FOI
TOTALFÖRSVARETS
FORSKNINGSINSTITUT

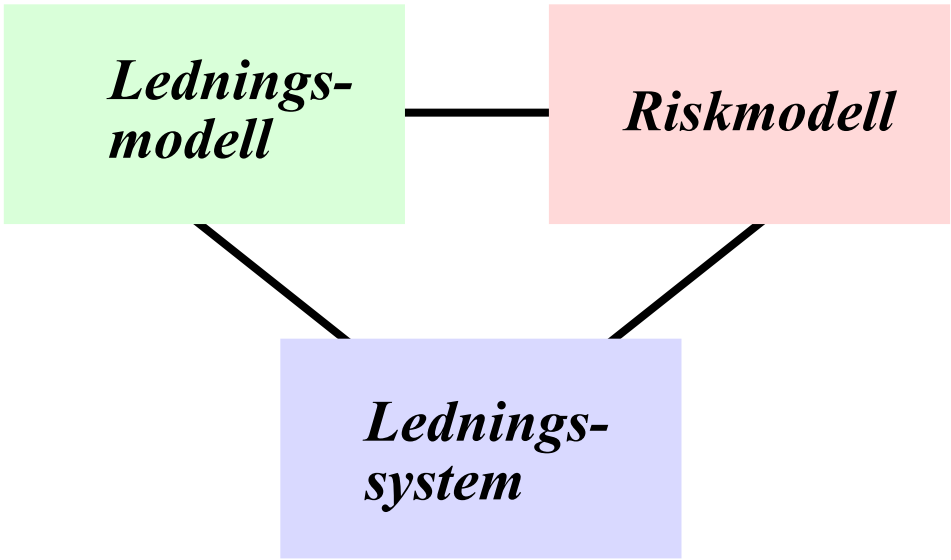
FOI-R--1183--SE
Mars 2004
ISSN 1650-1942

Metodrapport

Erland Jungert, Gunilla Derefeldt, Jonas Hallberg, Niklas Hallberg,
Amund Hunstad, Ronny Thurén

Pär-Anders Albinsson, Martin Holmberg, Hedvig Sidenbladh, Peter Stenumgaard, Arne Worm, Per Ånäs

Förstudie avseende förslag till integrerad lednings- och skyddsfunktion för preventiv och operativ krishantering



Ledningssystem
SE-581 11 Linköping

TOTALFÖRSVARETS FORSKNINGSINSTITUT

Ledningssystem
Box 1165
581 11 Linköping

FOI-R--1183--SE

Mars 2004

ISSN 1650-1942

Metodrapport

Erland Jungert, Gunilla Derefeldt, Jonas Hallberg, Niklas Hallberg,
Amund Hunstad, Ronny Thurén
Per-Anders Albinsson, Martin Holmberg, Hedvig Sidenbladh, Peter
Stenumgaard, Arne Worm, Per Ånäs

Förstudie avseende förslag till integrerad lednings- och skyddsfunktion för preventiv och operativ krishantering

Utgivare	Rapportnummer, ISRN	Klassificering
Totalförsvarets Forskningsinstitut - FOI	FOI-R--1183--SE	Metodrapport
Ledningssystem	**Forskningsområde**	
Box 1165	4. Ledning, informationsteknik och sensorer	
581 11 Linköping	**Månad, år**	**Projektnummer**
	Mars 2004	E7846
	Verksamhetsgren	
	5. Uppdragsfinansierad verksamhet	
	Delområde	
	41 Ledning med samband och telekom och IT-system	

Författare/redaktör		Projektledare
Erland Jungert	Pär-Anders Albinsson	Erland Jungert
Gunilla Derefeldt	Martin Holmberg	**Godkänd av**
Jonas Hallberg	Hedvig Sidenbladh	Johan Mårtensson
Niklas Hallberg	Peter Stenumgaard	**Uppdragsgivare/kundbeteckning**
Amund Hunstad	Arne Worm	Krisberedskapsmyndigheten
Ronny Thurén	Per Ånäs	**Tekniskt och/eller vetenskapligt ansvarig**
		Erland Jungert

Rapportens titel

Förstudie avseende förslag till integrerad lednings- och skyddsfunktion för preventiv och operativ krishantering

Sammanfattning (högst 200 ord)

Detta arbetet är en förstudie som beskriver ett förslag till ledningsfunktion för preventiv och operativ krishantering. Ledningsfunktionen föreslås bli baserad på en ledningsmodell som omfattar metoder för datainsamling, upptäckt, identifiering, bedömning och hantering av olika hot. Sådana hot skall med stöd av ledningssystemet genom analys kunna kopplas till andra existerande hot så att en sammanhängande hotbild kan byggas upp. Detta skall ske genom att man kan identifiera och bygga upp kedjor av potentiella hotfragment. Således, skall det med utgångspunkt från ledningsmodellen vara möjligt att beskriva och utveckla ett ledningssystem med dessa förmågor. Systemet måste också kunna utnyttjas för ledning i operativt syfte vilket avser förmågan att på högre systemnivå kunna leda arbetet med att avvärja eller åtminstone begränsa konsekvenserna av kriser. För att möjliggöra detta kommer metoder för samarbete och kommunikation mellan berörda myndigheter att krävas. Andra aspekter som måste beaktas i detta arbete utgör bl a IT-säkerhet, människa-systeminteraktion samt olika typer av beslutsstödsfunktioner.

