolaget värnade om livbojen. Men hur var kopplingen mellan bolaget och symbolen? Det var svårare att veta vad som skiljde Trygg-Hansa från sina konkurrenter än att man skänkte bort livbojar till höger och vänster.

Vissa märken är så starka att de inte behöver reklam. Greger Stenström nickar mot Lamborghinihandlaren på andra sidan Nybroviken.

- Men de har också en gång fått investera i sitt märke med reklam. När märket blivit tillräckligt starkt kan man dra ned på reklamen.

Och slutligen. Hur säljer man in det nya försvaret?

- Det jobbet skulle jag verkligen vilja ha.

Jan-Ivar Askelin är redaktör för Framsyn.

”Vi vill få bort mystiken kring informationsarenan”

Foto: Martin Nauclér

- Människan har alltid sysslat med informationsoperationer.

Nu sker det på nätet där informationen går på bråkdelar av sekunder. Snabbheten gör att det blir svårare att försvara sig. Det säger Håkan Gustafsson som reder ut hur Försvarsmakten ska arbeta med informationsoperationer i praktiken.

Av Jan-Ivar Askelin

Ett flygplan slår ut en av motståndarens staber. Det kan tyckas vara rätt för staber är så kallade värdiga mål. Samtidigt var staben den egna underrättelsetjänstens bästa källa som man över tiden inhämtade information från.

- Det här händer i moderna krig, säger Håkan Gustafsson vid Högkvarteret. Och så blir det när informationsoperationer inte samordnas med andra insatser i en gemensam operation.

Håkan Gustafsson tror att i framtiden kommer det att finnas en i insatsledningen som är ansvarig för informationsoperationer. Men dit är det fortfarande lång väg att gå.

Ett stort steg har dock tagits. Försvarsmakten har enats om termen informationsoperationer och förpassat gamla begrepp som ledningskrigföring, informationskrigföring och andra till historien.

- Jag tror att det handlar om en internationell trend. Man börjar mer och mer tala om informationsoperationer När regeringen i en proposition använde det uttrycket så följde försvaret efter. Sedan mitten av 90-talet har vi börjat betrakta detta område som en helhet.

Enligt försvaret är informationsoperationer en samordnad verksamhet som genomförs i syfte att påverka motståndarens eller andra aktörers beslut. Detta uppnås genom att påverka beslutsfattare, information och informationsbaserade processer och system. Samtidigt ska man skydda egna beslutsfattare, information och informationsbaserade processer och system. Informationsoperationer stödjer aktivt egna defensiva eller offensiva syften.

- Informationsoperationer kommer in tidigt i genomförandet av en operation. Det kan börja med exempelvis psykologiska operationer, psyops, och sluta med att man bombar motståndarens telenät. Men det handlar hela tiden om gränsdragningar och några spikraka gränser är ofta svåra att dra. Traditionell krigföring med digitala system och nätverkskrigföring kan ibland vara överlappande. Televapen där man avlyssnar en motståndare hör till vårt område medan system med varnare och motmedel bedöms just nu ligga utanför.

Håkan Gustafsson är tjänsteförrättande chef för arbetsgruppen för Försvarsmaktens informationsoperationer (Ag FM IO), en grupp på fem personer som inom Strategiledningen bland annat har arbetat med att reda ut definitioner och begrepp. Detta arbete har resulterat i Försvarsmaktens grundsyn på informationsoperationer. Även om dokumentet kallas för utkast så är det fastställt för tillämpning och det ska utvecklas under vintern för att harmonisera med övriga doktriner i Försvarsmakten. I nästa steg ska arbetsgruppen föreslå en organisation och hur informationsoperationer ska användas i praktiken.

- Vi ska ha en defensiv förmåga och kunskap om informationsoperationers offensiva delar. Det handlar alltså om hur Försvarsmakten ska kunna skydda sig själv, vilket är viktigt att betona, säger Håkan Gustafsson. Det har ju varit mycket debatt om informationssäkerhet i samhället och många är med och vill ta för sig. Försvarsmakten har ingen uppgift att försvara internet. Det är än så länge ett delat ansvar mellan många intressenter i samhället med Post- och telestyrelsen som tillsynsmyndighet. Det pågår en utredning om informationssäkerhet under utredaren Anders Svärd som ska presenteras nästa år och då räknar vi med att bilden ska klarna om ansvarsfördelningen.

Försvaret reder ut begreppen
Försvarsmakten har påbörjat en utveckling avseende informationsoperationer, vilket innebär att man reder ut begreppen och funderar på hur man ska organisera sig. Ett första steg blir att arbetsgruppen ska bli en ordinarie del i HKV organisation och öka i antalet personer för att kunna lösa givna uppgifter. Från årsskiftet ska FM IO överföras till krigsförbandsledningen i HKV och lyda under ledningsinspektören.

- Nu är det officerare och en operationsanalytiker från FOI som ingår i Ag FM IO. I framtiden kommer säkert flera civila att ingå. Vi tittar brett efter vilka specialister vi behöver, både inom teknikområdet och mjukare områden som till exempel beteendevetenskap.

Den fjärde arenan
I försvaret talar man om arenor. De klassiska sjö, luft och mark har fått sällskap av en fjärde - informationsarenan. Det säger kanske en del om att detta område tas på allvar. Generalmajor Christer Lidström är ledningsinspektör och ansvarar för arenan på samma sätt som de andra arenorna har sina inspektörer. Inom försvaret talar man nu om funktioner.

Ledningsinspektören ansvarar för funktionerna

- ledning
- informationshantering
- verkan på informationsarenan
- Det är inom den sista funktionen som informationsoperationerna återfinns. Verkansförmågorna inom informationsarenan indelas i:
- psyops

- elektronisk krigföring som är ett samlingsbegrepp för ett stort område (telekrig, Computer Network Operations och övrig signalkrigföring)
- vilseledning
- fysisk bekämpning, det vill säga vanlig vapenverkan mot IO-mål.

Hur förklarar man då för officerare att det finns en fjärde arena som inte är lika fysisk som övriga arenor , men som är lika viktig som de andra?

- Det är klart att när granaterna slår ned i backen så är det ju väldigt påtagligt. Vi vill ta bort mystiken kring den fjärde arenan. Många har försökt att göra detta till något väldigt komplicerat som bara några få kan syssla med. Det är viktigt att betona att det inte är något konstigt med det här. Det är något som alla inom försvaret måste förhålla sig till. Det bör finnas med till exempel vid internationell krishantering, säger Håkan Gustafsson.

- Människan har sedan länge använt andra medel än fysiskt våld i konflikter, även om man inte har kallat det för informationsoperationer. Dagens teknik och informationssamhället gör att det finns fler sätt att exploatera information på för egen vinning skull än tidigare Utvecklingen kan ge stora potentiella fördelar, men kan även ge upphov till sårbarheter. Man måste lägga mer kraft på att säkra och försvara sina informationstillgångar. Exempelvis kan ett datavirus slå till snabbt med en global spridning. För att försvara nätverken handlar det om reaktioner på sekunder.

Inte kört för alla över 40
Håkan Gustafsson ser inte någon generationsklyfta i inställningen till detta område och håller inte med om att det är ”kört” för alla över 40.

- Det här har inte med ålder att göra. Jag tror att officerare av ixxxdag har förståelse för opinioners inverkan vid konflikter och att man med de mjuka delarna av informationsoperationer kan hantera detta på ett bättre sätt än tidigare. Dessutom kan man med hjälp av teknik hindra någon från att använda sitt nätverk eller med hjälp av telekrig störa någons ledning.

Vad avser utbildning inom informationsoperationer finns det en grundkurs på Försvarshögskolan och en femveckors fördjupningskurs på chefsprogrammet. Håkan Gustafssons arbetsgrupp har skapat ett utbildningspaket för självstudier på förbanden.

- Man kan väl säga att vi lever som vi lär och har lagt vårt utbildningspaket på en CD. Det är ett smidigt sätt att förklara begrepp och samband och vi har fått en hel del uppskattning bland mottagarna. Det märks att det finns ett intresse för informationsoperationer. Det är många som hör av sig och vill jobba inom detta ”nygamla” och spännande område.

Jan-Ivar Askelin är redaktör för Framsyn.


Foto: Martin Nauclér

”Krig kräver kreativitet”

Krigföringens teori utvecklas inte av soldater med skit på stövlarna utan av stabernas teoretiker. Deras förhållande till kriget är som astronomernas till stjärnorna. De observerar och är objektiva. I fält kan man inte sitta och vänta på information utan måste söka den. Man måste vara kreativ, ställa hypoteser och testa dessa. Krig ska bedrivas av kreativa människor i fält. I det nätverksbaserade försvaret riskerar tyngdpunkten, tvärtemot vad som är tanken, att hamna i staben snarare än på fältet.

Av Bo Dahlbom

I vetenskapsteorin finns en klassisk diskussion om hur vi bäst skaffar oss kunskap.

Man kan använda sig av induktion och utan förutfattad mening samla in alla fakta (eller så

många som möjligt) och sedan finna generella samband mellan dem.

Eller man kan gå hypotetiskt-deduktivt tillväga genom att kläcka intelligenta hypoteser och aktivt söka upp de fakta som gör det möjligt att testa dem.

Den induktiva metoden ger uttryck för en vetenskapssyn enligt vilken forskaren skulle kunna ersättas av en enkel maskin. Den hypotetisk-deduktiva metoden kräver en kreativ och djärv tänkare som förmår förena sin kreativitet med empirisk noggrannhet. Den framgångsrike forskaren måste inte bara vara kreativ, utan också beredd att anstränga sig för att testa och eventuellt överge sina goda idéer.

Den induktiva metoden är kanske mest tilltalande när det gäller områden där vi inte kan påverka fakta. Astronomer får i stor utsträckning nöja sig med att passivt betrakta himlavalvet. Men så snart vi kan göra ett litet experiment, så snart vi kan ingripa i fakta, genom att vända på en sten, peta lite i myrstacken, eller skjuta en kulkärve mot det där som ser ut som ett kulsprutenäste, då blir den induktiva metoden ointressant. Vem vill hålla på att samla in en massa fakta när kulsprutan kanske snart ger eld? Det som behövs, i vetenskap som i krig, är en kreativ människa som snabbt kommer till en hypotes om situationen och lika snabbt och effektivt testar hypotesen.

Orimliga krav
Den induktiva metoden är objektiv. Den vill samla in alla fakta. Men frånsett att detta är omöjligt, ställer metoden orimliga krav på vår förmåga att sammanställa dessa fakta till något vettigt.

Det berättas att matematikern Johann Carl Friedrich Gauss (1777-1855) fann många av sina eleganta matematiska samband genom att sitta och bläddra i matematiska tabeller. Men dessa induktiva framgångar används just för att illustrera Gauss genialitet. För oss vanliga dödliga gäller att den induktiva metoden snarare riskerar att dränka oss i för mycket, osorterad information, än ge oss goda uppslag till mer generella samband.

På blodigt allvar
Den hypotetisk-deduktiva metoden är medvetet subjektiv. Den väljer ut aspekter av verkligheten som intresserar och undersöker dem i subjektivt relevanta avseenden. När Wienläkaren Ignaz Semmelweis ville veta varför kvinnor fick barnsängsfeber, var det för att han ville rädda deras liv. Han var ingen mekanisk, objektiv kunskapssökare. Han var engagerad, fokuserad, och beredd att envist driva sina undersökningar tills han nådde ett svar. Och just för att han tog sin uppgift på blodigt allvar, var han öppen för nya förklaringar och därför intresserad av fakta som hans kolleger avfärdade som irrelevanta.

Eftersom det är omöjligt att samla in alla fakta, innebär den induktiva metodens krav på objektivitet att man i stället gör en plan för vilka fakta som ska samlas in, och sedan håller sig till planen. Men vetenskapens historia är fylld av upptäckter som skett när någon forskare avvikit från projektplanen för att utforska någon irriterande sidoeffekt. Det mest spektakulära exemplet är kanske Röntgens upptäckter när han tog sig tid att undersöka varför några fotografiplåtar exponerats utan att han kunde förstå hur det gått till.

Den induktiva metoden, drömmen om att ha tillgång till alla fakta, all information, är en kraftfull dröm, i vetenskapen såväl som i krigskonst och näringsliv. Datatekniken har från första början understött den drömmen och med varje ny utveckling av tekniken sker en uppdatering av hur drömmen ska förverkligas. Idén om användningen av IT för insamling av information och skapande av en gemensam lägesbild är ett exempel på hur den revolution av försvaret som det nätverksbaserade försvaret sägs innebära, i själva verket använder gamla beprövade idéer. Detta är desto märkligare som IT just inbjuder till nytänkande på den här punkten. IT är framför allt en teknik för kommunikation människor emellan, snarare än en teknik för insamling, lagring och behandling av information, som den äldre datatekniken.

Med ett mer hypotetiskt-deduktivt tänkande utvecklar man i stället en mer operativ form för informationshantering. Informationen operationaliseras. Aktivt informationssökande, interaktion och kommunikation dominerar snarare än passiv informationsinsamling. Sensorer av alla de slag kommer att spela en växande roll i framtidens näringsliv, samhällsliv och vardagsliv. Men ju fler sensorerna blir, och ju intelligentare de blir, desto viktigare blir det att de också används på ett intelligent sätt. I ett alltmer teknologiskt avancerat krig kommer sensorer och robotar att ersätta människor, men det hindrar inte att det fortfarande blir viktigt att operativt kunna styra informationshanteringen.

Bakgrundsbevakning
Den induktiva metoden kan ligga till grund för en informationshantering som har karaktär av bakgrundsbevakning, ungefär som när vi håller reda på vädret. Men så snart det kommer till operativa insatser måste den hypotetisk-deduktiva metoden få ta över. Då räcker det inte med att på förhand räkna ut hur man ska agera. Då måste man pröva sig fram genom aktivt hypotestestande och genom att

fokusera på den information som är intressant för just den hypotes man driver. Då måste man ge utrymme för flexibelt utforskande av information som överraskar, även när detta ligger vid sidan om planen. Och man måste utnyttja det faktum att människor i grupp kan organisera komplexa operationer för att vaska fram information ur omgivningen.

Krigföringens teori utvecklas - det säger sig självt - huvudsakligen av teoretiker, skrivbordsmänniskor, snarare än av krigets praktiker. Den utvecklas av stabsmänniskor snarare än av soldater med skit på stövlarna. Deras relation till kriget påminner om astronomernas. Därför blir den induktiva metoden så attraktiv. Den moderna tekniken ska användas till att skaffa en lägesbild, vilken förväntas växa fram ur en fantastisk mängd information som hela tiden samlas in av ett stort antal - ju fler dess bättre - datoriserade sensorer. Men ju fler sensorerna blir, desto mer riskerar vi att dränkas i desinformation snarare än att bli informerade, och desto mer förskjuts tyngdpunkten i verksamheten från det operativa fältet till staben - helt i motsats till grundtanken i ett insatsinriktat försvar.

Bo Dahlbom är professor i informationsteknologi och forskningschef vid Svenska IT-institutet.

Centrum för informationsoperativa studier

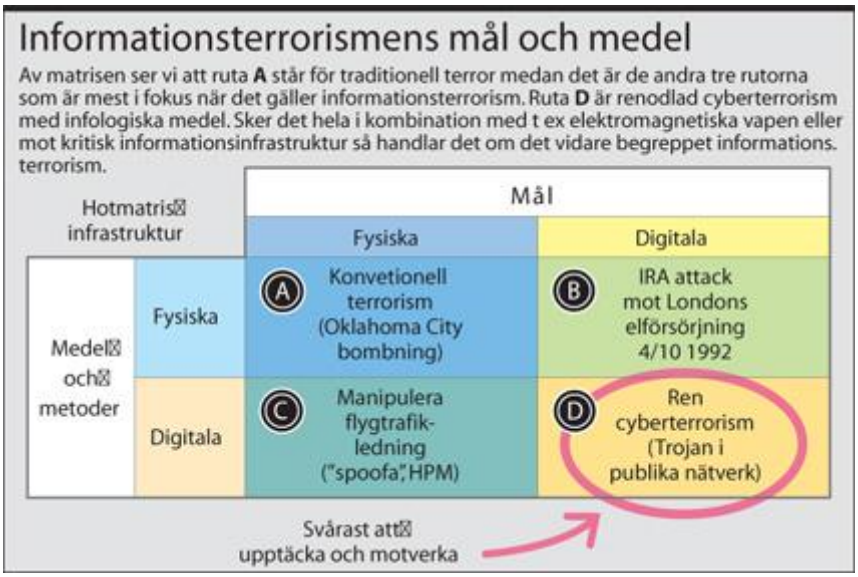
Vid Försvarshögskolan finns avdelningen Centrum för informationsoperativa studier (Cios). Mellan 1997 och 2002 var Cios även en kanslifunktion för regeringens arbetsgrupper när det gällde dessa frågor. Kanslifunktionen upphörde 2003 och i dag är Cios mer renodlat den enda FoU-funktion i Sverige för dessa frågor.