Nyckelord

Ledningssystem, krishantering, skydd, hot,

Övriga bibliografiska uppgifter	Språk Svenska
ISSN 1650-1942	**Antal sidor:** 68 s.
Distribution enligt missiv	**Pris: Enligt prislista**

Issuing organization	Report number, ISRN	Report type
FOI – Swedish Defence Research Agency Command and Control Systems P.O. Box 1165 SE-581 11 Linköping	FOI-R--1183--SE	Methodology report
	Programme Areas 4. C4ISTAR	
	Month year March 2004	**Project no.** E7846
	General Research Areas 5. Commissioned Research	
	Subcategories 41 C4I	

Author/s (editor/s)		Project manager
Erland Jungert	Pär-Anders Albinsson	Erland Jungert
Gunilla Derefeldt	Martin Holmberg	**Approved by** Johan Mårtensson
Jonas Hallberg	Hedvig Sidenbladh	
Niklas Hallberg	Peter Stenumgaard	**Sponsoring agency** Swedish Emergency Management Agency
Amund Hunstad	Arne Worm	
Ronny Thurén	Per Ånäs	**Scientifically and technically responsible** Erland Jungert

Report title (In translation)

A proposal for an integrated C2 and protection function for preventive and operative crisis management

Abstract (not more than 200 words)

This work is the result of a study in which a command and control function for crisis management is proposed. This function will be based on a model that includes methods for data collection, discovery, identification, scrutiny and handling of various types of threats. Such threats should, with support from the command and control system, be connected to other existing threats so that chains of potential threats can be determined. Consequently, by starting from the command and control model it should be possible to describe and develop systems with the above capabilities. Hence, it should be possible to exploit different command and control applications to prevent or at least to delimit consequences of crises. To make this possible, methods for cooperative work and communication between various agencies and organizations will be required. Important design aspects that must be considered are e.g. IT-security, human sytems interaction, and decision support tools of various types.

Keywords

Command and control, crisis management, protection, threat

Further bibliographic information	Language Swedish
ISSN 1650-1942	**Pages** 68 p.
	Price acc. to pricelist

Sammanfattning

Sveriges krishanteringsförmåga kommer att vara beroende av att insatsenheter kan samverka oberoende av organisationers kulturella olikheter, människors olika utbildning och expertis och systemens olika tekniska generationer. Det gäller att skapa förutsättningar för denna samverkan genom empiriskt baserad verksamhetsanalys och systemutveckling.

Detta arbetet är en förstudie som beskriver en ledningsfunktion för preventiv och operativ krishantering. Ledningsfunktionen föreslås bli baserad på en ledningsmodell som omfattar metoder för datainsamling, för upptäckt, identifiering, bedömning och hantering av olika hot. Sådana hot skall med stöd av ledningssystemet genom analys kunna kopplas till andra existerande hot så att en sammanhängande hotbild kan byggas upp. Detta skall kunna ske genom att man kan identifiera och bygga upp kedjor av potentiella hotfragment. Således, skall det med utgångspunkt från ledningsmodellen vara möjligt att beskriva och utveckla ett ledningssystem med dessa förmågor. Detta är emellertid inte tillräckligt. Systemet måste också kunna utnyttjas för ledning i operativt syfte vilket avser förmågan att på högre systemnivå kunna leda arbetet med att avvärja eller åtminstone begränsa kriser som brutit ut. För att möjliggöra detta kommer det att krävas metoder för samarbete och kommunikation mellan berörda myndigheter.

Genomförandet av denna verksamhet kräver en modell för ledning och ett ledningssystem med tekniker för bl a IT-säkerhet till skydd för systemet samt olika beslutstöd. Förutom ledningsmodellen kommer också att krävas en till ledningsmodellen och ledningsfunktionen hårt kopplad riskmodell. Syftet med riskmodellen är att ge stöd till ledningsfunktionen. Detta stöd är främst fokuserat mot olika sårbarheter, risker och för bedömning av hot, vilka kommer att behöva värderas för att initiera olika former av motåtgärder i olika krissituationer.

Ett av de huvudsakliga syftena med denna förstudie är att ge en kort beskrivning av grunderna för ledningsfunktionen samt ett lämplig förslag på tillämpning. Projektgruppen har enats kring följande grundläggande antagande som grund för den fortsatta forskningsverksamheten:

- För att en ledningsfunktion skall vara nyttig bör den kunna användas även då kris inte råder.
- Av denna anledning måste ledningsfunktionen kunna anpassas till den dagliga verksamheten.
- Ledningsfunktionen måste ha kapacitet för hantering av extraordinära händelser.
- Människan måste spela en central roll i ledningsfunktionen.

Ytterligare några andra aspekter är att man redan från början av själva utvecklingen av ledningssystemet *måste* ta hänsyn till en mängd olika faktorer såsom *IT-säkerhet, beslutsstödsfunktioner, systemstrukturfrågor, systemarkitekturer.* FOI har stor erfarenhet av att bedriva breda forskningsprojekt och är väl rustat för att bedriva forskning med hög komplexitet och generaliseringsgrad och med omfattande tillämpningar.Vidare ligger det också resultatmässigt ett *mervärde* i forskningsprojekt med bred inriktning dvs projekt med multidisciplinära inslag.

Området ledningsfunktion för krishantering är i sig mycket omfattande och i ett forskningsprojekt med denna inriktning kommer flera relativt omfattande begränsningar att bli nödvändiga för att projektet inte skall svälla ut till en omfattning som blir omöjlig att hantera. Dessa begränsningar kan inte vara för snäva eftersom detta kan leda till alltför triviala frågeställningar. Mot denna bakgrund har projektgruppen beslutat att det är lämpligt att primärt studera vad

som valts att kallas *det lokala samhället.* Med detta begrepp avses den del av samhället som kan omfatta en eller möjligen ett fåtal kommuner. I dessa kommuner skall det finnas några viktiga skyddsvärda objekt som kan knytas till den aktuella tillämpningen. För att genomföra ett projekt med sådan omfattning kommer kontakter med en eller två kommuner, samt med ansvarig länstyrelse, att bli nödvändiga. Dessa organisationer kan härvid agera som referensgrupp och på andra sätt bidra till att göra det möjligt att genomföra tester och demonstrationer som kan vara av intresse för Krisberedskapsmyndigheten. Vid sidan av dessa intressenter finns naturligtvis även andra verk och myndigheter som kan komma att delta; detta beroende på vilka skyddsvärda objekt som kan bli aktuella. Lokal industri med intressen för den angivna problematiken kan på sikt också bli viktiga partner till FOI. I övrigt bör man ha klart för sig att det kan bli nödvändigt att också knyta andra forskningsorganisationer (främst universitet och högskolor men även speciella forskningsinstitut kan komma i fråga) med speciell kompetens till projektet.

Enligt vad som nämnts ovan är det av stor betydelse att ledningsfunktionen skall fungera även under normala omständigheter för att sedan vid behov omvandlas till ett mer kraftfullt instrument för ledning när en kris inträffar. Det huvudsakliga motivet för ett sådant synsätt är självklart att man vill att olika användare skall besitta tillräckligt stor vana vid systemet så att det blir naturligt för dem att använda det när en kris inträffar. Exempel på områden som lämpar sig för detta kan vara:

- sjukdomar; registrering och övervakning (t ex visussjukdomar),
- miljöfaktorer (t ex luftkvaliteteten),
- transporter av farligt gods; kontroll och övervakning,
- kriminella aktiviteter,
- bränder.

De flesta exemplen ovan har potential för att både enskilt och i kombination med någon av de övriga kunna utvecklas till olika typer av kriser. I anslutning till bekämpning av kriser i ett operativt sammanhang behöver också den preventiva aspekten studeras. Detta kan göras som en del av övervakningsprocesserna för någon eller några skyddsvärda objekt. Exempel på skyddsvärda objekt som skulle kunna hanteras här är:

- flygplatser (extern och/eller intern övervakning),
- hamnar (extern och/eller intern övervakning),
- kärnkraftverk (extern övervakning),
- infrastrukturer, t ex för elöverföring.

En lämplig region för den föreslagna inriktningen skulle kunna vara Östergötlands län, t ex i anslutning till Linköpings men också Norrköpings kommun.

Bland de förslag, som framgår av denna rapport, och som kan beteknas som huvudresultaten av denna förstudie kan pekas på att en ledningsfunktion för preventiv och operative krishantering bör baseras på dels en modell för ledning och en modell för riskhantering. Tillsammans utgör dessa båda modeller hörnstenar i det ramverk som bör bilda grunden för det fortsatta arbetet med att utveckla den förslagna typen av ledningsfunktion för krishantering.

I denna rapport utgör kapitel 1 en introduktion till själva förstudien. I kapitel 2 ges en bakgrund till den problematik som tas upp i denna rapport. Hot av olika slag diskuteras i kapitel 3. Vidare sker i kapitel 4 en genomgång av ledningsproblematiken. I kapitel 5 sker sedan en

genomgång av det ramverk som utgör en central del av denna förstudie. I detta ramverk diskuteras strukturen för lednings- och riskmodellen. I kapitel 6 sker en genomgång av de aktuella forskningsområden som kommer att få stor aktualitet för ett forskningsprojekt med denna inriktning. Därpå sker en genomgång, i kapitel 7, av den föreslagna tillämpningen. Kapitel 8, slutligen, ger en översikt av relaterade arbeten med inriktning mot ledningssystem för krishantering.