Vid Cios bedrivs även forsknings- och studieverksamhet på uppdrag av Krisbered-kapsmyndigheten (KBM) rörande policyåtgärder för skydd av kritisk infrastruktur i omvärlden. Under 1999-2001 bedrevs även forskning på uppdrag av Styrelsen för Psykologiskt försvar, vilka förväntas återkomma med uppdrag under 2004. Likaså har Cios samverkat med Rikspolisstyrelsen om polisiära/legala aspekter rörande IT-hot och skydd mot informationsoperationer. På uppdrag från Försvarsmakten/Högkvarteret bedrivs från och med 2003 också en treårig studie rörande psykologiska operationer och perceptionsstyrning.

I dag finns det inte någon forskning i Sverige som rör cyberaspekter på terrorism. Någon sådan forskning finns inte heller på en av världens ledande institutioner för terrorismforskning, St. Andrew´s University i Skottland. Detta har lett fram till en gemensam insikt om att en samverkan mellan Försvarshögskolan/Cios och St. Andrew´s kan ge starka synergieffekter. Bägge institutionerna har två stora databaser på sina respektive områden vilka verksamt kan stödja en sådan forskningsinriktning. Inriktningen handlar alltså om den funktionella terrorismen - vilka medel och metoder terrorister av olika slag använder sig av - till skillnad från traditionella terrorismforskningen, area studies, som fokuserar kring ideologiska och religiösa motiv samt kulturella och etniska särarter etcetera.

Ett övergripande långsiktigt syfte är att försöka etablera Informationsoperationer (IO) som ett akademiskt ämne/inriktning inom den statsvetenskapliga sfären. Vetenskaplig rådgivare är Dr. Magnus Ranstorp vid St Andrew´s University. Han är sedan 2003 knuten till Centrum för IO-studier som gästprofessor.

Terrorismen byter skepnad



När bedömer en terroristledare att attacker med infologiska eller elektromagnetiska medel kan ge samma mediala effekt som konventionella terroristattacker? Den frågan står i fokus på Försvarshögskolans avdelning Centrum för informationsoperativa studier (Cios).

Av Lars Nicander

Hittills har terroristorganisationer prioriterat att det ska säga ”pang” snarare än att använda sofistikerad teknik och internet-angrepp - främst beroende på att de sekundära medieeffekterna är det som skapar den uppmärksamhet och det politiska tryck som terroristorganisationerna är ute efter.

Problematiken kring informationsoperationer (IO) och skydd mot detta är ett angeläget område som betonats i flertalet av statsmakternas styrdokument under senare år. Ett viktigt delområde är cyberterrorism och statsmaktsåtgärder för att förebygga ett sådant framväxande hot. Informations-/ cyberterrorism är till sin natur en tvärsektoriell fråga, där säkerhetspolitiska, juridisk/polisiära och tekniska aspekter möts.

På Centrum för informationsoperativa studier (Cios) har arbetet hittills fokuserats på att försöka ge en kvalificerad bedömning om när den traditionella terorrismen och informationsterrorismen kommer att mötas.

Mångfunktionella
Informationsoperationer är till sin karaktär mångfunktionella. De kan - i samverkan med underrättelsetjänst - rangeras in som de förmågor som samhället behöver för att hantera asymmetriska hot.

IO handlar här om:

- skydd - informationstekniskt och perceptionsmässigt,
- policy - säkerhetspolitiskt, strategiskt och folkrättsligt
- samt den militära operativa kärnkompetensen med åtgärder/motåtgärder (informationskrig, ledningskrig, dator- och nätverksoperationer och psykologiska operationer).

Detta måste alltså byggas på en grund av en vitaliserad underrättelse- och säkerhetstjänst för att detektera aktörer (cyberterrorister etcetera) vilka kan tänkas utnyttja nya hotmöjligheter.

Informations-/cyberterrorism kan här betraktas som ett specifikt delområde vid sidan av viktigare övriga delområden som skydd av kritisk informationsinfrastruktur (strategisk CIIP), perceptionsstyrning samt underrättelsetjänst.

Terrorismens karaktär
För att närmare dissekera informationsterrorismens karaktär kan följande matris ställas upp (se inledande illustration).

Av matrisen ser vi att ruta a står för den traditionella terrorn, medan det är de andra tre rutorna som är mest i fokus för oss beträffande informationsterrorismen. Ruta d är renodlad cyberterrorism med infologiska medel. Sker det hela i kombination med till exempel elektromagnetiska vapen eller mot kritisk informationsinfrastruktur så handlar det om det vidare begreppet informationsterrorism.

Om en terrorist med ett elektromagnetiskt vapen exempelvis lyckas störa ut ett flygplan som landar på Schipol och planet störtar med cirka 400 döda, och att man samtidigt dokumenterar detta med videokamera eller rent av en kameramobil med en kognitv sekundäreffekt som följd, så torde vi få en 11 september-effekt.

Vi har ju ännu inte sett något konkret genomfört fall, men det har ju funnits flera tecken på planeringar från såväl IRA, Aum Shinrikyo och al-Qaida.

Aum Shinrikyo är ju en terroriströrelse med en à la carte-meny. Där handlade det inte bara om att hålla på med sarin i Tokyos tunnelbana. Man bedrev även utveckling av radiologiska och biologiska stridsmedel, samt med mjukvarumanipulering där både civila och militära japanska ledningssystem exploaterades.

I al-Qaidas fall fanns det i de interna videofilmer, vilka återfanns i Afghanistan, detaljerade planer för attacker på infrastrukturen i västra USA - bland annat styrdatasystemen i kraft- och vattenanläggningar.

Dyster bedömning
Vid en workshop med internationell expertis som genomfördes i november 2003 på Gällöfsta utanför Stockholm, var bedömningen om när den traditionella terorrismen och informationsterrorismen kommer att mötas mer sinister än väntat. Frågan var om det handlade om ett år, fem år eller tio år. Vissa amerikanska bedömare och organisationer har hittills varit de mest pessimistiska med att en rimlig tidshorisont ligger kring fyra år. På Gällöfstaseminariet visade det sig dock att det fanns annars vanligtvis konservativa internationella bedömare som menade att tidshorisonten sjunkit till ett år.

Ett brett samhällsförsvar för informationsåldern måste fokuseras kring ett antal studieområden för IO. Det måste också bygga på en grund av en vitaliserad underrättelse- och säkerhetstjänst för att detektera aktörer (cyberterrorister etcetera) som kan tänkas utnyttja nya metoder för att uppnå operativ verkan.

Avsaknaden av fantasi och out-of-the-box-tänkande var ju till exempel det som ordföranden i den amerikanska 11 septemberutredningen, senator Thomas Kean, framhöll som den främsta faktorn bakom det amerikanska misslyckandet att förhindra al-Qaidas attack. Denna faktor kom till och med före den annars vanligaste förklaringen om för lite samverkan och för mycket stuprörstänkande på underrättelseområdet. Kanske en del av detta också gäller för Sverige?

Lars Nicander är chef för Centrum för informationsoperativa studier (Cios) vid Försvarshögskolan.

Så ser regeringen på informationsoperationer

Informationsoperationer är samlade och samordnade åtgärder i fred, kris och krig till stöd för politiska eller militära mål genom att påverka eller utnyttja motståndares eller annan utländsk aktörs information och informationssystem. Det kan ske genom att utnyttja egen information och egna informationssystem samtidigt som dessa också måste skyddas. Ett viktigt inslag är att påverka beslutsprocesser och beslutsfattande.

Det finns både offensiva och defensiva informationsoperationer. De genomförs i politiska, ekonomiska och militära sammanhang. Exempel på informationsoperationer är till exempel informationskrigföring, massmediemanipulation, psykologisk krigföring och underrättelseverksamhet.

Defensiva informationsoperationer är samordnade och samlade åtgärder i fred, kris och krig avseende policy, operationer, personal och teknik för att skydda och försvara information, informationssystem och förmåga till rationellt beslutsfattande.

(Prop 1999/2000:86, sid 36).

Trovärdighet är allt

För att kunna genomföra psykologiska operationer krävs det goda kunskaper om hur man skapar säljande budskap. Principerna liknar dem som gäller för marknadsföring. Budskapen måste hela tiden anpassas efter målgruppen. Trovärdigheten i budskapen är helt avgörande för om den ska få någon effekt.

Av Fredrik Konnander

Varje dag nås vi av olika budskap. De kan till exempel vara kommersiella för att få oss att köpa en vara eller tjänst, de kan vara politiska för att få oss att rösta på ett parti eller på annat sätt engagera oss, eller budskap som kommer från andra typer av organisationer. Budskapen har dock samma syfte, nämligen att påverka oss så vi förändrar våra uppfattningar eller förstärker våra redan bestämda uppfattningar på ett sätt som gynnar avsändaren av budskapet. Ofta är vi så vana vid budskapen att vi sällan lägger märke till dem, men de påverkar oss ändå. Denna typ av påverkan återfinns självfallet även inom den militära sektorn. Det finns många olika benämningar på militära motsvarigheten men en av de vanligaste är psykologiska operationer (psyops). Psyops kan nästan liknas vid militär marknads-föring, där man i stället för att sälja en produkt säljer en idé.

En svensk tiger

Sverige har under lång tid ägnat sig åt skydd mot psykologiska operationer. Ett klassiskt exempel som nästan alla känner till är ”en svensk tiger”, som syftade till att öka säkerhetsmedvetandet. För att hitta exempel på tillfällen då psyops har använts för att sprida budskap måste man gå tillbaka till andra världskriget. Ett exempel på framgångsrik psyops under andra världskriget är den kampanj som genomfördes för att övertyga svenskarna om att de skulle spara pengar i de så kallade försvarslånen som drog in 2,3 miljarder kronor i dåtidens penningvärde. Går man längre tillbaka i tiden så kan man hitta Gustav II Adolfs försök att spela på den tyska myten om ”Lejonet från Norden” som skulle komma och befria den protestantiska befolkningen i Tyskland från det ”katolska oket”.

Om svensk militär sätts in i framtiden är chansen stor att det kommer att genomföras utanför Sveriges gränser inom ramen för internationella insatser. Insatserna skulle kunna vara av de typer som benämns fredsframtvingande eller fredsbevarande.

Dagens svenska militära organisation ger en chef främst möjligheten att agera med våld. Om Försvarsmakten väljer att skapa förband för psykologiska operationer ges den militära chefen möjlighet att agera med ytterligare ett instrument. Chefens möjlighet att agera utökas då han ges ett instrument som kan lösa situationer där möjligheten att kommunicera med sina målgrupper innebär att man inte behöver ta till våld. Det kan innebära att chefen kan lösa uppgiften med mindre risk för både egen personal, motståndaren och civilbefolkningen i området.

Praktiska exempel

Även om svenska förband skulle tvingas till att använda våld finns det även där en roll för psyops. Det finns många praktiska exempel på när uppmaningar till militära enheter om att de ska ge upp har visat sig mycket verkningsfulla. I många av dessa fall har budskapet att ge upp motståndet genomförts i form av psyops med någon annan form av aktivitet som har psykologisk påverkan, till exempel beskjutning med olika stridsmedel. Under Gulfkriget 1991 hade ett stort antal av de irakiska soldaterna som togs till fånga flygblad, så kallade Safe Conduct Passes, där koalitionen lovade att ge skydd, mat och arabisk gästfrihet till de irakiska soldaterna som gav upp. Trovärdigheten i dessa budskap bedöms ha varit hög då det var belagt med dödsstraff i irakiska armén att inneha dessa flygblad.

Psykologiska operationer har även använts med framgång i fredsbevarande operationer. Bland annat har svenska förband i Bosnien och Kosovo ibland använt sig av verksamhet liknande psyops för att kommunicera budskap till olika målgrupper. Många av dessa insatser har skett i samverkan med andra funktioner som till exempel civil-militärt samarbete (Cimic), där uppgiften för psyops har varit att förstärka effekten av de egna, oftast humanitära, insatserna.

Utmaningar och kunskapsbehov

Trovärdigheten i de budskap som lämnas i psyops är helt avgörande för om de skall få någon effekt. Det är därför av yttersta vikt att agerandet från de egna styrkorna står i samklang med de budskap som lämnas. Trovärdigheten försvinner snabbt om man kommunicerar att man kommer som befriare, för att därefter agera på ett sätt som är mindre demokratiskt.

För att få trovärdighet krävs mycket god kunskap samt samordning av alla budskap som lämnas, från strategisk till taktisk nivå. Detta ställer stora och delvis nya krav på militära chefer på alla nivåer.

Planering, genomförande och utvärdering av psykologiska operationer kräver goda baskunskaper inom ett antal områden. Kunskapsfälten som behövs sträcker sig över antropologi, sociologi, historia, ekonomi, marknadskommunikation, kommunikationsvetenskap för att bara nämna några. Ska Försvarsmakten genomföra psyops står det klart att Försvarsmakten aldrig kommer att kunna ha dessa kunskaper själv utan måste sannolikt arbeta i nätverk med övriga delar av samhället för att kunna få tillgång till denna kunskap.

När man skall planera och genomföra psyops krävs mycket god kunskap om de målgrupper man vill påverka. Detta ställer delvis nya krav på underrättelsetjänsten att lämna underlag. Man måste också ha goda kunskaper om hur man skapar säljande budskap, där principerna är mycket lika de som gäller för marknadsföring. Även kunskap om lokala medievanor kan vara avgörande. Är målgruppen van att söka på internet efter information kan nätet vara det ställe vi skall genomföra vår psyops. Är målgruppen däremot van att lyssna på musik för att få sina information kanske vi skall hyra sångskrivare och ett band för att framföra våra budskap. Budskapen måste hela tiden vara anpassade efter målgruppen vi vill påverka, för det är faktiskt de som bestämmer om de vill acceptera våra budskap eller inte.

De produkter som ska lämnas måste också testas innan de ges spridning. I den optimala situationen kan produkterna testas på någon från den målgrupp som ska påverkas. Likaså måste man kunna undersöka resultatet av de genomförda insatserna. Principerna för detta är liknande de som används för marknadsundersökning. Dock kan det vara svårt att få reda på budskapens effektivitet under en pågående operation.

Psyops kan rätt använd vara en funktion som ger ett förband mereffekt då de ska lösa sin uppgift. Funktionen kräver resurser men kan också leverera resultat som kan vara mycket svåra att nå med konventionella militära medel. Det kan därför vara intressant att notera att Försvarsmakten har i alla förslagna nivåer i försvarsbeslutsunderlaget tagit med enheter för psykologiska operationer.

Fredrik Konnander är lärare i psykologiska operationer och underrättelsetjänst vid Försvarshögskolan. Han är major i reserven och var 1991-2000 vid Högkvarteret och är utbildad vid amerikanska arméns underrättelseskola.

Fredsuppdrag kräver kulturell förståelse

Svenska styrkor är i dag engagerade i konflikter över hela världen. Psykologiska operationer (psyops) kan vara en metod för de fredsfrämjande styrkorna att minska fientligheten mellan stridande parter. För att kunna genomföra dessa operationer krävs dock en ingående kunskap om såväl den kulturella situationen i landet som de stridande parternas propaganda.

Av Kersti Larsdotter

Psykologiska operationer (psyops) är främst ett medel för att påverka männi-skors attityder och beteenden i en konflikt. Därigenom kan psyops vara en bra metod för att minska fientligheten mellan stridande parter, sänka potentialen för våld och bygga upp förtroendet mellan parterna i ett konfliktområde. Då detta är några av de viktigaste uppgifterna för fredsfrämjande operationer har psyops blivit en allt viktigare del i dessa operationer.

Internationella insatser har under senare år blivit en av Försvarsmaktens huvuduppgifter och därigenom kan även psyops bli en viktig del av Försvarsmaktens uppgifter framöver. Den svenska psyops-förmågan befinner sig i dag dock på en relativt rudimentär nivå och det finns många frågor som behöver diskuteras under den fortsatta utvecklingen. Hur fungerar då psyops? Vilka problem kan uppstå i denna process? Hur kan svenska styrkor förbättra sin psyops-förmåga?

Kulturella skillnader
Kulturella skillnader är ett tydligt problem vid internationella insatser där insatsstyrkorna kommer från en annan kultur än befolkningen i ett konfliktområde. Dessa skillnader kan enkelt leda till en situation där de internationella styrkorna ökar spänningen i ett område, till exempel genom ett beteende som bryter mot den lokala sedvänjan, och därigenom motarbetar målen för den fredsfrämjande operationen. Men kulturella skillnader är också ett stort problem vid effektiv användning av psyops.

Det finns många exempel på fredsfrämjande operationer där psyops inte har fungerat som planerat. I Bosnien hade man till exempel problem med att målgrupperna inte tog till sig de psyops-produkter som Ifor spred ut, vilket ledde till att vissa mål inte kunde uppnås. Varför blev det så? Varför betedde sig

målgrupperna inte som beräknat? För att förstå hur man ska utforma budskap som helt assimileras av målgruppen måste man förstå hur attityder formas, hur människor uppfattar sin omgivning och vilken påverkan symboler kan ha.

Kulturella tolkningsramar
Enligt socialkonstruktivismen är vår uppfattning och kategorisering av omvärlden primärt en produkt av historiskt och kulturellt specifika föreställningar. Människor strukturerar, förstår och uppfattar världen utifrån tidigare erhållna kunskaper och erfarenheter. Meningsskapandet av omvärlden är således en process där man tolkar nuet genom sina föreställningar om sitt förflutna, genom sina så kallade tolkningsramar.

Eftersom människors tolkningsramar och sociala identitet är konstruerade av byggstenar från exempelvis historia, geografi, biologi, religion, kultur och kollektiva minnen, kan representationer, både visuella och verbala, ha helt olika mening för olika människor. Enligt en analys av verksamheten i Bosnien berodde vissa problem på att man förtestade psyops-produkterna i områden vars kontext till stor del skilde sig åt från de områden där produkterna skulle användas. Till exempel testades vissa produkter i Sarajevo, vilka sedan skulle spridas på den bosniska landsbygden. Eftersom landsortsbefolkningen inte hade samma tolkningsramar som grupperna i Sarajevo kunde de inte relatera till de utsända budskapen.

För att förstå hur människor i en viss kontext uppfattar sin omgivning och vilka idéer de kopplar samman med vissa symboler och situationer, måste man således förstå deras tolkningsramar. Detta kan till viss del uppnås genom en analys och fördjupad förståelse av de byggstenar målgruppens tolkningsramar är uppbyggda av det vill säga kultur, historia, politik, språk med mera.

Propagandaanalys
För att kunna utforma effektiv psyops räcker dock inte en detaljerad analys av målgruppens kontext. Man måste även ha förmågan att tolka denna kontext utan influenser från egna värderingar och tolkningsramar. En metod för att underlätta denna process kan vara att analysera de stridande parternas propaganda mot befolkningen i konfliktområdet.

Eftersom stridande parter i lågintensiva konflikter ofta är beroende av stödet från det lokala samhället, och ofta använder sig av propaganda för att uppnå detta, är det troligt att de har utvecklat en nära förståelse för den lokala befolkningens tolkningsramar. Eftersom dessa grupper ofta kommer från samma miljö, har samma kultur, samma språk etcetera som målgruppen, är det mer troligt att de har en större förståelse för dessa tolkningsramar än de internationella styrkorna.

Genom att analysera de stridande parternas propaganda mot befolkningen i området torde man således kunna hitta viktiga noder i befolkningens tolkningsramar, viktiga symboler, som kan användas vid utformningen av budskap.

Nya utmaningar
Användning av psyops och målen för fredsfrämjande operationer har lett till ett stort behov av detaljerade underrättelser om konflikters demografiska, politiska, ekonomiska, historiska och kulturella situation, likväl om de stridande parternas propaganda. För att kunna påverka målgruppens attityder måste man även förstå hur deras samhälle fungerar, hur de konsumerar media, vem som har inflytande i samhället och hur beslut tas.

Denna typ av underrättelser (så kallade kulturella underrättelser) har traditionellt inte prioriterats utan endast i undantagsfall uppmärksammats, och då vanligen på strategisk nivå. Psyops och fredsfrämjande operationer kräver dock denna typ av underrättelser även på operativ och taktisk nivå. Human Intelligence (humint) och Civil Affairs (CA) är två områden som ixxxdag bidrar till denna typ av underrättelser men stora brister existerar ännu.

En metod som på senare tid fått mer uppmärksamhet inom bland annat den amerikanska underrättelsetjänsten är användningen av så kallade Human Factor Analysis (HFA), där alla ovanstående faktorer tas i beaktande. Precis som övriga områden har dock detta traditionellt setts som strategiska underrättelser, och tyvärr är de flesta analyser fortfarande på en strategisk/operativ nivå som stöd för beslutsfattare och högre militära chefer, även om vissa framsteg på taktisk nivå har skett.

Samarbete viktigt
Dessa nya behov av kulturella, icke-traditionella underrättelser på operativ och taktisk nivå har lett till att nya problem har uppstått. Genom tidigare erfarenheter från fredsfrämjande operationer har man upptäckt svagheter, särskilt inom underrättelsearkitekturen och i samarbetet med civila organisationer.

I Bosnien blev det tidigt uppenbart att andra källor än de tänkta blev viktiga källor till kulturella underrättelser, till exempel de taktiska psyops-teamen, och ett behov av samarbete mellan flera olika

källor uppstod. På grund av brist på standardiserade arbetsmetoder för dessa processer blev dock samarbete och synkronisering ett avsevärt problem och trots daglig koordinering mellan brigadens psyops och humint-celler spreds inte underrättelserna från psyopsteamen vidare till de stödda enheternas underrättelseceller.

Även problem med civil-militär samverkan (cimic) uppstod. Så kallade Non Governmental Organisations (NGO) har ofta en omfattande lokal kännedom om historia, kultur, konfliktdynamik och lokala beslutsstrukturer tack vare långvarig närvaro i konfliktområden och de kan ofta gå förbi lokal byråkrati på grund av väl utvecklade nätverk. Dessa uppgifter har tidigare skötts av bland annat CA men på grund av det ökade behovet av kulturella underrättelser ses samarbete med NGO:s som en allt mer viktig underrättelsekälla.

Trots hundratals NGO:s i konfliktområdena i exempelvis Kosovo och Bosnien, har dock samarbetet med dessa organisationer varit dåligt strukturerat och flera problem har uppstått på grund av oenigheter inom underrättelseutbyte och brist på grundläggande förståelse för värdet av Cimic hos lägre chefer.

Konsekvenser för svenska styrkor
Psyops är i dag en viktig del i fredsfrämjande operationer med potential att stävja våldsamma konflikter. Detta betyder inte att psyops är lätt att hantera. De mänskliga processerna bakom skapandet av världsbilder och attityder är mångfacetterade fenomen som måste studeras ur flera aspekter för att psyops ska kunna utvecklas till en mer effektiv nivå.

Det finns naturligtvis andra problem som också behöver studeras för ett effektivt användande av psyops, till exempel hur man ska kunna mäta effekten av psyops med en större precision eller hur man ska handskas med de problem som uppstår på grund av det nära avståndet mellan den strategiska och taktiska nivån, men inga av dessa frågor kommer att vara viktiga om den kulturella aspekten av psyops glöms bort.

I dag är svenska styrkor engagerade i konflikter över hela världen och i flera fall är de kulturella skillnaderna uppenbara, i exempelvis Afghanistan, Kosovo, Liberia och Kongo. För att kunna genomföra effektiv psyops och öka potentialen för lyckade fredsfrämjande operationer behöver de svenska styrkorna en ingående kunskap om kulturens roll i dessa operationer.

En förståelse för att kulturen är en integrerad del av genomförandet av psyops och att detta bland annat leder till nya underrättelsebehov och krav på inhämtning är därmed viktig. Dagens krav på detaljerad och integrerad underrättelse och planering har lett till att problem uppstått inom till exempel samarbetet mellan olika militära funktioner och med civila organisationer. För att svenska styrkor ska kunna genomföra effektiv psyops och öka sin förmåga behövs en ingående förståelse för denna typ av problematik.

Kersti Larsdotter är forskningsassistent i militärteori vid Försvarshögskolans krigsvetenskapliga institution.

Sociala nätverk viktig resurs i nya försvaret

Innan det nätverksbaserade försvaret byggs upp rent tekniskt borde de nätverk som redan finns - de sociala nätverken - tas till vara. Att organisera en funktion som kan fånga upp personlig kompetens, kunskap och erfarenhet vore ett värdefullt bidrag för en nation med internationella ambitioner. Det skriver Petter Larsson på Försvarshögskolan.

Av Petter Larsson

Ett alltmer nätverksbaserat försvar och samhälle ställer nya krav på teknisk förståelse och komplex interaktion mellan tekniktung verksamhet. Mot den bakgrunden kan man fråga sig i vilken utsträckning nationella organisationer och näringslivsorganisationer tar tillvara de nätverk som redan finns - de sociala nätverken. Innan vi ger oss in i den tekniska lösningen bör vi fråga oss själva hur väl vi tar hand om de befintliga nätverken, tar vi tillvara de möjligheter som redan finns? Frågan är relevant, inte bara i underrättelsekretsar utan även ur ett bredare nationellt perspektiv.

I denna artikel presenteras hur en organisation kan arbeta med sitt relationskapital och medvetengöra dess värde för att implementera detta som en del av arbetet med kunskaps- och informationshantering. Ett förslag på att utveckla detta vidare lämnas genom att en särskild metodik, kallad relationsföring,

introduceras som ett strategiskt kunskapsverktyg. Relationsföring syftar till att underlätta koordinering samt utveckling av kommunikationen genom personliga relationer och bidra till att stärka organisationens omvärldsuppfattning. Sammanfattningsvis tas ett helhetsgrepp på synen på organisationers sätt att använda personliga relationer. Tre alternativa sätt att förhålla sig till relationskapitalet presenteras.

Det är naturligt att organisationer utnyttjar sina befintliga relationer och nätverk. Oftast sker detta emellertid på ett icke-koordinerat och icke-strukturerat sätt. Personliga kontakter inleds, underhålls och avslutas, för att uttrycka det enkelt, från höften och ofta helt reaktivt. Relationsföring skulle kunna utgöra ett framtida strategiskt verktyg för organisationer som har insett värdet av sitt sociala kapital, det vill säga sitt relationskapital. På ett mer systematiskt sätt skulle detta kunna införas i utbildning och i uppmuntrande diskussion kring organisationens tillvaratagande av sitt relationskapital och hur detta kan utvecklas vidare.

Presentation av relationsföring
Hur kan en organisation använda den teoretiska kunskapen kring relationer, och omsätta och föra in den i den praktiska verksamheten? Självklart finns det flera sätt - i allra högsta grad är varje organisation unik och kräver sin unika lösning. Här presenteras några tankar kring hur ett förslag skulle kunna se ut. Syftet är att visa ett alternativt sätt att förhålla sig till sitt eget och sin organisations sociala nätverk.

Relationsföring kan enklast beskrivas som en sorts rationalisering av de personliga relationerna i och kring en organisation. Detta skulle möjliggöra för en organisations beslutsfattare att förstå, tolka, kommunicera med och påverka utvalda personer såväl internt som externt. Relationsföring bör alltså betraktas som en metodik för riktad kommunikation och relationsutveckling. Behovet av att ha goda personliga relationer med interna såväl som externa nyckelpersoner finns ju hos alla organisationer.

Tre alternativ
En organisation har i princip tre möjligheter att förhålla sig till utvecklingen av sitt sociala kapital och sin förmåga att tillvara den kunskap och de möjligheter detta nätverk innehåller.

Det första alternativet innebär att man inte engagerar personal för relationshantering, inte heller att medarbetarna i någon form uppmuntras att utbilda sig inom styrkor och svagheter med personliga relationer och hur dessa kan utvecklas. En organisation som väljer detta alternativ riskerar att utgöra en av de mindre drivande eller ledande organisationerna inom ramen för individ- och organisationsutveckling. Att uppmuntra personliga relationer och social utveckling får anses som mycket viktigt för moderna organisationer.

De mer konstruktiva och framåtskridande handlingsmöjligheterna utgörs av följande två riktningar. Ena riktningen innefattar hela organisationen och den andra riktningen innebär att en särskild enhet rekryteras och organiseras. Här redogörs för styrkor och svagheter hos de bägge alternativen.

Hela organisationen
Ett företag som väljer att sträva efter att höja den lägsta nivån på social insikt och utveckla sin personals syn på personliga relationer och sin egen roll däri vinner flera fördelar. En av de främsta fördelarna är att man aktivt tillvaratar de värden som de mångfacetterade sociala nätverk organisationens anställda utgör, inte bara internt utan även externt. Genom etisk och positiv utbildning inbjuder man organisationsmedlemmar till dialog om nätverksutveckling och relationer och vilken kunskap dessa kan innehålla. Relationsutbildning kan vara ett sätt att uppmuntra ett aktivt och konstruktivt informationsutbyte inom och utom organisationen. Enkelt uttryckt bidrar det till att organisationen får fler relationer och därigenom kunskap och access till nya och tidigare outnyttjade nätverk, men också möjlighet att sända sina egna budskap i den nya riktningen.

Genom att öka medvetenheten om organisationens och medarbetarnas samlade sociala nätverk ökar möjligheterna att sända och kommunicera kunskap med bredd. En naturlig fortsättning på detta är att man genom att öka den sociala insikten dessutom ökar möjligheter att fånga upp svaga signaler i omvärlden. Signaler som kan fångas in, följas upp och undersökas av till exempel organisationens funktion för omvärldsanalys. En brist med detta alternativ är att det i allt väsentligt kommer att vara personer som inte har en särskild utbildning och erfarenhet inom kommunikation och beteendekunskap som uppmuntras att nyttja och utveckla sina och kollegornas personliga relationer för att kommunicera. Det är därför viktigt att man under utbildningen av organisationsmedlemmarna markerar vilka nivåer som är rimliga och vilka etiska och därmed anseendemässiga risker och möjligheter ett ökat relationshanterande medför.

En organisation som väljer detta breda alternativ kommer att ha mindre kontroll och ledningen kommer inte att kunna dirigera och inrikta den nya ”resursen”. Med detta alternativ höjer man i allt väsentligt den

individuella förmågan hos de enskilda anställda vilket i sig är mycket värdefullt men alternativet främjar inte organisationen som helhet avsevärt.

Detta alternativ medför således inte nödvändigtvis att organisationens ledning får ett nytt verktyg. Det stärker organisationen på bredden, men inte på djupet. En styrande faktor för hur framgångsrikt en organisation kan höja sin personals lägsta nivå beträffande relationer är den tid och de resurser som avsätts. Genom att hyra in externa konsulter kan man injicera kunskap men knappast vidmakthålla organisationens förmåga över tiden. Denna lösning skulle främst tjäna till att stärka organisationens dagliga arbete och de många dagliga kontakter som organisationens medarbetare handhar skulle utnyttjas optimalt.

En specialistavdelning
Detta alternativ skulle framför allt rikta sig till ledningen av organisationen. Att engagera och organisera en specialistavdelning inom organisationen medför att man tar tillvara det fulla värdet av personliga relationer och medvetet strävar efter att utnyttja hela dess potential. En specialistavdelning medför att ledningen eller annan ges möjlighet att med hög precision, djup och kontroll kommunicera och inhämta kunskap från ett urval av grupper och personer.

En specialistavdelning skulle innebära att högre precision och högre kvalitet i relationsarbetet med nyckelpersoner infrias. Mot bakgrund av att organisationen använder professionella ”relationsförare” skapar man utrymme för ett befäst etiskt förhållningssätt och mindre risk för klavertramp och felutnyttjande. En professionell relationsförare förstår riskerna med ett etiskt vanskligt agerande och dess motsats - värdet av att transparent kommunicera och dialogisera med nyckelpersoner och andra intressenter. Organisationens strategiska arbete skulle sannolikt stärkas genom att specialister stödjer den strategiska ledningen att kommunicera budskap till och förstå nyckelpersoner i organisationens omvärld. En specialistavdelning medför ett ökat behov av granskning och öppenhet kontra det bredare alternativet. Detta smalare alternativ skulle innebära att risken för missuppfattningar skulle öka och vikten av att presentera och introducera denna avdelning på ett skickligt sätt kan inte understrykas.

De anställda i organisationen skulle däremot inte hjälpas av specialistavdelningen i någon större utsträckning. Närmast kan detta alternativ likställas med en ambassadörsfunktion och tillika rådgivarfunktion för ledningen.

Utökad specialistavdelning
Ett tredje alternativ innebär att en utökad specialistavdelning även skulle kunna engageras för att utbilda och rådgiva övriga kollegor i organisationen beträffande relationer och på så sätt främja en ökad social och strategisk insikt. På så sätt förs vinster med det breda alternativet även in i detta ledningsalternativ. För en uthållig utveckling och förvaltning av relationskapitalet och det sociala nätverk som organisationen de facto utgör rekommenderas att organisationen rekryterar en egen specialistavdelning, en relations- och kunskapsavdelning, som kan agera bollplank och utbildningsyta men också utgöra ett precisionsinstrument för ledningens kommunikation och kunskapsutnyttjande internt såväl som externt.

Att organisera en funktion som på ett transparent och etiskt ansvarstagande sätt inventerar personliga kompetenser, kunskaper och erfarenheter vore ett värdefullt bidrag för en nation med internationella ambitioner, inte minst inför militära internationella insatser. Som sagt, nätverken finns redan i dag, men tar vi tillvara informationen, kunskapen och de personliga erfarenheterna de innehåller?

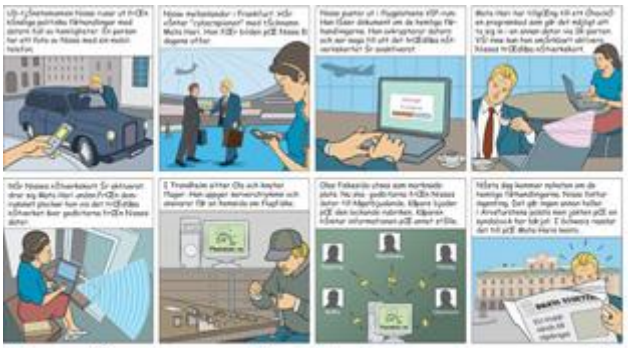
Petter Larsson utvecklar metoder för lägesförståelse vid Centrum för informationsoperationsstudier, FHS.