Innehållsförteckning

1 Inledning

Samhället och civilbefolkningen är numera både mål och arena för existerande och framtida hot [10]. Det moderna samhället är beroende av olika tekniska infrastrukturer, d v s grundläggande system väsentliga för att samhället skall fungera och som direkt eller indirekt används av flertalet medborgare. Framförallt avses infrastrukturen för energiförsörjning, telekommunikationer, distribution av etermedia och IT-system, bl a inom den finansiella sektorn. Dessutom omfattas de lokala försörjningssystemen (vatten, avlopp och fjärrvärme), transportnätet (flyg, järnväg, sjöfart och större vägnät), sjukvårdsresurser och samhällsviktig industri. Energiförsörjningen är en funktion av särskilt intresse eftersom flertalet verksamheter för sin funktion är beroende av en fungerande energiförsörjning. Utvecklingen har lett till att många system kopplas samman genom komplexa nätverk. Detta och den ökade integrationen av främst telekommunikationer, IT-system och massmedia innebär att de ömsesidiga beroendena mellan olika infrastruktursystem ökar. Omfattande störningar kan leda till bortfall av viktiga funktioner, avsevärda ekonomiska konsekvenser samt i värsta fall förlust av liv och egendom. I förlängningen kan angrepp mot samhällsviktig infrastruktur också hota säkerheten på nationell nivå.

Sveriges framtida krishanteringsförmåga kommer att vara beroende av att insatsenheter kan samverka mellan olika organisatoriska kulturer, mellan människor med helt olika utbildning och expertis och mellan system av olika tekniska generationer. Det gäller att skapa förutsättningar för denna samverkan genom empiriskt baserad verksamhetsanalys och systemutveckling.

Komplexiteten vid ledning i krishantering förväntas öka i avsevärd grad med hänsyn till att framtida kriser befaras bli mer omfattande och att de kommer att inverka på snart sagt alla samhällsfunktioner. Mot denna bakgrund måste system, som skall bidra till att skydda enskilda människor och samhället, omfatta såväl en preventiv som en operativ skyddsfunktion för att minska konsekvenserna av kriser och svåra påfrestningar. Detta ställer stora krav på den ledningsfunktion som behövs för att göra det möjligt att på ett kraftfullt sätt ge stöd för att lösa dessa kriser och samtidigt vidmakthålla och skydda samhällets olika funktioner. Redan från början av utvecklingen av en sådan ledningsfunktion måste hänsyn tas till en mängd olika faktorer såsom IT-säkerhet, beslutsstödsfunktioner, systemstrukturfrågor, systemarkitekturer, människa-systeminteraktion och systemtilltro. Om någon väsentlig aspekt inte från början är inkluderad kommer detta att leda till att det senare blir svårt, för att inte säga omöjligt, att integrera de saknade aspekterna. Det är därför nödvändigt att alla dessa aspekter beaktas redan i utvecklingsfasen och det är av samma skäl nödvändigt att ta ett helhetsgrepp över problematiken med ledningsfunktionen vid krishantering redan i ett tidigt skede. Ett sådant arbete bör också omfatta stöd för skydd av olika objekt och strukturer samt frågor om sårbarhet och planering. Fokus behöver således inriktas mot ett ledningssystem som sträcker sig från dess indatakällor till dess olika aktörer. Huvudmålsättningen för ett sådant ledningssystem är att det skall kunna utnyttjas mot aktiviteter som innefattar hot riktade mot samhället och dess medborgare. En sammanfattning av syftet med denna förstudie är mot denna bakgrund väsentligen

- att definiera strukturen för *den tekniska ledningsfunktionen* i ett ledningssystem för krishantering, med hänsyn till såväl *operativ* som *preventiv krishantering.*

- att föreslå ett forskningsprojekt i vilket man skall ta ett helhetsgrepp över problematiken med ledningsfunktionen vid krishantering.

I kapitel 2 ges en bakgrund till den problematik som tas upp i denna rapport. Hot av olika slag diskuteras i kapitel 3. Vidare sker i kapitel 4 en genomgång av ledningsproblematiken. I kapitel 5 sker sedan en genomgång av det ramverk som utgör en central del av denna förstudie. I detta ramverk diskuteras strukturen för lednings- och riskmodellen. I kapitel 6 sker en genomgång av de aktuella forskningsområden som kommer att få stor aktualitet för ett forskningsprojekt med denna inriktning. Därpå sker en genomgång, i kapitel 7, av den föreslagna tillämpningen. Kapitel 8, slutligen, ger en översikt av relaterade arbeten med inriktning mot ledningssystem för krishantering.