Kampen om tanken

Informationsoperationer, IO löper längs två vägar – den mjuka och den hårda. Bästa effekten nås när verktyg från två spår samtidigt används. Målet med IO är att påverka motståndarens förmåga och vilja. Man ska få motståndaren att anpassa sig till vår vilja. För att uppnå detta mål måste mottagaren känna igen budskapet. Man kan inte hota med något som denne inte förstår.

Ladda hem Martin Eks illustration "Kampen om tanken" som pdf-fil.

Internet - ny marknad för brottslighet



Klicka på serien ovan för att ladda hem den som pdf-fil.

Brottsligheten tros skapa virtuella miljöer på nätet. Avancerade tekniska lösningar och metoder används. Dessa brottslighetens nya arenor är mycket svåra att hitta. Vardagsteknik som fildelning kan också användas för att planera mörka gärningar.

Av Malin Fylkner

Mycket talar för att kriminella i större utsträckning kommer att använda sig av teknikens möjligheter - inte enbart för att komma över känslig information utan även för att sälja denna till en vidare, men sluten, krets.

Den ensamma hackern är sällan ett kvalificerat hot. Hackern vill briljera med sin teknik och inte genom att störta regeringar eller tjäna pengar. Det som utmärker ett mer kvalificerat IT-relaterat hot är att det finns en bakomliggande aktör med avsikt och förmåga att uppnå viss strategiskt viktig verkan.

Olika aktörer väljer olika sätt beroende på vilka resurser som står till buds - och i vilket sammanhang som aktören verkar. Den som har råd kan köpa den kompetens som fattas. Och den som har kompetensen behöver inte vara rik.

För att ett hot ska vara kvalificerat utifrån ett nationellt säkerhetsperspektiv räcker det inte med att det finns en aktör med vilken förmåga och intention som helst. Det krävs en högre förmåga för att genomföra ett IT-relaterat angrepp med syfte att skada den nationella säkerheten än att skaffa känslig information om en konkurrent. Med utgångspunkt från ovanstående resonemang kan en matris skapas för att illustrera tre olika aktörskategorier:

- icke kvalificerad antagonist,
- icke-antagonistisk kvalificerad aktör
- kvalificerad antagonist.

I FOI-rapporten Aktörer, antagonister och angrepp - En studie om det kvalificerade IT-hotet har olika aktörstyper analyserats och placerats in i ovan nämnda kategorier. Det finns relativt få kvalificerade antagonister ur ett nationellt perspektiv; de som identifierats är statliga säkerhets- och underrättelsetjänster samt organiserad brottslighet.

Högteknologisk brottslighet
Brottssyndikat använder internet allt mer. Traditionella brott som utpressning och bedrägerier sker nu med internet. Brottslingarna anpassar snabbt sin verksamhet. I takt med att nätet erbjuder nya möjligheter till lukrativa affärer flyttar den brottsliga verksamheten efter. Kriminella misstänks rekrytera programmerare . I Sverige har de IT-relaterade brotten ökat kraftigt de senaste åren. Rikskriminalen talar om en fördubbling av antalet anmälningar. Dock råder ett stort mörkertal. En majoritet av de drabbade polisanmäler inte.

Kontokortsbedrägerierna ökar dramatiskt. Personer blir av med sina kontouppgifter (exempelvis kortnummer och giltighetsdatum). Ofta sker detta genom att bedragare kommer över databaser hos e-handelsföretag vartefter uppgifterna används för att handla på nätet.Vi ser även en begynnande byteshandel med kreditkortsinformation via filbytartjänster som exempelvis Kazaa.

Hotet från den organiserade brottsligheten mot Sveriges säkerhet är främst indirekt. Det är svårt att tänka sig att denna aktörsgrupp skulle slå mot den nationella säkerheten, exempelvis genom iscensättandet av en större infrastrukturell attack.

Gruppen är snarare intresserad av ekonomisk vinning och vill knappast såga av den gren de själva sitter på. Däremot skulle deras brott på sikt kunna leda till väsentliga ekonomiska konsekvenser för samhället genom undanhållande av skatteintäkter, penningtvätt och så vidare. Om staten inte kan hantera denna brottslighet, vilket troligtvis kommer att bli än svårare i framtiden, kan medborgarnas förtroende för rättssystemet minska.

Virtuella miljöer
Det är viktigt att studera framväxten av så kallade virtuella miljöer och den roll som de troligen kommer att spela i egenskap av arenor för kvalificerade IT-relaterade hot. Internet är ett forum som kan stärka

demokratin, men detta forum kan givetvis också missbrukas. Ett exempel är distributionen av musik på nätet via fildelningsprogram.

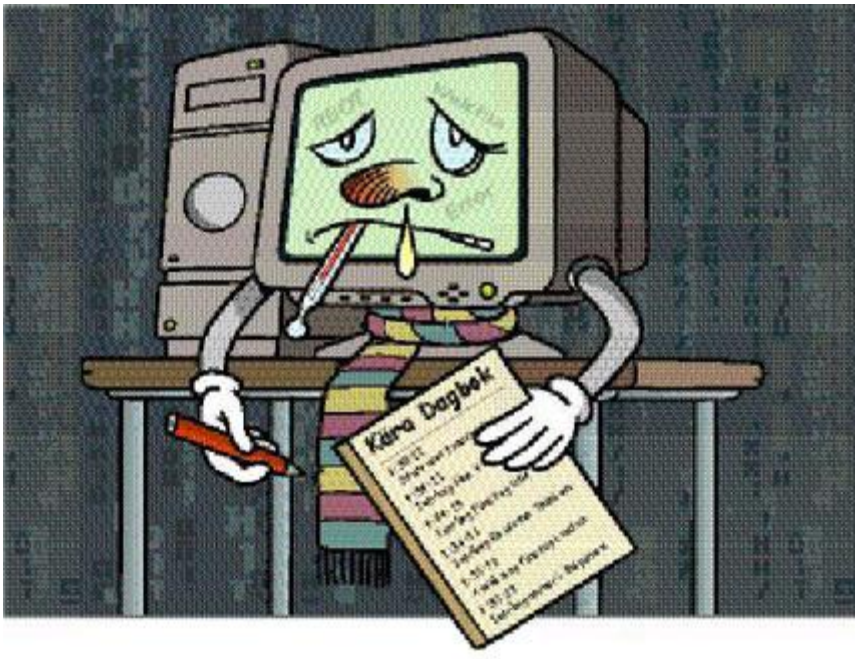
Detta har rönt stort intresse, både från musiktörstande och från musikindustrin som desperat försöker säkra sina tillgångar. Varför är detta exempel intressant? Jo, därför att denna musikindustrins kamp à la David och Goliat har drivit utvecklingen mot mer dolda nätverk som använder sofistikerade fildelningsprogram. Man kan tänka sig att farligare aktörer än musikintresserade kan använda sig av dessa program.

Virtuella miljöer där kriminella skaffar kontakter och utbyter information tros få större betydelse. Utbytet av kreditkortinformation via filbytartjänster pekar i denna riktning. Huvudtanken med de virtuella nätverken och miljöerna är att de ska hindra obehöriga.

Detta möjliggörs genom att de är svåra att hitta och inga krypteringsnycklar delas ut förrän förtroende etablerats. Metoder för initiering av nya medlemmar utvecklas redan i dag. Ofta bygger de på att medlemskap erhålls genom att personer rekommenderas av medlemmar. Det finns alltså redan nu en dold och säker handel på internet. En annan trend, som väntas få stort genomslag bland medlemmarna i nätverken, är virtuella datalagringsföretag. Man kan tänka sig att datalagringsmöjligheterna används för att på ett distribuerat sätt lagra känslig information som inte kan upptäckas och spåras. Detta kräver program för att sammanställa ursprungsdokumentet. Detta lagringskoncept, som vi inte vet om det finns, borde även vara attraktivt för dem som arbetar med att ta fram illasinnad kod. Denna skulle kunna lagras på olika servrar för att vid ett attacktillfälle plockas ihop och distribueras.

Malin Fylkner, vid FOI:s avdelning för försvarsanalys, har tillsammans med Henrik Carlsen, Birgitta Lewerentz och E. Anders Eriksson skrivit rapporten ”Aktörer, antagonister och angrepp - En studie om det kvalificerade IT-hotet."

Virusattackerna började direkt



En oskyddad dator är ett lätt byte för virus och maskar på internet. Redan efter några sekunders uppkoppling blir datorn attackerad. Utan försvar, i form av virusskydd och brandvägg, är risken stor att datorns hela operativsystem kraschar. Det visar experiment som gjorts på Totalförsvarets forskningsinstitut, FOI.

Av Martin Karresand och Arne Vidström

”Det har bara gått tre minuter sedan det första angreppet och redan sviktar försvaret. Underrättelseinhämtningarna har pågått oavbrutet sedan vi blev upptäckta och anfallsvåg efter

anfallsvåg sköljer oavbrutet över oss. Det verkar som om de andra i gruppen har det minst lika illa. Kalle har visst brutit samman och gått över till motståndarsidan. Allt är ett enda mörker. Jag undrar hur länge till vi kan hålla ut."

Det här skulle kunna vara ett utdrag ur en soldats dagbok i vilket krig som helst. I just det här fallet handlar det om tre datorer som anslöts till internet utan brandvägg, virusskydd eller säkerhetsuppdateringar. Experimentet utfördes för att undersöka vad som händer en dator med standardinställningar när den ansluts till internet. Utgångspunkten var att efterlikna en vanlig hemdator som ägs av någon utan djupare kunskaper om datorer i allmänhet och IT-säkerhet i synnerhet. Operativsystemen som användes var Windows 98, Windows 2000 och Windows XP, vilka är vanliga i hemdatorer. Datorerna användes inte aktivt med surfning, e-post eller dylikt, utan de var bara passivt uppkopplade mot internet. Ändå blev resultatet fatalt för två av tre datorer.

Datorerna var inkopplade i fyra timmar och under den tiden skedde det ständiga avsökningar, intrång - både försök och lyckade. Datorn med Windows XP startade om flera gånger under försöket och efter ett par timmar var muspekaren det enda som fortfarande fungerade, skärmbilden var i övrigt helt svart.

Typ av angrepp avgör krasch
När försöket avslutades visade datorn med Windows 98 inga synbara tecken på intrång eller annan manipulation. Det hade förekommit ganska mycket trafik mot den, men i och med att den nästan inte hade några nätverkstjänster igång så hade det inte hänt något allvarligt.

Datorn med Windows 2000 installerat såg på ytan ut att må bra efter experimentet, men den hade enligt loggfilen utsatts för flera lyckade angrepp. En normal hemdator med Windows 2000 installerat kan alltså vara i en angripares händer utan att ägaren har en aning om det.

Datorn med det nyaste operativsystemet installerat, Windows XP, visade redan efter en kort stund tecken på att allt inte stod rätt till. Den började ge meddelanden om att olika processer i operativsystemet hade kraschat och att datorn är på väg att starta om. Till slut blev skärmen helt svart och det gick inte göra något annat än att röra muspekaren. Det här är tydliga tecken som får användaren att inse att något är fel.

Det här resultatet får dock inte tolkas som att Windows 2000 aldrig kraschar vid angrepp, eller att XP, som kraschade, är sämre. Krascher beror till stor del på vad som angriper.

Både Windows 2000- och Windows XP-datorerna försökte, efter att de blivit smittade, angripa de övriga datorerna i det egna nätet. För en hemanvändare, som har flera datorer sammankopplade i ett nätverk, innebär detta att det räcker med att en dator blir smittad för att de andra ska riskera att drabbas. Det kan också vara så att en fullt uppdaterad och därmed synbarligen säker dator blir infekterad om den har samma användarnamn och lösenord som den först infekterade datorn.

350 olika maskar och virus på nätet
De allra flesta intrång utförs av maskar som rör sig helt automatiskt på internet och mer eller mindre slumpmässigt väljer ut sina offer. Intrången i listan härintill utfördes av maskarna Welchia och RBOT. Trafiken bildade ett bakgrundsbrus av angrepp som alltid finns på internet. Så fort en dator kopplas in mot internet är den också utsatt. Är den då inte fullt uppdaterad och skyddad är intrånget snart ett faktum.

Uppdateringarna som förhindrar lyckade angrepp från Welchia och RBOT kom ut under andra halvan av år 2003. Experimentet visade att det fortfarande finns datorer som är infekterade och sprider maskarna. Dessa datorer är förmodligen inte uppdaterade och saknar virusskydd. Welchia och RBOT är två av ungefär 350 maskar och virus som för tillfället är aktiva på Internet.

Situationen förvärras avsevärt om datorn faktiskt används, vilket får anses vara normalfallet. En hemdator kanske används ett par timmar i veckan för att surfa, skicka och läsa e-post, chatta, ladda ner filer med mera. Alla dessa aktiviteter innebär en betydande risk om inte datorns mjukvara är uppdaterad, det finns virusskydd och en personlig brandvägg. Användaren bör dessutom vara säkerhetsmedveten.

Martin Karresand och Arne Vidström arbetar vid FOI:s institution för systemutveckling och IT-säkerhet.

Maskarna slog till direkt

Vad händer om en dator utan virusskydd kopplas upp mot Internet? FOI gjorde ett experiment med tre olika datorer. Följande lista beskriver några av de händelser som inträffade under de första sex minuterna som experimentdatorerna var uppkopplade mot Internet. Händelser av mindre allvarlig karaktär finns inte med.

9:33:22 Datorerna startas och kopplas upp mot Internet.
9:34:11 Nätet avsöks från ett
värdepappersföretag i New York.
9:34:13 Intrång i Win2000 från värdepappersföretaget.
9:34:41 Nätet avsöks från en bredbandskund hos Deutsche Telecom.
9:34:43 Intrång i Win2000 från bredbandskunden.
9:35:52 Nätet avsöks från ett video-on-demand-företag i London.
9:36:38 Anslutningsförsök mot Win98 från Kina.
9:36:53 Intrång i Win2000 från en bredbandskund hos Pacific Bell i USA.
9:37:29 Flera anslutningsförsök mot Win2000 från Bulgarien.
9:39:15 Intrång i WinXP från en bredbandskund hos British Telecom.

Nytt verktyg ska spåra säkerhetsbrister


Foto: Martin Nauclér

Att spåra säkerhetsbrister i ett datasystem handlar inte bara om teknik. I stället gäller det att undersöka under vilka förutsättningar systemet utvecklades. Först då går det att undvika att bristerna uppkommer igen. Nu har Totalförvarets forskningsinstitut (FOI) tagit fram ett ramverk för att göra det lättare att spåra orsaker till säkerhetsbrister.

Av Lars Westerdahl

Datorsystem innehåller fel och brister. Systemen blir fler, större och mer komplexa. Ofta kopplas de även samman och då ofta via internet. Nya hot dyker upp regelbundet samtidigt som de gamla inte försvinner. Det är troligt att en systemägare förr eller senare drabbas av någon form av incident, till exempel intrång eller virus. Konsekvensen av en incident beror på hur väl förberedd systemägaren är.

De flesta system har olika former av skydd mot hot, men det finns ingen garanti för att det fungerar. En systemägare kan testa säkerheten i sitt system genom att själv angripa det. Oftast sker detta genom att systemägaren hyr en grupp konsulter, populärt kallade Red Team, vilka får i uppgift att försöka ta sig in i systemet och uppnå ett visst mål innanför skyddet. Syftet med ett Red Team är att kunna påvisa systemets tillförlitlighet alternativt få en tydlig fingervisning om vad som behöver åtgärdas i systemets säkerhet. Men det finns begränsningar på vad ett Red Team kan uppnå. Ett Red Team angriper ett existerande system, rapporterar vilka brister som hittats och, om det är noggrant, hur man ska åtgärda dessa brister. De kan däremot inte avgöra hur bristerna uppstod och därmed oftast inte ange hur man ska undvika att liknande brister uppstår. Ett Red Team svarar på frågan vad som är fel, men inte varför det är fel.

Långsiktigt lärande
För att en organisation ska kunna utveckla eller beställa bättre system på sikt, krävs en ökad förståelse

av hur och varför fel uppstår. Även om de fel vi hör talas om är tekniska orsakas de ändå av människor, vilket gör att tekniska problem ofta kan ha en icke-teknisk lösning.

Två grundläggande slutsatser utifrån praktisk erfarenhet är följande:

- De som besitter djup teknisk kunskap inom IT-säkerhetsområdet har ofta dålig insikt i övergripande frågor inom en organisation och/eller dåliga möjligheter att påverka dessa.
- De som ägnar sig åt övergripande frågor saknar ofta insikt i vad IT-säkerhet handlar om på djup teknisk nivå.

På en övergripande nivå ägnar man sig, med rätta, inte åt några tekniska detaljer. Däremot finns möjlighet att påverka exempelvis planering av kompetensutveckling, anställning av personal, anlitande av konsulter, arbetsmiljö, organisationskultur, ansvarsfördelning och många andra viktiga faktorer. Det finns mängder av viktiga faktorer och mängder av komplexa och svåranalyserbara samband mellan dessa. Varje faktor kan påverka säkerheten i enskilda system. För beslutsfattare på övergripande nivåer skulle det vara användbart att känna till vilka konsekvenser olika beslut får för säkerheten. Man kan inte begära att samma personer ska ha goda kunskaper, stor erfarenhet och möjlighet att påverka, när det gäller både djupa tekniska och breda övergripande frågor. Därför vore det mycket önskvärt att kunna påvisa någon form av tydliga kopplingar mellan nivåerna.

De två ovannämnda slutsatserna gäller i synnerhet inom organisationer med kärnområden utanför det informationstekniska. Ett exempel på detta är samhällsviktig infrastruktur där informationsteknik har blivit en kritisk komponent. Ofta har man stora, svåröverskådliga system som dessutom är starkt heterogena både med avseende på teknik och på organisation. Det är inte ovanligt att personer som tidigare arbetat med icke IT-relaterade uppgifter får fler och fler uppgifter inom IT-området trots relativt begränsad vidareutbildning. Dessutom kommer det in rena IT-experter som inte har någon större kompetens inom kärnområdet.

Att spåra bakomliggande orsaker
Ett sätt att få en djupare kunskap om orsaken till att fel uppstår är att studera bakgrunden till hur en brist kom in i ett system. Med detta avses inte enbart att studera de tekniska lösningarna som systemet bygger på utan snarare under vilka förutsättningar som systemet utvecklades. Således är organisation, utvecklingsmetodik, rutiner och så vidare av större intresse än teknik. Ur ett spårningsperspektiv är det alltså mer intressant att studera vad som ledde fram till ett val av teknisk lösning än att studera lösningen i sig själv.

Det är dock inte speciellt vanligt att en organisation utvecklar sina egna system. Oftast köps färdiga lösningar in. Detta kan göra det problematiskt att analysera utvecklingsprocessen för ett system. Men även om en organisation inte har utvecklat sitt system på egen hand finns det ändå beslut fattade, vare sig de är aktiva, passiva eller policybaserade, vilka påverkar vad som köps in. Till exempel måste ett system förvaltas. Beslut som ligger till grund för vilka resurser som tilldelas för underhåll, uppdateringar och kontroll påverkar den totala säkerheten i systemet.

Ramverk ska hjälpa till
Det finns flera orsaker till att säkerhetsbrister förs in eller uppkommer i ett system. Vid Totalförsvarets forskningsinstitut (FOI) har institutionen för Systemutveckling och IT-säkerhet har tagit fram ett ramverk för att spåra orsakerna till säkerhetsbristerna. Syftet med ramverket är att man på ett systematiskt och strukturerat sätt ska kunna undersöka de händelser och bevis som finns, för att därefter kunna dra slutsatser om vad de faktiska orsakerna var till att säkerhetsbristen uppkom. Ramverket bygger på öppna intervjuer och studier av dokumentation rörande organisation och rutiner i den organisation som vill spåra orsakskedjor.

En viktig beståndsdel i ramverket är utnyttjandet av metodiken i grundad teori. Det specifika med grundad teori är att man förutsättningslöst studerar faktiska händelser och iterativt grupperar dessa efter liknande egenskaper. Till slut erhåller man en huvudkategori vilken förklarar alla de ingående händelserna.

Målsättningen är att ramverket ska resultera i att organisationer kan optimera användandet av de resurser som finns till för att få en rimlig nivå på IT-säkerheten.

Lars Westerdahl är forskningsingenjör vid FOI:s institution för systemutveckling och IT-säkerhet.

Boktips:
IT-krigets lagar
Cecilia Hellman
ISBN 91-89683-81-1

Vem är vår fiende i cybervärlden? Finns det neutralitet i cybervärlden? Vilka lagar gäller när nätverken blir slagfält? Folkrätten anger vad som är rätten till krig och vad som är rätten i krig. Vilka regler finns för nätverkskriget?

I boken IT-krigets lagar tar folkrättsjuristen vid Försvarshögskolan, Cecilia Hellman, upp frågan om folkrätten har hängt med i IT-revolutionen.

När informationsarenan har blivit en arena vid sidan av de gängse mark, luft och sjö måste man fråga sig om det finns regler från de tre senare arenorna som är tillämpliga på den nya.

Ett hackerangrepp kunde tidigare inte skapa något större kaos i samhället. Men i takt med att vitala funktioner i samhället är helt beroende av att nätverket håller, kan ett angrepp på nätverket få allvarliga konsekvenser. Ett så kallat datornätverksangrepp (DNA) i stor skala, utfört av en stark aktör, kan få följder som ligger nära effekterna av ett väpnat angrepp.

Folkrätten står här inför en ny utmaning, skriver Cecilia Hellman. Det finns visserligen inga folkrättsliga bestämmelser som förbjuder DNA som sådant, men det innebär inte att inga regler som gäller för det konventionella kriget skulle kunna vara tillämpliga också på det nya cyberkriget.

När hela världen blir ett enda stort Google

Nätverket som organisation och måltavla för attacker är några av de viktigaste frågorna när det nätverksbaserade försvaret (NBF) ska byggas. På senare år har fenomenet nätverk vuxit till en tvärvetenskaplig gren där olika relationer studeras, både biologiska och tekniska. Ett av de mer lyckade, moderna nätverken är sökmotorn Google, vars styrka är att den prioriterar sidor med många länkar.

Av Christian Carling och Henrik Carlsen

Efter en del krånglande och dröjsmål blev det ändå som många hade trott: börsintroduktionen av sökmotorföretaget Google på Nasdaq blev den största introduktionen någonsin. På mindre än fem år har Google blivit den ledande sökmotorn och en av de allra mest använda tjänsterna på Internet. Varje dag besvarar Google mer än 100 miljoner sökförfrågningar.

De flesta som använder Google känner förmodligen inte till den bärande tanke som gjort Google till en så framgångsrik söktjänst. Idén är enkel: Skapa en sökmotor som rankar webbsidor inte bara efter innehåll, utan också tar hänsyn till hur de olika sidorna förhåller sig till varandra. Webbsidor som många andra sidor länkar till kommer högt upp på resultatlistan efter en sökning med Google. Uppenbarligen synes det som om denna strukturella information - det vill säga hur sidorna är länkade till varandra - ger ett mervärde som användarna uppskattar.

Under samma korta period som Google funnits har studiet av nätverk som system utvecklats starkt. Ur många separata vetenskapsområden har det utvecklats en framväxande tvärvetenskaplig disciplin där vitt skilda fenomen studeras: sociala relationer mellan människor (eller djur), sammankopplade tekniska system som internet eller infrastrukturen för elkraftförsörjning, länkad information som i exemplet ovan med Google, kopplingar i biologiska system (neurala nätverk, ”vem äter vem i djurriket”) eller kopplingar i företagsvärlden där produkter, tjänster, leverantörer och underleverantörer tillsammans kan utgöra ett komplext nätverk.

I denna tvärvetenskapliga miljö har en fördjupad och delvis förnyad förståelse växt fram kring generella problemställningar från en rad områden. En viktig förklaring till områdets snabbt växande popularitet är att de metoder som gemensamt utvecklas kan appliceras inom så vitt skilda fält. Omvänt gagnas den gemensamma teoriutvecklingen av experimentellt inflöde från olika områden.

Vi har under några år följt denna utveckling för att finna kopplingar till de utmaningar som Försvarsmakten står inför idag.

Det hänger på relationen
Den centrala utgångspunkten när man studerar nätverkssystem är att ”relationerna spelar huvudrollen”.

För att förstå hur ett komplext, sammankopplat system fun-gerar, förändras, fallerar och förstörs är det viktigare att studera hur systemets delar är relaterade till varandra, och mindre viktigt hur de enskilda delarna fungerar var för sig. I någon mån spelar det inte ens någon roll vad systemet består av; den senaste tidens forskning visar att många komplexa nätverkssystem har stora likheter i översiktlig struktur och dynamik, oavsett vad de består av.

I arbetet att följa den här utvecklingen har följande perspektiv på nätverk använts:

Nätverk som organisation och resurs. Att öka ett systems eller en organisations effektivitet genom att länka samman dess delar på nya sätt. Paradexemplet i detta sammanhang är förstås det nätverksbaserade försvaret (NBF).

Nätverk som hot. Terroristgrupper och andra kriminella är redan i hög grad organiserade som nätverk. Hotet är därför av ny art.

Nätverk som måltavla för attacker. De samhällsvärden som ska försvaras utgörs i hög grad av komplexa infrastrukturnätverk. När nätverken är den centrala resursen för försvaret, kommer de också att vara primära mål för attacker.

Nätverk som verktyg. Har forskare och analytiker de rätta verktygen för att förstå utvecklingen som beskrivs av de tre övriga perspektiven?

Det är på det sistnämnda området vi gjort mest eget arbete, genom att försöka hämta nya verktyg och metoder från olika fält inom nätverksforskningen, och tillämpa dem på problemställningar i vår dagliga verksamhet. Till stor del handlar det om att använda enkla datorverktyg för visualisering och analys av stora datamängder.

Ett exempel på detta är det metodstöd som FOI bistår med i ansträngningarna att analysera den Europeiska försvarsforskningen inom sexnationssamarbetet, där Europas ledande nationer inom försvarsmateriel och -forskning ingår.

Nätverk och hierarki
Ofta görs en distinktion mellan nätverk och hierarki. Revolutionärer har i alla tider propagerat för att gamla hierarkier måste rivas ner, och modet för dagen föreskriver i stället nätverk överallt. I teoretisk mening är en hierarki bara en särskild typ av nätverk, men alla har ändå en bild av vad som skiljer en hierarki från ett nätverk.

Lite schematiskt kan sägas att i gamla tider var det sociala nätverk som var den rådande strukturen i den privata sfären, medan det offentliga livet organiserades med hierarkier. Nu tenderar de två sfärerna att bli allt mer sammankopplade. Vad som också händer är att sociala nätverk tenderar att variera mer över tiden och att människor ingår i många olika nätverk.

Hierarkier är trots allt i många situationer en oslagbart effektiv lösning, och ofta uppstår de spontant. I praktiken visar sig de flesta verkliga system ofta vara blandformer mellan idealtyperna hierarkier och platta nätverk. Internet är återigen ett bra exempel. Peer-to-peer-nätverk (P2P) är distribuerade system som organiseras spontant mellan likvärdiga användare, utan någon central kontroll. Den fysiska infrastrukturen som P2P-trafiken färdas över är däremot tydligt hierarkisk, med internationella långdistanslänkar, nationella stomnät, regionala subnät, ända ner till ditt lokala nätverk. Ironiskt nog är de flesta populära fildelningsnätverk av denna typ av effektivitetsskäl är uppdelade i två typer av noder: vanliga användare och ”supernoder”. Liksom djuren på Orwells farm finner vi alltså att alla P2P-klienter är lika, men en del är mer lika än andra…

Nätverksvärlden är liten...
Sociala nätverk är ofta bra för att exemplifiera olika nätverksfenomen. Devisen ingen är längre bort än sex handslag har kommit att stå för att världen trots allt är ganska liten. Med ett förvånat tonläge kan man få höra att det finns en vänskapskedja mellan dig och Kofi Annan som inkluderar endast sex personer. Kanske än mer förvånande, och sällan nämnt, är att det gäller även mellan dig och en jordbrukare i västra Kina.

Frasen six degrees of separation kom att bli populär efter ett känt experiment som utfördes av den amerikanske socialpsykologen Stanley Milgram på 1960-talet. Det statistiska underlaget i Milgrams arbete är relativt bristfälligt, men nyligen genomfördes en betydligt större e-postbaserad studie med 60 000 deltagare. Även om en del förbehåll har tillkommit i denna moderna forskning, kvarstår det faktum att korta kedjor existerar mellan de flesta människor.

Milgrams experimentet visade inte bara att det existerar korta kedjor mellan människor, utan att det också är möjligt att hitta dem. Bara för att det existerar korta vänskapskedjor mellan människor är det inte alls säkert att de går att hitta. Man kanske har ett vagt hum om sina vänners vänner, men sen? Hur kan man, utan vetskap om hela nätverkets utseende, veta hur man ska navigera? Om man inte känner till nätverkets struktur går det inte att navigera på ett sätt som är optimalt för att hitta de korta kedjorna. Den enda rimliga förklaringen är att nätverket självt måste ha någon egenskap som gör det möjligt att navigera i det, trots lite information.

... men hur ser den ut då?
Hur ser då komplexa, framväxande nätverk som internet och World-Wide-Web egentligen ut? Båda har vuxit explosionsartat under det senaste decenniet och någon ”karta” över hela nätverket har inte funnits förrän flera forskargrupper oberoende av varandra för cirka fem år sedan började kartlägga systemen.

I båda fallen visade sig systemen vara starkt heterogena: majoriteten av alla noder har endast en eller få länkar, medan ett fåtal har ett mycket stort antal länkar. Fördelningen av länkar beskrivs alltså inte av vad som brukar kallas en normalfördelning, det vill säga att det finns ett typiskt antal länkar per nod och att de allra flesta noder har ett länktal som inte skiljer sig så mycket från det typiska värdet. Detta faktum har, som vi ska se, en avgörande betydelse för hur nätverket reagerar på störningar och angrepp och hur information sprids i ett sådant nätverk.

Liknande studier har senare gjorts på ett stort urval av nätverk från en mängd olika områden: ekologiska näringskedjor, biokemiska reaktionsnätverk i celler, olika former av sociala nätverk med mera. Gång på gång återkom samma mönster: de flesta noder har få länkar till andra, ett fåtal har oerhört många.

Gemensamt för alla dessa exempel är att de är nätverk som vuxit successivt över tiden, somliga under ett fåtal år, andra under miljoner år av naturlig evolution. Tanken att det är något i tillväxtprocessen i sig som leder fram till detta återkommande mönster ligger därför nära till hands då man vill skapa en modell för hur dessa nätverk ser ut.

Fysikerna Albert-Lazlo Barabási och Reka Albert formulerade 1999 en enkel modell för växande nätverk. Utgångspunkten är en process där nya noder kontinuerligt läggs till ett existerande nätverk. Om det etableras en länk mellan en ny nod och en gammal nod bestäms av hur många länkar varje nod i nätverket redan har: Om en nod redan har många länkar ökar sannolikheten för att denna nod får ytterligare en länk. Noder som av slumpen tidigt fått fler länkar än genomsnittet kommer alltså att fortsätta att ”gynnas” i den fortsatta utvecklingen. Resultatet är ett nätverk med än struktur som överraskande väl överensstämmer med verkliga nätverk.Denna enkla modell har sedan vidareutvecklats och förfinats av många andra.

Attacker och smittspridning
Frågor kring hur olika typer av nätverk klarar att motstå attacker, och hur robusta de är mot olika typer av fel är förstås centrala i militära sammanhang. Många naturligt förekommande nätverk - av den heterogena typen som beskrevs ovan - uppvisar ett tydligt mönster när det gäller robusthet: de är tåliga mot slumpmässigt uppkomna fel, men väldigt känsliga för riktade attacker.

Egentligen är det inte så konstigt. Om vi slumpmässigt tar bort noder i ett nätverk där det stora flertalet noder endast har ett fåtal länkar, kommer högst sannolikt just dessa att slås ut. Om vi å andra sidan får välja fritt vilka noder vi ska ta bort, väljer vi givetvis de få som är länkade till ett mycket stort antal andra noder. Om dessa noder slås ut kommer en stor del av kommunikationen att hämmas.

En annan intressant aspekt är hur spridning sker på nätverk, exempelvis infektionsspridning eller spridning av datavirus. Om man antar att alla noder, människor eller datorer i de två exemplen, har i genomsnitt lika stora lokala kontaktnät uppkommer en så kallad epidemisk tröskel. Om sannolikheten att smittas ligger under denna tröskel kan inte spridning ske till hela populationen, i annat fall riskerar alla att smittas.

Internet och många sociala nätverk beskrivs bättre med en heterogen nätverksstruktur. När man tar hänsyn till detta finner man att tröskeln försvinner. Det finns alltså alltid en stor risk att smittan får fäste i hela nätverket.

Smittspridning för in oss på det kanske viktigaste - och svåraste - området inom nätverksteori. Man brukar prata om ett nätverks struktur, det vill säga hur noder och länkar är kopplade till varande, och processer som sker på denna struktur. Att sprida datavirus eller brev, som i Milgrams experiment, är exempel på processer på nätverk. Strukturen hos det underliggande nätverk där dessa processer pågår, påverkar givetvis hur processen sker. Vilken nätverksstruktur gör att sökning kan ske snabbt? Vilka egenskaper hos sociala nätverk gör att människor verkligen hittar varandra? Att söka en fördjupad

förståelse av kopplingen mellan nätverksstrukturer och processer på nätverk är den största drivkraften inom dagens nätverksforskning.

Christian Carling och Henrik Carlsen forskar vid avdelningen för försvarsanalys och har sedan 2002 följt nätverksforskningens utveckling inom det så kallade Metanetprojketet.