2 Bakgrund

En enkel definition av krishantering är *hantering av den påverkan som destruktiva händelser har på samhället i de fall man kan bedöma att denna påverkan kan komma att pågå under lång tid och i stor skala*. Hanteringen av dessa problem måste ske både operativt och preventivt med hjälp av ett ledningssystem för krishantering.

2.1 Ledningssystem för krishantering

Krishantering är i sig en komplex verksamhet och därmed blir även ledningssystem för krishantering komplexa och måste innefatta ett antal funktioner såsom stöd för att kunna

- uppnå samverkan mellan olika organisationer och myndigheter,
- samla in nödvändig information,
- hantera stora datavolymer som kan innefatta osäker och motstridig information,
- bearbeta och analysera inkommande information; även mot bakgrund av andra kunskaper,
- ta fram underlag för beslutsfattande,
- säkerställa sekretess, tillförlitlighet och tillgänglighet av information,
- delge inblandade parter en adekvat och konsistent (i betydelsen korrekt, entydig) lägesbeskrivning,
- integreras med förekommande och nödvändiga nätverkstillämpningar,
- kommunicera beslut, och
- bidra till att informera allmänheten.

Huvudsakliga tillämpningsområden för ett sådant system kommer att vara:

- identifiering av och skydd mot olika potentiella hot
- skydd av olika skyddsvärda objekt inklusive människor
- ledning vid extraordinära händelser i samverkan med bl a polis, räddningstjänst, kommuner, länstyrelser etc.

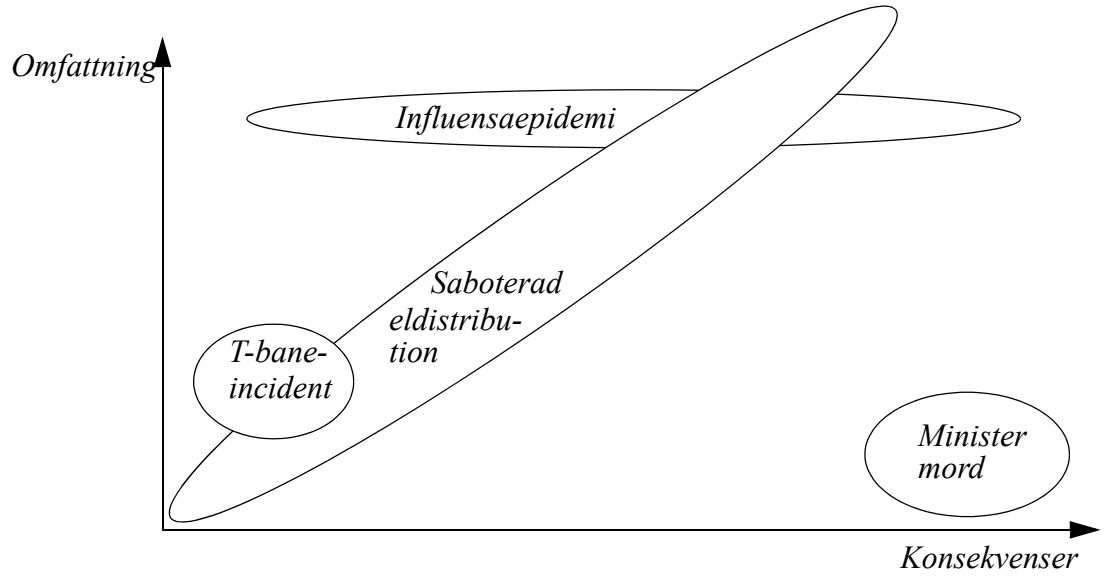
Systemet skall kunna användas på olika nivåer. Dessa nivåer kan omfatta den lokala nivån, dvs kommuner, och den regionala nivån, för bättre samordning mellan de olika aktörerna. Slutligen bör ett sådant system också kunna användas på nationell nivå.

2.2 Kriskaraktäristik

En kris i samhället med en relativt begränsad omfattning kan ändå innebära stora konsekvenser för invånarna, samtidigt som även motsatsen (dvs stor omfattning och begränsade konsekvenser) kan gälla. En influensaepidemi kan t ex lätt få stort fäste bland människor i samhället utan att för den skull konsekvenserna genast blir stora. Tid och möjligheter till tillfrisknande har förmodligen större inverkan på hur samhället reagerar. En för riket allvarlig händelse som t.ex. ett ministermord, som ju egentligen drabbar få personer direkt, kan genast få svåröverskådliga konsekvenser. Ett försök att åskådliggöra detta visas nedan i figur 1.

Om flera händelser läggs till varandra ligger det nära till hands att anta att konsekvenserna växer snabbare än omfattningen. Detta ställer stora krav på det ledningssystem som används att inte bara begränsa och häva den befintliga krisen utan även ha viss förmåga att förutse och förhindra ytterligare händelser. Ett antagonistiskt hot skulle kunna utnyttja sådana tillfällen där

en åtgärd av liten omfattning kan medföra stora konsekvenser genom att samhället redan befinner sig i ett begynnande krisläge.



Figur 1. Exempel på kriser med deras omfattning och konsekvenser

2.3 Regional och lokal krishantering

Utgångspunkten för ansvarsfördelning gällande samhällets beredskap för och hantering av svåra kriser och påfrestningar är att detta skall baseras på normal, i fredstid genomförd, verksamhet. Detta bygger på tre centrala och grundläggande principer för ansvarfördelning [93]:

- Ansvarsprincipen innebär att den som har ansvar för en verksamhet under normala förhållanden skall ha motsvarande ansvar under kris- och krigssituationer.
- Likhetsprincipen innebär att en verksamhets organisation och lokalisering så långt som möjligt skall överensstämma i fred, kris och krig.
- Närhetsprincipen innebär att kriser skall hanteras på lägsta möjliga samhällsnivå.

Dessa principer innebär att varje myndighet och organisation ansvarar för sitt verksamhetsområde i samband med stora olyckor eller kriser. Denna "normala" verksamhet kompletteras för att stå emot och hantera svåra påfrestningar. En fundamental del i detta är att på lokal nivå ha beredskap och krishanteringsförmåga, och sedan komplettera detta med samordning och viss förmåga på regional och nationell nivå. Vid sida av verksamhetsansvaret finns geografiskt områdesansvar. Det geografiska områdesansvaret innefattar ett lednings- och samordningsansvar. Detta skall finnas på lokal, regional och nationell nivå. Det lokala områdesansvaret har pålagts kommuner, länsstyrelser det regionala och regeringen det nationella områdesansvaret. Regeringen bedriver även ett utvecklingsarbete för att stärka sin förmåga som nationellt områdesansvarig.

En kris får alltid konsekvenser på lokal nivå. Kommunerna har därför en nyckelroll i krisberedskapen. En hög förmåga att hantera kriser på lokal nivå ökar också samhällets förmåga att hantera kriser som drabbar flera kommuner. På regional nivå ansvarar länsstyrelserna för motsvarande samordning. En viktig uppgift i detta är att stödja kommunerna i deras arbete. (Krishanteringssystemet)

2.3.1 Regional krishantering

Det regionala områdesansvaret innehas av länsstyrelserna som utgör den högsta civila totalförsvarsmyndigheten i respektive län. Deras uppgift är att samordna samhällets resurser vid en svår påfrestning eller under en kris. I denna samordning ligger också ett informations- och kriskommunikationsansvar.

Länsstyrelserna skall hålla sig underrättade om händelseutvecklingen i sådana situationer i fredstid som berörs i "krisberedskapsförordningen" och verka för att nödvändig samverkan kan åstadkommas. De skall upprätthålla och utveckla kompetensen inom det civila försvaret, den fredstida krishanteringen samt inom räddningstjänsten. I deras ansvar ingår även att planera för hur konsekvenserna av svåra olyckor, stora påfrestningar på samhället, eller i yttersta fall krig kan minskas. För att förebygga allvarliga olyckor granskar länsstyrelserna anläggningar som hanterar farliga kemikalier och processer både ur risk- och miljösynpunkt. Detta ständigt pågående arbete med förebyggande riskhantering och riskanalyser är i hög utsträckning långsiktigt förebyggande. Syftet är att skapa ett mindre sårbart samhälle som allt bättre ska klara av olika typer av påfrestningar och störningar. Länsstyrelserna ansvarar även för att se till att de organisationer i samhället som samverkar vid kriser övar tillsammans. Vid mycket svåra händelser har Länsstyrelsen möjlighet att ta över ledningsansvaret för att underlätta samordningen.

I länsstyrelsernas lednings- och samordningsroll ingår ett informationsansvar [94]. Detta innebär att vid omfattande olyckor eller svåra påfrestningar skall länsstyrelserna samla in information för att kunna lämna saklig information om händelseutvecklingen till allmänheten. Länsstyrelserna skall även i förebyggande syfte sprida information om risker, beredskap och civilt försvar.

Slutligen skall länsstyrelserna ge kommunerna stöd med att utveckla och genomföra deras uppgifter som områdesansvariga. I detta ingår att länsstyrelserna kontrollerar de kommunala räddningstjänsterna för att se till att de kan fullgöra sina uppgifter [95].

2.3.2 Lokal krishantering

Det lokala områdesansvaret innehas av kommunerna vilket innebär att de ansvarar för att krishantering inom kommunens geografiska område samordnas, så väl förberedande som operativt. Kommunernas samordningsansvar innebär dock ej att de tar över någon annan organisations verksamhetsansvar i samband med en kris, utan enbart att de skall verka för samverkan och samordning.