Nätverket bakom 11 september 2001

Så här samarbetade flygkaparna och deras medhjälpare inför attackerna den 11 september 2001. (Länk till pdf-fil).

Konsten att skilja en lada från en Lada

En googlande nätsurfare skiljer lätt en lada från en Lada. Men det klarar inte maskinen. Nätets sökmotorer kräver en människa som tolkar. I det nätverksbaserade försvarets underrättelsesystem ska maskiner kunna tolka informationen. Framtidens underrättelsedimmor ska skingras med hjälp av smarta hyperlänkar och en brittisk präst från 1700-talet.

Av Martin Eklöf , Pontus Hörling, Robert Suzic och Choong-Ho Yi

Så länge det har funnits krig har det funnits militär underrättelsetjänst. Från 1900-talets början blev underrättelsetjänsten viktig även i fredstid. Vilka resurser och avsikter fanns på andra sidan? I dag har hotbilden breddats. Underrättelsetjänsten sysslar inte enbart med militära ting. Snarare har detta sjunkit i bakgrunden efter kalla krigets slut. Däremot gäller gamla sanningar. Det krävs mycket arbete för att samla in underrättelser och uppgifterna ska helst vara säkra. Är uppgiften osäker ska man kunna veta om det och inte behandla den som säker. Vilket det finns färska exempel på.

Kraven på underättelsetjänst är hårda. Det gäller människor och maskiner. I det nätverksbaserade försvaret (NBF) ingår den nätverksbaserade underrättelsetjänsten (NBU). Det kan tyckas vara en enkel match. I stället för att lägga pussel och gömma mikrofilm i skoklacken kan man göra som alla andra - gå ut på nätet. Som vi ska se här, är det inte så enkelt.

NBU ska utgöra en datorintensiv miljö med hög tilltro, vars tjänster producerar användaranpassad information för att möta krav från användare i varierande situationer, såväl nationellt som internationellt. Vid utveckling av NBU är det viktigt att se hur modern informationsteknologi kan användas, men kanske ännu viktigare är att se vad morgondagens it kan ge. NBU kommer liksom dagens och gårdagens underrättelsetjänst att innehålla faserna planering, insamling, bearbetning, produktion samt delgivning. Framför allt i bearbetningsfasen med sin slagsida åt analys- och syntesarbete kan modern it utnyttjas för att hitta relationer och strukturer i stora mängder information.

Den semantiska webben
För informationshantering i webbsammanhang framstår i dag utvecklingen inom den så kallade semantiska webben som ett stort kliv framåt. Här belyses vad den semantiska webben står för, varför den är viktig och vilken roll den kan komma att spela i ett framtida underrättelsesystem.

World Wide Web har inneburit tidigare oanade möjligheter för informationsutbyte mellan människor. Men informationen är gjord för att tolkas av människor, inte maskiner. En människa kan skilja på en lada och en Lada. Av sammanhanget framgår vad som är en byggnad och vad som är en bil. En maskin klarar inte detta. Datorbaserade underrättelsesystem samlar in enorma mängder information där lador och Lador blandas friskt. Det är här den semantiska webben kommer in. Informationen är redan från början gjord för att tolkas av maskiner.

Den semantiska webben var en del av Tim Berners-Lees vision av webben. Berners-Lee, som forskade vid det europeiska kärnforskningscentret Cern, var webbens egentliga upphovsman. Hans idé fick dock aldrig någon större genomslagskraft då webben främst riktade sig till tänkande människor. Den grundläggande tanken bakom den semantiska webben är att införa maskintolkbar information i webbapplikationer som är definierad enligt en mall. Detta medför att information lättare kan lokaliseras, integreras och återanvändas, samt att kommunikationen maskin till maskin, eller maskin till människa, kan genomföras på ett sätt som alla ”förstår” (interoperabilitet). Grunden är så kallade ontologier. Ontologier kan sägas vara de fack som informationen hamnar i samt relationen mellan dessa fack. Ursprungligen är ontologi ett begrepp från den filosofiska världen. Det handlar i grunden om läran om de

begrepp eller kategorier som krävs för att skapa en sammanhängande, motsägelsefri och uttömmande beskrivning av någon del av verkligheten.

I den datalogiska världen kan ontologi i stället ses som en samling av de mest viktiga begrepp (till exempel typer av objekt), samt relationer mellan dessa, som ett system omfattar. Ontologier ses i allmänhet som ett medel för att ge Försvarsmakten interoperabilitet inom informationsområdet. Med interoperabilitet avses krav på ett systems förmåga att kunna utbyta information med andra system så att man kan skilja på en lada och en Lada.

Måste tala samma språk
Utvecklare av mjukvara måste ha ett gemensamt specifikationsspråk. Det dominerande språket, som i praktiken är standard, är UML. Dock räcker det inte med UML när informationen ska tolkas av maskiner. Ett mer lämpligt, men inte tillräckligt bra språk, är Extensible Markup Language (XML). Det beskriver vanligen information i hierarkiska klasser med tillhörande attribut. Det kan ge information vars struktur och basala relationer kan tolkas av maskiner. Men det är inte tillräckligt bra på att förklara meningen med informationen, det vi kallar semantik. Mest hopp sätts i dag till språket Web Ontology Language (OWL). Det kan sägas vara en utveckling av språket Resource Description Framework (RDF). OWL stöds av det konsortium (W3C) som skriver reglerna för webben. Det fina med OWL är bland annat att man med detta språk kan resonera om information. Det forskarna kallar inferens. Ny information kan härledas baserat på regler och befintlig information.

Den semantiska webbens språk kan komma till stor nytta för den framtida nätverksbaserade underrättelsetjänsten.

RDF och OWL kan skapa en delad modell för information inom en viss begreppsvärld. Med delad informationsmodell avses en modell som kan nyttjas och förstås av alla delar av ett system.

RDF och OWL representerar informationen på ett modulärt, strukturerat och distribuerat sätt. Det ger goda möjligheter till avancerad bearbetning av information, automatisering av processer och precis lokalisering av information.

Ett underrättelsesystem ska kunna visa relationer mellan olika företeelser, vilket är en naturlig del hos språk som RDF och OWL. I dessa språk kan relationer mellan företeelser uttryckas explicit, men även genereras automatiskt utifrån en uppsättning regler (inferens). Explicit kan vara att A beror på B och B beror på C. Då kan man skriva regeln att alla A beror på C. Den här förmågan gör att datorn mycket lättare än en människa kan hitta samband.

Men RDF och OWL är långt ifrån svaret på frågan om hur man skapar ett fungerande nätverksbaserat underrättelsesystem. Mycket arbete återstår, och det är oklart om det går att använda ontologier. Det vill säga sättet att dela upp informationen i fack. Dessutom har både RDF och OWL brister som gör att de ännu inte lever upp till de krav som NBU ställer. Information är en färskvara. Den kan dessutom vara osäker eller ofullständig. Det krävs metoder och tekniker som kan hantera osäkerheter i information, och vilka konsekvenser osäkerhet får på härledd information och slutsatskedjor. Dagens OWL klarar inte det. Det är därför en viktig forskningsuppgift att se om de mest lovande dataspråken RDF och OWL ändå är rätt väg mot att lösa problemet med osäkerheter.

Statistisk metod från 1700-talet
En möjlig väg är de så kallade Bayesianska nätverken som fått sitt namn efter den engelske 1700-talsprästen och amatörstatistikern Thomas Bayes. Bayesianska nätverk är en statistisk metod. Den kan hantera osäker information och även resonera om den. Metoden påminner i vissa delar om språken RDF och OWL. Det gör att en del information som hanterats med RDF och OWL skulle kunna översättas till ett Bayesianskt nätverk. Vid resonemang kring informationen kan då även hänsyn tas till informationens osäkerhet.

Den nätverksbaserade underättelsetjänsten är det nätverksbaserade försvarets syskon. Syskonen ska passa ihop. De ska ha samma regler och krav. När program och hårdvara byggs upp för NBU måste den passa in i NBF.

Det går inte att skapa en ontologi som kan möta alla krav från en domän. Det är bättre om underrättelsetjänsten har flera specialgjorda ontologier som tillsammans utgör en generell ontologi. Det är således viktigt att bygga infrastruktur som tar hänsyn till ontologier på flera nivåer, från generiska modeller som kan appliceras för hela underrättelseområdet till ontologier skapade för specialiserade grupper.

Martin Eklöf, Robert Suzic och Choong-Ho Yi från FOI:s systemteknikavdelning, samt Pontus Hörling från

avdelningen för ledningssystem, arbetar med forskning kring informations- och kunskapshantering i framtida underrättelsesystem.

Nytt radionät i skogen men samma naturlagar

Framtidens kommunikationsnät ska sända dolt, säkert och mycket. Problemet är kapaciteten. Risken är stor att det nya nätet blir överbelastat. Då kan fiberoptiska kablar och laser fungera som komplement till radiokommunikationen.

Av Jan-Ivar Askelin


Foto: Martin Naucler

I det gamla invasionsförsvaret var kablarna dragna i förväg till de troligaste slagfälten. Det nya flexibla insatsförsvaret behöver en annan typ av kommunikationsnät. Eftersom förbanden ska vara rörliga, vare sig de är hemma i Sverige eller utomlands, så är trådlös kommunikation det enda som gäller. Det behövs ett kommunikationsnät som kan hänga med förbanden.

- Hur det ska se ut hänger ytterst på vad försvaret vill, säger Lars Ahlin som tillsammans med Karina Fors, Anders Hansson och Mattias Sköld vid institutionen för informationsöverföring vid FOI studerar framtidens radio och radionät. Det handlar om vilka uppgifter försvaret ska ha. Mycket kan man klara med dagens teknik, men för de svåra uppgifterna (försvarets kärna) behövs ny teknik. Viktiga egenskaper för ett sådant nät är att det ska fungera utan en fast infrastruktur samt vara flexibelt för försvarets olika krav.

Den klassiska tekniken för mobil kommunikation är att bygga en infrastruktur med ett antal basstationer som mobilerna kommunicerar via. Basstationerna länkas samman och från mobilen når man i stort sett hela världen. Men basstationerna kanske inte finns eller har förstörts i ett konfliktområde. För militära nät i framtiden möts två spår. Det ena är den så kallade mjukvaruradion. Det andra är det tillfälliga nätet eller ad hoc-nätet som forskarna säger.

Ett ad hoc-nät behövs, framför allt av fyra orsaker, enligt Anders Hansson:

- Ett cellnät, som till exempel mobiltelefonnätet, har inte täckning överallt.
- En basstation kan förstöras och då fun-gerar inte cellen.
- Vid en katastrof kommer mobiltelefonnätet, om det finns ett sådant, att vara överbelastat.
- Det är självkonfigurerande och går snabbt och lätt att starta. Det är bara att trycka på on-knappen, så organiserar sig enheterna automatiskt till ett nät.

Blåljusmyndigheternas nät, Rakel, kommer att ha fasta basstationer. Det utnyttjar bland annat försvarets nät och sänder på en lägre frekvens än mobiltelefonerna. Därmed fås större räckvidd och det behöver inte vara så tätt mellan masterna. Ett framtida militärt radionät kommer förmodligen att kunna kopplas ihop med Rakel.

Radion laddas med olika program
Mjukvaruradion är enkelt beskrivet en dator med ett förstärkarsteg och antenn. Den kan, som en vanlig dator, laddas med olika program. Programmen kallas för vågformer. En vågform är radions själ. Det fina med mjukvaruradion är att den kan byta själ med en knapptryckning. En gammal truppradio kan bytas ut mot en radio som bara finns på ritbordet. En radios egenskaper omtolkas till mjukvara som laddas ner i mjukvaruradion.

- Om en hårdvaruradio kan liknas vid ett instrument, som till exempel en flöjt, så är en mjukvaruradio en hel orkester. Fast den kan bara spela med ett instrument i taget, säger Karina Fors. Än så länge finns det visserligen inte en färdig mjukradio.

- Men på detta område gäller Moores lag, säger Lars Ahlin. Var 18:e månad blir datorn dubbelt så bra. Eller hälften så dyr.

Det kan komma en radio som inte är större än en mobiltelefon som har hundratals vågformer på hårddisken. Idén med mjukvaruradio är 20 år gammal och den första generationen militär mjukvaruradio kommer från industrin om drygt ett år. Ett stort jobb har varit att ta fram en standard för hur mjukvaran ska byggas. Det är också standardtanken som är den bärande för hela mjukvaruradion. Programmen ska passa till alla radioapparater oberoende av tillverkare. I dagens värld har varje armé sin egen truppradio, därför kan de inte kommunicera med varandra, vilket försvårar samarbeten vid till exempel internationella insatser.

- Det här området är ett av de få där den militära tekniken fortfarande leder över den civila, säger Lars Ahlin. Det är militären som har mest pengar att tjäna om det här fungerar. På det civila området tänker man sig främst att använda tekniken för basstationer. Då kanske man kan kosta på sig att betala en miljon för en mjukvaruradio. USA är ledande inom området och Europa ligger efter. Det kan vara svårt att tjäna pengar på militär mjukvaruradio på nationell nivå. Det handlar inte om stora serier som när Ericsson tillverkade den svenska truppradion. Truppradion introducerades i förbanden i början på 1990-talet. Fast smärtgränsen för vad en militär mjukvaruradio kan få kosta höjs väl när det blir så få förband.

Lars Ahlin håller upp sin mobiltelefon och förklarar varför den inte är mjukvarutelefon fast den klarar två olika system.

- Det beror på att den är två telefoner i en, det som är radiospecifikt finns i dubbel uppsättning. Det är fortfarande en hårdvarutelefon.

Dolt, säkert och mycket
Totalförsvarets forskningsinstitut (FOI) forskar i första hand inte på uppbyggnaden av radioapparaterna utan på ad hoc-nätet och nodernas (byggklossarna i nätet) förmåga att adaptivt anpassa sig till användarnas krav. Detta nät ska klara tre viktiga uppgifter. Kunderna, eller noderna, som tillsammans utgör näten vill att nätet ska kunna sända dolt, säkert och mycket.

Robustheten eller störskyddet är ett gammalt krav från kalla kriget. Det vanliga är att man sänder på hoppande frekvenser. Mottagaren vet i förväg vilka frekvenser som kommer när. I stort sett alla moderna militära truppradioapparater är så kallade frekvenshoppare. Idén är gammal och vet ni vem som har det amerikanska patentet? Jo, den på den tiden mycket kända skådespelerskan Hedy Lamarr som förutom att vara den tidens sexbomb på vita duken också var uppfinnare. Patentet är från början av 1940-talet och idén skulle användas för styrning av torpeder.

Ett annat sätt att öka störskyddet är så kallade smarta antenner som kan ”vända ryggen” till störningskällan. Den robusta radion kan sägas tillhöra arvet som hänger med i framtiden. Smygradion och högkapacitetsradion är nyare idéer. En smygradio sänder en svag, men bred (i frekvens) signal. Den är så svag att den gömmer sig i radiobruset. Mottagaren vet dock var den ska leta. Det här fungerar också som ett störskydd eftersom det inte är effektivt att störa brett på frekvensbandet. Enskilda bitar kan förstöras, men mottagaren har teknik för att kunna fylla i luckorna.

Svårt med kapacitet
Det svåraste problemet är kapaciteten. Här står nätverksvisionärerna med sina informationsfloder i konflikt med naturlagarna. Det finns helt enkelt bara en viss bandbredd som är tillgänglig för ett visst förband på en viss terrängyta. Börjar några sända i bredbandstakt kommer de andra inte in. Kapacitetsfrågan är den stora nöten.

- Vem bestämmer hur resurserna ska fördelas, frågar sig Mattias Sköld. Ska löjtnanten alltid gå före furiren eller är det läget som avgör. Är det maskiner som bestämmer reglerna? Det är viktigt att nätet ger ett bra stöd att fördela knappa resurser.

Och hur ska nätet fungera när förbandet rör sig i terrängen? Det kan komma ett berg i vägen som har inverkar på alla tre egenskaperna smyg, robusthet och kapacitet.

- Eftersom ad hoc-nätet inte styrs centralt så måste radionoderna själva hitta bra vägar i nätet, säger Anders Hansson. Vi vill inte belasta nätet i onödan, men å andra sidan blir vägarna effektivare ju mer noderna tillåts att uppdatera sin bild av var andra finns i nätet.

- Vi forskar också på hur noderna i nätet ska kunna anpassa sig till de varierande krav som användarna har och hantera variationer i terrängen när förbandet rör på sig, säger Karina Fors.

- En sak är säker, säger Mattias Sköld. Det väntar ingen lösning om hörnet som åtgärdar alla problem över en natt. Tanken på rörliga bilder i färg och i realtid till alla i nätet blir nog bara en dröm när förbandet är i rörelse. Lösningen ligger i att tänka klokt. All trafik behöver kanske inte gå med radio. Uppdateringar kan göras via optofiber eller satellit när enheter står stilla. Det viktiga är att ha tillgång till rätt information på rätt plats vid rätt tidpunkt.

Jan-Ivar Askelin är redaktör för Framsyn.

Smart låda ljus i radiodjungeln

Många apparater, sladdar och kontakter. Så kan det se ut i en ledningscentral idag. I framtiden kommer mjukvaruradion. Då blir det en låda som har flera radioapparater i sig som program i en dator.

Grafik "Flexibel kommunikation med mjukvaruradio" (pdf-fil).

I dag finns hundratals olika radiosystem inom försvaret. På sikt kommer dessa att ersättas av moderna mjukvaruradiostationer, som byggts efter internationell standard. Mjukvaruradion kan uppdateras med nya program, precis som en pc.

Av Ulf Hassgård

Under de senaste åren har radiotekniken utvecklats oerhört snabbt. I dag pratas det om mjukvaruradio, mjukvaruvågformer, internationella samarbeten och standarder på ett sätt som vore otänkbart för bara några år sedan.

Under 2000 och 2001 startade några studier med uppgift att analysera denna teknikutveckling och vad den skulle kunna innebära för Försvarsmakten. Studierna Försvarsmaktens framtida taktiska telekommunikationer (FFTK) och Gemensamt taktiskt mobilt samband (GeTaS) pekar på behovet av försvarsmaktsgemensamma lösningar.

I dag finns flera hundra radiosystem i försvaret. En del är över 40 år gamla. Något krav på interoperabilitet har inte funnits vare sig inom Försvarsmakten eller mot utlandet. Att ersätta detta arv med moderna mjukvaruradiostationer byggda på internationell standard skulle ge stora taktiska och operativa vinster. Dessutom skulle Sverige för första gången få ett trådlöst kommunikationssystem som inte bara är gemensamt för hela försvaret utan också kan användas tillsammans med andra försvarsmakter.

En mjukvaruradio, Software Defined Radio (SDR), kan förenklat betraktas som en dator uppbyggd på standardiserad hårdvara där det går att ladda in ny mjukvara oavsett tillverkare. Nyckeln är en långt driven standardisering, ungefär som i pc-världen i dag. Många företag har tillverkat mjukvaruradio sedan lång tid tillbaka. Det nya är standardiseringen. I dag har vi en apparat för varje egenskap. I morgon kommer olika egenskaper att kunna samsas under samma skal. Egenskaperna sitter i mjukvaran. I praktiken innebär det att man kan få flera radioapparater i en.

Exempel på egenskaper som kan hanteras i mjukvara är signalbehandling, protokollhantering, överliggande applikationer, krypto, skydd mot störning och så vidare.

Uttrycket waveform (vågform) beskriver dessa delar. En vågform omfattar dock mer än så. Den kan vara allt mellan användargränsytan - exempelvis handmikrotelefonen - till antennutmatningen. En vågform kan betraktas som mjukvaran till en dator. På samma sätt som det går att uppgradera en pc ska man kunna uppgradera sin radio med ny mjukvara vid ändrade taktiska och tekniska krav.

Utvecklingen sker i kluster
USA är ledande inom området radioutveckling. Sedan 1998 bedrivs all radioutveckling inom programmet Joint Tactical Radio System (JTRS). Programmet är uppdelat i ett antal så kallade kluster (cluster):

Cluster 1: Stridsfordon, främre flygledning, helikoptrar. Över 130 000 enheter är beställda. Tas i bruk från 2006.

Cluster 2: Handhållna stationer.

Cluster AMF: Flyg- och marina installationer.

Cluster 5: Handhållna, burna och så kallade inbäddade system (exempelvis i skyddsvästar samt sensor- och vapensystem).

Frekvensområdet är stort (2 MHz till 55 GHz), ett 30-tal vågformer utvecklas, mjukvarukrypto utvecklas med mera. Det handlar om en familj av radioapparater som till det yttre kan se mycket olika ut, men innanför skalet finns samma grundläggande teknik och arkitektur. Detta ger i framtiden helt andra möjligheter till samverkan och interoperabilitet än i dag.

I Försvarsmakten från 2006
Försvarsmakten bedriver sedan några år tillbaka en omfattande verksamhet inom mjukvaruradioområdet. Hösten 2003 genomförde FMV en mycket lyckad demonstration av möjligheterna med mjukvaruradio och ad hoc-nätbildning på S1 i Enköping. Demonstrationen var resultatet av ett samarbete mellan US Army Cecom, Rockwell Collins Government Systems och Försvarets materielverk (FMV).

Samtidigt slutfördes den första fasen i ett samarbete i syfte att ta fram en mjukvaruvågform för Tetra som används i Kosovo - och i framtiden sannolikt också i blåljusmyndigheternas nya radiosystem Rakel. Detta projekt genomfördes tillsammans med den myndighet som är ansvarig för det amerikanska JTRS-programmet.

Projekten syftar till kunskapsuppbyggnad för en anskaffning av såväl mjukvaruradio som vågformer till dessa. De första nya radioapparaterna, som ska kunna hantera mjukvaruradiotekniken, beställdes i juni i år. Dessa är avsedda för den demonstration inom NBF-utvecklingen, som ska ske 2006, och för de mekaniserade bataljonernas framtida stridledningssystem SLB (Stridsledning bataljon).

Denna beställning omfattar en förserie till det kommande försvarsmaktsgemensamma radiosystemet Gemensamt taktiskt radiosystem (GTRS). De första leveranserna till denna förserie kommer under 2006 och projektet avslutas 2007. GTRS Demo utnyttjas för att skapa kunskaps- och beslutsunderlag för att sedan kunna gå vidare med seriebeställningar från 2008 och framåt.

Anskaffningen av övriga delar inom GTRS-programmet sker efterhand till insatsorganisationens alla delar. Samtliga förband kommer att ha GTRS 2014. Anskaffning sker i takt med utvecklingen. Det innebär att när försvaret får nya erfarenheter och del av ny teknikutveckling, införs dessa i nästa upphandling. Därför kommer de stationer som levereras 2014 med stor sannolikhet skilja sig från dem som levereras 2008.

Det är viktigt att påpeka att GTRS inte är en ny radiostation. GTRS är ett program bestående av följande hårdvarudelar plus navigationssystemet GPS (Global Positioning System):

- Radio för en vågform. Denna radio är liten. Den kan vara buren, handhållen eller till och med inbyggd i soldatens utrustning.
- En radio för en till fyra vågformer. Den kan finnas i stridsfordon, stridsbåtar och i helikoptrar.
- En radio för fyra till åtta vågformer. Den ska finnas i flygplan, ledningsplatser, fasta installationer och så vidare.

En radiostation för stridsfordon kommer i vissa lösningar att kunna hantera tre samtidiga vågformer. Med andra ord kan denna radio betraktas som tre ”gamla” radioapparater, med tillägget att dessa vågformer kan bytas när man så önskar.

I en mekaniserad bataljon har varje fordon en radio som kan hantera mellan en och fyra samtidiga vågformer, ledningsfordonen fyra till åtta. På kompani- och plutonsnivå finns bärbara radiostationer. Varje soldat ska ha en egen radio för kommunikation inom gruppen.

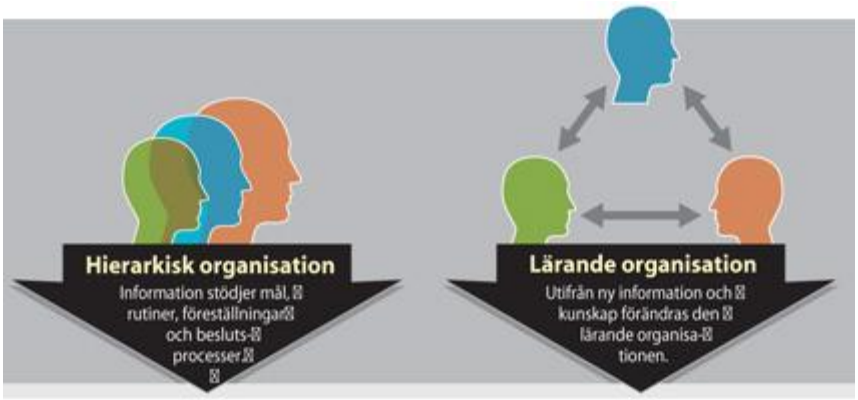
De flesta vågformer som anskaffas ska kunna klara kommunikation med äldre radioapparater - arvet. Även vågformer för att kunna verka inom olika koalitioner vid internationella insatser måste anskaffas, liksom bredbandiga vågformer för höga dataöverföringshastigheter. Överföringshastigheter upp till 10 Mbit/s är förmodligen verklighet 2014.

GTRS löser inte alla problem
GTRS är i första hand ett sätt att skapa ett försvarsmaktsgemensamt taktiskt radiosystem. Det kommer fortfarande att finnas behov av vissa typer av system som anskaffas ”stuprörsmässigt”. Det kan vara system med väldigt få stationer eller system utan krav på avancerad signalbehandling eller störskydd. Syftet är dock att en GTRS-station ska kunna trafikera även dessa nät.

GTRS löser inte alla problem men är ändå ett paradigmskifte avseende de mobila telekommunikationerna. En kraftigt ökad flexibilitet tillsammans med ökad dataöverföringshastighet, och inte minst ett försvarsmaktsgemensamt tänkande, kan förverkliga de tankar och visioner som finns inom NBF-utvecklingen. GTRS är en förutsättning för det flexibla insatsförsvarets mobila delar.

Överstelöjtnant Ulf Hassgård har varit materielsystemansvarig vid Högkvarteret för försvarsmaktsgemensam radiomateriel. Han är nu samverkansofficer vid US Joint Forces Command i Norfolk, Virginia, USA.

Så ska försvaret styras åt rätt håll



Klicka på bilden för att ladda hem hela grafiken som pdf-fil.

Att bygga det nya försvaret är en lång och svår process. Avdelningen ÖB Controller på Försvarshögkvarteret arbetar med att förändringen genomförs enligt ÖB:s vilja.

Av Jan-Ivar Askelin

Den gamla tunga försvarsmakten brukar ibland beskrivas som en supertanker. Det dröjer innan det märks att kursen läggs om. Supertankerns huvuduppgift var att gå rakt fram under en längre tid.

Nu ska Försvarsmakten byta båt, till något lättare, snabbare, mindre och mer lättmanövrerat. En båt som fortare ska kunna svara på omvärldens förändringar. En sådan båt kan inte styras som en supertanker. Risken finns att instruktionen för hur man styr en supertanker kommer att följa med in på den nya båtens kommandobrygga.

Den 10 januari 2003 inrättades en ny enhet vid Högkvarteret för att bidra till att förbättra och utveckla nya styrformer. Den kallas ÖB Controller och består av sex personer, varav tre är militärer. Chef är överste Björn Ekstedt. Han är flygingenjör och har sin bakgrund i såväl den militära världen som den akademiska. För att bli flygingenjör krävs en civilingenjörsexamen. Elisabeth Nyström är ekonom och samhällsvetare.

- Jag är ingen ekonom som räknar pengar utan är inriktad på hur verksamhetsstyrning och utveckling, säger hon.

Controller är ett etablerat begrepp. Enkelt uttryckt kan en controller arbeta på olika nivåer i organisationen och med verksamhet, ekonomi eller inom en specifik funktion, som till exempel inköp. ÖB Controller arbetar med verksamhetscontrolling på myndighetsnivå. Den är alltså inte tillbakablickande för att se vart pengarna har gått eller inte har gått. Den tittar i stället framåt för att se hur försvaret ska kunna fortsätta att förändras och dessutom i en högre takt än tidigare. Inom Nato och de västliga försvarsmakterna används det engelska begreppet Transformation för att beskriva samma förändringsprocess som den svenska Försvarsmakten nu genomgår. För Nato finns det till och med ett Allied Command Transformation (ACT) i Norfolk, USA.

ÖB controller är som namnet anger direkt underställd ÖB och i praktiken innebär det ett nära samarbete med chefen för strategiledningen. Funktionen ska som det heter, analysera verksamheten vid Försvarsmakten och föreslå hur verksamheten ska utvecklas för att tillgodose statsmakternas krav på en rationell och effektiv myndighet.

- Vi ska, enkelt uttryckt, stödja ÖB med att analysera och följa upp centrala områden på myndighetsnivå och utveckla metoder, principer och processer för att styra Försvarsmakten, säger Björn Ekstedt.

Handbok saknas
Någon instruktion för hur den nya båten ska styras finns nu inte att hämta på förrådet.

- Nej, någon handbok i hur man styr ett försvar finns ju inte. Man får använda beprövade modeller och teorier och anpassa dessa utifrån Försvarsmaktens förutsättningar. För att anpassa och pröva dessa behövs resultatinriktad forskning eller uppdragsforskning om man så vill.

FOI-studien som beskrivs här är en av flera studier som pågår eller har avslutats. De övriga inom området modeller och metoder för verksamhetsstyrning är:

- Stockholms universitet: Styrning, effektivitet och ansvar inom Försvarsmakten med fokus på medborgarperspektiv, 2003-2004.
- FOI, Strategiprocesser på HKV, 2003-2004,
- FOI, Ekonomistyrning inom Försvarsmakten, 2001-2003.

- Uppdragsforskningen måste omsättas i konkreta åtgärder, säger Björn Ekstedt. Det är en av våra uppgifter, men detta sker långsiktigt. Förändringsarbete kan inte kommenderas fram, det måste i vissa fall få ta tid och då är det viktigt att controllern, i detta fallet vi, är uthålliga och klarar av att hantera det förändringsmotstånd som alltid med naturlighet finns. Många frågor går djupt ned i vår organisation och det innebär att vi måste ändra på rådande föreställningar om hur saker hänger ihop och hur vi ska arbeta och se på olika förhållanden. Projekten pågår ofta i tre år, för att det ska vara möjligt att gå ned på djupet, men rapporteras årsvis.

- För att kunna motivera att man använder en viss metod och förstå dess för- och nackdelar måste det finnas forskning bakom, säger Elisabeth Nyström. Hur fungerar Försvarsmakten nu och hur bör den fungera i framtiden? Man måste kunna plocka ner organisationen i smådelar och analysera varje enskild del, utan att för den delen tappa helhetssynen.

- Det är då man har nytta av en akademisk bakgrund, säger Björn Ekstedt. För en ingenjör handlar det om att kunna bryta ner större problem i små delar och se sambanden, och att ha en verktygslåda med olika metoder och modeller som kan användas. Förändring kräver ett abstrakt tänkande.

Stabil osäkerhet
- Den gamla tidens osäkerhet hade ändå en stabilitet i sig, säger Elisabeth Nyström. Man kunde blicka framåt och visste att det ungefär skulle se likadant ut. I dag lever vi i en säkrare värld i den meningen att en stor konflikt i Europa är mycket svår att föreställa sig. Men vi har en annan osäkerhet som består i att hoten har ändrat karaktär och att vi inte kan bedöma framtiden lika lätt som vi gjorde förr. Samtidigt använder nu statsmakterna Försvarsmakten mer aktivt, som ett säkerhetspolitiskt instrument. För att möta denna osäkerhet och dynamiken i våra uppgifter och uppdrag krävs en flexibel ledning. Vi går nu från var vi var förr till något helt nytt. Det är inget annat än en organisatorisk revolution. Vi ska göra något annat och vi ska göra det på ett helt nytt sätt.

Björn Ekstedt fortsätter:

- Den stora organisationens problem är att den lätt blir alltför inåtblickande. Vid problem letar man gärna inne i organisationen efter lösningen. Vi måste få Försvarsmakten att i ökad utsträckning titta ut och få impulser utifrån. Uppdragsforskningen är en mycket viktig del av detta. Den ska belysa viktiga områden och ge nya idéer om hur vi kan gå vidare.

- En central fråga är vem som avgör vilka områden som är viktiga, säger Björn Ekstedt. De områden som behöver studeras utgår från Försvarsmaktens strategiska målsättningar och dessa är det naturligtvis ÖB och hans chefsgrupp som anger.

Förutom ÖB och ställföreträdande ÖB består chefsgruppen av cheferna för grundorganisationen, krigsorganisationen, operativa insatsledningen, militära underrättelse- och säkerhetstjänsten samt chefen för strategiledningen tillika chef för Försvarshögkvarteret.

För att kunna klara en så genomgripande förändring som Försvarsmakten nu genomför måste det finnas en strategisk ledningsprocess som klarar ut och tydliggör de strategiska målsättningarna. För att kunna se sammanhangen och beroendeförhållanden mellan målsättningarna är de beskrivna i ”ÖB:s strategiska karta”.

- En mycket viktig aspekt i detta är att kommunicera vart och vad ÖB vill, det vill säga de strategiska målsättningarna, och här är den strategiska kartan ett bra verktyg. Avsikten är att chefsgruppen aktivt ska mäta och värdera om och i vilken utsträckning de strategiska målsättningarna uppfylls.

- När detta sker kontinuerligt, ordnat och systematiskt, inom ramen för en strategisk ledningsprocess, kommer det att resultera i att chefsgruppen ser vad som fungerar och vad som inte fungerar. Samtidigt kommer de efterhand att behöva ompröva sina ståndpunkter och antaganden. Detta är grunden i ett organisatoriskt lärande och det gör att ÖB chefsgrupp arbetar med en strategisk lärandeprocess.

Jan-Ivar Askelin är redaktör för Framsyn.