Vid kris skall många verksamheter och ledningsnivåer verka och samverka. Detta ställer höga krav på planering och förberedelser. Utarbetade organisationsformer, inhämtad kunskap, nyttjande av modern teknik etc. skapar förutsättningar för att kommunerna skall kunna fullfölja sitt uppdrag att samordna krishanteringen. Även möjligheten att samverka över kommungränser är viktigt, då kommunerna kan ge varandra stöd i krishanteringen, såväl med strategisk planering som operativa insatser [96].

Vid uppkomst av kris skall alarmeringsrutiner medföra att insatser sätts igång snarast möjligt. Detta förutsätter att en krisledning med rätt till beslutsfattande kommer igång snabbt och att denna har tillgång till en ledningsplats.

Kommunerna har även ett verksamhetsansvar vilket innefattar säkerställande av att den kommunal verksamhet som anses oumbärlig alltid måste kunna genomföras. Det inkluderar även

förmågan att kunna tillgodose särskilda behov av exempelvis information och stöd till enskilda, som uppkommer genom krisen.

För att kommunerna ska kunna klara denna uppgift måste varje kommun ha en organisation för krishantering som ska vara bemannad, utbildad och övad. Kommunerna måste också ha planer och annat underlag för krishanteringen, förberedda lokaler m m.

2.4 Skyddsvärda objekt

Av specifik betydelse är också att identifiera objekt som kan utsättas för olika typer av hot. Sådana objekt måste kunna skyddas och av denna anledning krävs att preventiva åtgärder kan vidtagas. Vilka åtgärder som skall vidtagas är i hög grad betingat av vilka typer av objekt som skall skyddas. Dessa objekt kan klassificeras på en mängd olika sätt. Exempelvis kan man skilja på skyddsvärda objekt där hotet också riktar sig mot människor som befinner sig i eller omkring det aktuella objektet. Bland dessa kan nämnas:

- Järnvägs- och tunnelbanestationer
- Flygplatser
- Hamnar
- Transporter av allmänfarligt gods
- Polisstationer
- Räddningstjänster
- Maktcentra av olika slag (politiska, ekonomiska, militära etc.)
- Allmänna kommunikationsmedel (bussar, tåg, flygplan etc.)
- Nöjesevenemang och politiska stormöten
- Kärnkraftverk

Andra skyddsvärda objekt, som där antalet människor i direkt anslutning till själva objektet inte är så stort men där ett stort antal människor kan hotas indirekt om de aktuella skyddsvärda objekten förstörs eller på annat sätt slås ut, är till exempel:

- TV-/radiostationer (sändare)
- Telekommunikationscentraler
- Infrastruktur, t ex el-nät

2.5 Övergripande forskningsfrågor

På övergripande nivå kan ett stort antal forskningsfrågor identifieras som har bäring enligt den ovan angivna problematiken. Bland dessa forskningsfrågor kan bl a nämnas:

- Hur skall olika skyddsvärda objekt övervakas i preventivt syfte?
- Vilka objekttyper är skyddsvärda?
- Vilka typer av hot kan tänkas förekomma?
- Hur kan man avgöra om en händelse eller en person utgör ett hot eller en del av ett hot?
- När skall ansvariga myndigheter larmas?
- Vilka metoder behövs för hotbestämning?
- Hur kan komplexa relationer mellan olika objekt som var för sig kan utgöra ett hot identifieras?
- Hur kan olika typer av hot och deras status beskrivas så att aktören får en relevant lägesuppfattning i varje givet ögonblick?

I kapitel 7 kommer några viktiga forskningsfrågor att diskuteras vidare i anslutning till förslaget till ett forskningsprojekt om en ledningsfunktion för krishantering.

2.6 Forskningsområden

Kunskap och forskningsinsatser från ett antal och vitt skilda discipliner krävs för att ta ett helhetsgrepp gällande utveckling av ledningssystem för preventiv och operativt krishantering. Exempel på centrala kunskapsområden är:

- Systemarkitektur
- Systemutveckling
- Beslutsstöd
- Människa-systeminteraktion
- Systemtilltro
- Informationsfusion
- Systemorganisation
- IT-säkerhet i bred mening
- Sensordataanalys
- Nätverk för datakommunikation
- Databrytning
- Logistik
- Träning och utvärdering
- Geoinformatik

3. Hotbilden och preliminära slutsatser om dess tillämpningar för ledningssystem och ledningsverksamhet

I detta kapitel diskuteras de hot som bedöms vara aktuella för ledningsfunktionen inklusive ledningssystemen, och de konsekvenser som kan uppkomma. Viktiga frågor att analysera är:

- Hur kan krisen tänkas uppkomma?
- Vilka hot, allmänt riktade mot samhället, är mest aktuella för en ledningsgrupp att hantera konsekvenserna av?
- Vad hotar ledningen, dess system, verksamhet och personal?