”Försvarsmakten måste bli mer flexibel”

Försvarsmakten bör lämna den hierarkiska organisationen och bli mer flexibel. Toppstyrningen måste minska och den mekaniska, ingenjörsmässiga synen på organisationen måste försvinna. Utan flexibilitet kommer Försvarsmakten inte att klara de nya krav som ställs, anser artikelförfattarna.

Av Charlotte Collin, Magnus Kaiser och Per Larsson

Organisatorisk flexibilitet handlar om att kunna agera utifrån ny information och kunskap. Försvarsmaktens koncept för ett nätverksbaserat försvar (NBF) är ett uttryck för att skapa en ny flexibel insatsorganisation som är anpassad till en förändrad säkerhetspolitisk dagordning och nya uppgifter. Hur organisatorisk flexibilitet skapas i Försvarsmaktens löpande verksamhet har hittills inte fått motsvarande uppmärksamhet i utformningen av den framtida Försvarsmakten.

Att utveckla flexibiliteten i den löpande verksamheten är av stor vikt eftersom insatsverksamheten och den löpande verksamheten i många avseenden hänger samman. Utan ökad organisatorisk flexibilitet i Försvarsmaktens löpande verksamhet lär man få svårt att svara upp mot de nya krav som ställs, och att uppnå den flexibilitet i insatsverksamheten som man eftersträvar med konceptet NBF.

Studier som Totalförsvarets forskningsinstitut (FOI) har gjort visar att Försvarsmakten för att nå ökad flexibilitet behöver bli bättre på att i genomförandet av den löpande verksamheten beakta flera olika typer av information, bredare kunskap, olika föreställningar och nya lösningar. (Studierna presenteras i rutan här intill). Framför allt behöver Försvarsmakten lösgöra sig från budgetstyrningen som den dominerande styrformen.

FOI-studien av ledningsorganisationsutredningen (LU 02) visade att utredningsförslagen avsåg att skapa ännu mer tydlighet och strikt ansvarsfördelning, vilket snarare motverkar än stödjer organisationens behov av flexibilitet och lärande för att kunna hantera en alltmer osäker och dynamisk omvärld. FOI-studien av Högkvarterets ledning av förbanden inför och under ett löpande verksamhetsår, visade att budgetstyrningen är helt avgörande för de beslut som fattas under det löpande budgetåret inom processen för att utarbeta verksamhetsuppdragen och följa upp dess genomförande. Detta begränsar förmågan att söka nya perspektiv och lösningar.

Frågan är om Försvarsmakten i dag uppmärksammar rätt information inför och vid olika beslutssituationer. Försvarsmakten behöver fundera mer över vilken information som organisationen bör hantera och löpande uppmärksamma. Försvarsmaktens problem, att inte få den effekt av försvarsbudgeten som önskas, skulle kunna förklaras av att den koncentrerar sig på information som tillfredsställer planeringsbehoven snarare än sökande efter förståelse för verksamhetsrelevanta samband.

Kontroll eller förståelse?
Styrningen av en organisation har till uppgift att vägleda och inrikta organisationens verksamhet. I många organisationer sker styrning med ett avstånd mellan ledning (som formulerar vad som ska göras) och verksamhet (som gör). För denna så kallade top-down styrning är det viktigt att samla in information från organisationen till ledningen, något som förenklats av informations- och kommunikationstekniken. Processandet av information har ofta till syfte att öka kontrollen genom att bryta ner problem och målsättningar i hierarkin. I en föränderlig och osäker omvärld tycks behovet av mer information öka på central nivå, man försöker hantera osäkerheten med mer information.

En ökad mängd information stärker dock inte automatiskt organisationens förståelse för verksamhetens villkor och samband. Denna förståelse skapas genom de perspektiv och förhållningssätt som människor i organisationen har till verksamheten. Förståelse för Försvarsmakten, dess uppdrag och omvärld har tidigare skapats genom organisationens rutiner, planering och formella plandokument. Detta är gångbart för en statisk verksamhet. Ställs däremot flexibilitetskrav på Försvarsmakten förutsätter det att organisationens medlemmar ges utrymme att tänka och agera utanför ”ramarna”. Flexibilitet skapas inte genom gamla styrformer som prioriterar information, tydlighet och plandokument. Den skapas ”här och nu” och är i högre grad en fråga om prövande av förståelsen av verksamheten och dess samband, än om planering.

För att få bredare information och nya impulser om organisationens verksamhet, måste styrningen dels ge utrymme för ifrågasättande och prövande inställningar gentemot strategi och verksamhet, dels vara mer decentraliserad. Kort sagt behövs en styrning som öppnar organisationen för nya lösningar och därmed för flexibilitet. Styrningen behöver övergå till en strategisk ledning där avståndet mellan strategi och genomförande blir mindre genom att strategin görs vägledande för beslut i den löpande verksamheten.

Behov av förändrad styrning
Förändringen i synen på vad som är funktionellt för en organisation som eftersträvar flexibilitet i en föränderlig omvärld går bland annat att finna i teorierna kring organiska organisationer och i teorierna om lärande organisationer. I de två rapporterna som FOI presenterat återfinns redogörelser för teorierna och resonemang kring hur dessa kan tillämpas på sättet att se på Försvarsmakten.

Behovet av denna nya syn på styrningen av organisationer uppmärksammades inom forskningen under senare delen av 1900-talet. Grunden är förståelse av verksamheten och dess samband. Förståelse kräver ifrågasättande av gällande föreställningsvärldar och prövande av nya perspektiv. För att åstadkomma detta behöver man lämna den ingenjörsmässiga och mekaniska synen på organisationer. Man behöver minska styrningen ovanifrån som:

- endast utgörs av budgetmässig information,
- begränsar åtkomsten av kunskap i hierarkin,
- skapar ett avstånd mellan dem som hanterar strategin och dem som hanterar genomförandet.

I stället måste behovet av en flexibel organisation betonas. Skillnaden mot nuvarande sätt att organisera och styra Försvarsmakten är stor och kräver inte minst en förändrad syn på hierarkin och lärandet i organisationen. Försvarsmakten i Sverige är inte ensam om att stå inför detta skifte. Myndigheter, företag och även andra försvarsmakter ser behov av nya styrformer som stödjer en betydligt flexiblare verksamhet.

Det amerikanska kriget mot terrorismen visar på svagheterna med traditionella metoder och på behovet av att utveckla nya strategiska styrformer och ageranden. Den amerikanska militären ser övergången till en lärande organisation som en överlevnadsfråga. Mycket talar för att Försvarsmakten i Sverige behöver satsa seriöst på en ökad organisatorisk flexibilitet för att kunna lösa de framtida uppgifterna.

Charlotte Collin, Magnus Kaiser och Per Larsson är försvarsanalytiker med särskild inriktning på olika organisationstyper.

Ny syn på skyddet

Kalla krigets syn på NBC-skydd med kända hot, stora anfall och stora säkerhetsmarginaler håller på att bytas ut. Den nya synen präglas av exakt information i realtid och nya typer av hot.

Av Jan-Ivar Askelin Foto Martin Nauclér

Informationen kommer att finnas där ute. Det gäller bara att plocka upp den och sammanställa den. Det säger överstelöjtnant Bernt Åke Nensén, funktionshandläggare för skyddsfrågor vid Högkvarteret, tidigare stabschef vid Totalförsvarets skyddscentrum i Umeå.

För att hantera ett NBC-hot eller en händelse på ett rationellt sätt krävs god information, såväl sensordata som underrättelser, rapporter från rekognosceringar, samt en ledningsfunktion. Målsättningen är att öka precisionen i skyddsåtgärderna för att bibehålla förbandets effekt och skydda individen.

Vid bedömning av ett hot ställs frågor som: Hur kan hotet påverka förbanden? Vad kan vi göra för att minska hotet? Hur ska man placera ut sensorerna på bästa sätt? Behöver förbanden vidta förebyggande åtgärder, som att hela tiden bära NBC-stridsdräkter? Hur påverkas förbandet av skyddsåtgärder?

Vid NBC-händelser ställs frågor som: Vad har hänt? Vad är det för ett ämne? Hur omfattande är det? Hur länge är det farligt? Vilka har blivit drabbade? Hur påverkar det förbandets förmåga att lösa uppgiften?

Stor skillnad mot förr
Tidigare tog man, i brist på tillräcklig information, det säkra för det osäkra. Detta kunde leda till att en hel bataljon fick ta på sig skyddsutrustning fast det kanske bara var aktuellt för ett kompani, eller att alla skulle saneras trots att behovet var betydlig mindre.

IT-revolution och Berlinmurens fall. Det är i korthet drivkrafterna bakom inte bara försvarets förändring utan också hur uppgifter ska lösas. Man kan fråga sig om det inte märks särskilt tydligt på NBC-skyddsområdet. Överstelöjtnant Rune Karkea vid Skyddscentrum har anledning att fundera på detta. Han är ansvarig för att skapa en funktionsutvecklingsplan för hela försvarets NBC-skydd.

- Förr visste vi vem fienden var, vilka vapen han hade och taktiken. Skyddet dimensionerades mot storskaligt NBC-anfall. Idag utgörs hotet av det som brukar kallas skurkstater, terrorister och andra kriminella organisationer. Och vi vet inte när anfallet kan komma.

- Vi räknar även in i hot som inte är avsiktliga som till exempel ett utsläpp av farliga kemikalier eller från kärnkraftverk. Vi måste ha ett flexibelt NBC-skydd som kan anpassas till aktuellt hot och som med minimal påverkan på förbandet ska kunna ge ett fullgott skydd under en lång tid. En förutsättning för detta är effektiv informations- och ledningsförmåga.

Förr hade vi ett invasionsförsvar med en massarmé. Då gällde enkel utrustning och enkel utbildning. Idag talar vi om insats- och kompetensförsvar som ska kunna lösa uppgifter såväl nationellt som internationellt, och man betonar att Försvarsmaktens kärnförmåga är väpnad strid. Samtidigt är trenden, både här hemma och utomlands, en allt lägre förlusttolerans, vilket i sin tur ställer krav på förbandens skydd.

- Det här har en särskild betydelse för NBC-skyddet, säger Rune Karkea då NBC-hot är kopplat till både rädsla och okunskap. Följden blir att även en mindre NBC-händelse sannolikt uppmärksammas betydligt mer än en vanlig krigshändelse, till exempel att någon skadas av en mina. Detta är något som man måste ta hänsyn till när man bedömer NBC-hot och dess verkningar.

Annan syn på förluster
Mycket av förmågan förr handlade om att kunna göra något när attacken väl skett utan att ha riktigt ”koll på läget”. En stor del av NBC-skyddsförmågan var därför delegerad ned på en relativt låg nivå. Varningssystemet var syn, känsel, hörsel och lukt samt manuell indikering och larmning. När man trodde att faran var över fick en soldat ta av sig skyddsmasken medan de andra tittade på. Soldatens reaktion fick avgöra om faran kunde anses vara över eller inte. Det håller givetvis inte nu när synen på förluster är en helt annan än när nationens existens stod på spel.

I och med att man under kalla kriget utgick ifrån ett stort NBC-angrepp samtidigt som situationsuppfattningen och ledningsförmågan var begränsad handlade skyddet dels om fysiskt skydd, till exempel dräkter och övertryck i fordon, och dels om omfattande sanering. NBC-skydd var därför till stor del en underhållsfråga som krävde stora resurser. Det var tonvis med materiel och kalk som skulle släpas med när svenska armén drog in i de djupa skogarna. NBC-frågorna kom därför att hamna långt ner i organisationen.

I morgon blir NBC-skyddet mer integrerat med kontinuerlig övervakning och inte något som man hänger på i efterhand som ett ”löst paket”.

I och med en förbättrad situationsuppfattning som möjliggör NBC-ledning kommer NBC upp på beslutsfattarnas bord då de faktiskt kan påverka och begränsa effekterna vid en NBC-händelse, och NBC-frågor kommer att ingå som en naturlig del när operationer planeras och leds.

Tekniken kommer även att stödja ledningsprocessen samtidigt som NBC-kompetens kan distribueras via nätverket, och följden kan bli att man till exempel har specialister högre upp i organisationen där de gör mer nytta. Systemet ska väcka beslutsfattarna i och med att beslutsunderlaget snabbt kommer upp på lägeskartan. Här kommer en varning. Här har vi ett problem. Ska vi ta itu med det eller kan vi strunta i det? Ska vi fråga specialisterna i den operativa staben om råd?

Rune Karkea ser ett koncept bestående av:

Ett grundskydd som alla förband ska ha och som främst är riktat mot förbandets och den enskilda soldatens överlevnad vid oförutsägbara NBC-händelser.

Ett förbandsanpassat skydd som ska utgå från förbandets uppgifter och den hotbild som det ska kunna hantera. Till exempel så kommer det att finnas skillnader i det förbandsanpassat skyddet mellan en rörlig mekaniserad bataljon och en flygbasbataljon.

Ett uppdragsanpassat skydd som tillförs förband som ska lösa uppgifter eller verka i en hotmiljö som det förbandsanpassade skyddet ej är dimensionerat för. Det kan till exempel vara att förbandet på stort avstånd stöds av en expertgrupp, att förse fordonen med NBC-sensorer. Utrymmet för sensorn är förberett. Det är bara att jacka in. Men när det inte finns något hot är det ju onödigt att ha sensorn med sig. I vissa fall kan det även vara aktuellt på plats stödja med särskilda NBC-skyddsenheter.

Man också se på problemet ur ett tidsperspektiv, säger major Björn Nyström vid Skyddscentrum.

Före ett uppdrag eller mission ska fokus vara på analys och kartläggning av hotet för att vidta förebyggande åtgärder, som att uppdragsanpassa förbandets skydd för att kunna verka under det aktuella hotet, taktikanpassning och att minska hotet.

Under uppdraget eller missionen fokus vara på att kontinuerlig övervaka och följa upp NBC-läget för att snabbt kunna varna och bibehålla ledningsförmågan trots en NBC-händelse.

Efter uppdraget eller missionen ska en sammanställning göras avseende eventuell exponering av skadliga ämnen och strålning på individnivå.

NBC-skyddsstrategin kan beskrivas enligt följande:

Genom avtal, konventioner och politiska påtryckningar minska hotet. Det gäller i första hand i förhållande till stater.

Ett effektivt NBC-skydd ska ha en avhållande inverkan.

Kunna avvärja NBC-hot, genom aktiva åtgärder så som att slå ut enheter/system eller säkra objekt i kemiska industrier.

Kunna skydda förbandet mot effekterna av ett angrepp.

Kunna att återställa förbandets förmåga efter en NBC-händelse

Med återställning menas att ersätta mängdmateriel och endast sanera materiel som behövs för att lösa uppgifterna. Att alltid ta hand om personalen är en självklarhet.

Allt det här låter ju väldigt bra, men i denna nya värld är vi inte än.

- Fortfarande finns tänkandet från det kalla kriget kvar, säger Rune Karkea. Då tänkte man sig ett öppet och stort NBC-anfall. Mycket av dagens resonemang utgår från att vi känner till mycket av händelsen till exempel plats, tid och väder. Då blir det ganska enkelt att hantera problemet.

- Men den stora frågan är vem som har gett oss den informationen? Det finns idag inga sådana system och ingen taktik för att under längre tid ha igång ett övervakningssystem som skulle kunna detektera och automatiskt larma att något skett. Vi har en prototyp på Skyddscentrum för automatisk övervakning, och vi är på väg att köpa några till. Vi borde ha ett sensornätverk som både har komponenter för övervakning och kartläggning. Så mycket som möjligt bör baseras på automatiska system och dataöverföring i realtid. Stridsfordon och soldater ska kunna ha sensorer för eget skydd. Ger dessa utslag sänds informationen ut på nätet. Man ska inte alltid behöva skicka iväg ett NBC-fordon eller en NBC-specialist för att få koll på läget.

Nu tas ett helt nytt grepp på NBC-problematiken. NBC-skydd ska inte vara en gren i sig utan en hjälp för att kunna lösa uppgiften, det vill säga utgå från det taktiska behovet där NBC-skyddet måste passa in. Ett 75-procentigt NBC-skydd som är lätt att använda är kanske bättre än hundraprocentigt skydd som är svårt eller kraftigt reducerar förbandets stridsvärde?

Det finns en målbild som ligger tio år bort. Kruxet är att orientera sig fram till målet. En massa kontroller ska passeras på vägen. Här finns doktriner, perspektivplaner, det nätverkbaserade försvaret och den allmänna teknikutvecklingen. Det kan man kalla för grundvärden. Vägen till målet är funktionsplanen och den ska vara klar i höst. I planen ingår faktorer som studier, forskning och teknik, förbandsutveckling, med mera.

I arbetet så understryks att NBC-förmåga består av teknik, metodik, struktur och kompetens.

- Som vanligt hamnar man lätt i tekniken, säger Bernt Åke Nensén. Ska man lösa problem så blir svaret nya prylar. Istället borde man satsa på det andra. Försvarsmakten ska satsa på informationshantering, taktik/metodik, utbildning och övning.

NBC-skyddet är inte längre en fråga om att kunna transportera mängder av kalk utan om att bearbeta och rätt tolka information.

Jan-Ivar Askelin är redaktör för Framsyn.