Diskussionen sker här kring de två första frågorna ovan vilka ger den mesta informationen om den miljö som ledningsfunktionen har att verka i, och om de uppgifter som skall hanteras. Vår bedömning är därför att dessa bör behandlas i första hand. Hot som mer specifikt riktar sig mot ledningsfunktionen behandlas också, men mer kortfattat i slutet av kapitlet.

	Mänskligt agerande		**Ej mänskligt agerande**
	ANTAGONISTISKT	**ICKE-ANTAGONISTISKT**	
Inre orsaker	Infiltration Insiderverksamhet	Felhandlingar Bristande underhåll Dimensioneringsfel Konstruktionsfel	Tekniskt fel Tillverkningsfel
Yttre orsaker	Sabotage Terrorism Väpnat angrepp	Felhandlingar	Naturrelaterade händelser Brister i andra system (beroenden)

Tabell 1. Olika typer av hot.

3.1 Hotstrukturer

Hotbilden kan konkretiseras och hoten struktureras på olika sätt beroende på syftet. För denna studies syfte förefaller det naturligt att främst skilja på *antagonistiska* och *icke antagonistiska* hot, se tabell 1.

Antagonistiska hot innebär att det finns en angripare som strävar efter att åstadkomma en skada. Typiska exempel på antagonistiska hot är sabotage och krigshandlingar. Icke antagonistiska hot som beror på människors agerande är olika typer av felaktigt agerande, i första hand i den akuta situationen (”den mänskliga faktorn”). Icke antagonistiska hot som inte beror på människors agerande är exempelvis olika naturrelaterade händelser samt felfunktion eller haverier i olika tekniska produkter och system. Sådana tekniska fel kan givetvis bero på fel-

konstruktion eller bristande underhåll, dvs på människors agerande, varför gränsen mellan dessa hot är flytande.

I detta sammanhang måste man också beakta de beroenden som finns mellan olika tekniska system, och som innebär att en skada i ett system leder till att ett annat drabbas av störningar eller avbrott. Mycket viktigt att framhålla är att många system i samhället är beroende av elektricitet och alltså kan drabbas av svåra störningar om eltillförseln störs

De hot som kan bedömas orsaka så svåra konsekvenser för samhället att de bör kunna vara dimensionerande för ledningen och ledningssystemet är främst olika former av antagonistiska hot, naturrelaterade händelser, samt sådana svåra störningar i olika infrastruktursystem (främst el- och telesystemen), som ger allvarliga konsekvenser för hela samhället.

Ledningsfunktionen, dess personal och lokaler kan av en potentiell angripare ses som en del av ”systemet” som angriparen vill attackera. Sabotagemässiga attacker direkt riktade mot funktionen är därför tänkbara. Mest troliga är attacker mot el-, tele- och vattenförsörjningen, men attacker direkt mot personalen kan inte heller uteslutas. Särskild uppmärksamhet måste ägnas åt insiderproblematiken.

3.1.1 Antagonistiska hot

Viktiga grundläggande dokument som beskriver hotbilden beträffande antagonistiska hot är propositionerna [1],[2]. I kort sammanfattning innebär dessa att militära angrepp från staters sida tonas ner, även om de inte kan uteslutas på sikt. Specifika åtgärder för att möta dessa hot vidtas inte idag, utan planeras ske under en s k anpassningsperiod. Vad som förs fram är hot från andra aktörer än stater, men som förfogar över avancerade metoder och vapen. Händelserna i USA den 11 september 2001 nämns som exempel som påvisar att sådana organisationer kan genomföra terroraktioner med stora konsekvenser. Därefter spreds mjältbrandssporer via postförsändelser samtidigt som flera mjältbrandshot utfördes i form av brev med misstänkt innehåll. Regeringens slutsats är att terroraktörer i framtiden kan komma att använda B-, C-stridsmedel och även radioaktiva ämnen, samt att dessa hot måste uppmärksammas i ökad utsträckning. Massförstörelsevapen kan te sig attraktiva för terroristgrupper och kriminella genom att de kan drabba många personer, och genom att de innebär mycket spektakulära attacker.

En annan slutsats regeringen drar är att de tekniska infrastruktursystemen får en allt mer uttalad fundamental betydelse för samhället. Angrepp mot dessa anses kunna få mycket allvarliga konsekvenser. Ett antal faktorer framförs också som innebär större möjlighet även för mindre intressegrupper, kriminella grupper och terrorister att påverka, och dessa oavsett var i världen dessa aktörer befinner sig. Betydande åtgärder bör vidtas för att minska både sårbarheten i systemen och reducera konsekvenserna för samhället av störningar i systemen. Vidare säger propositionen att åtgärder bör inriktas på att hantera de beroenden och kopplingar som finns.

Vår bedömning är att antagonistiska handlingar från extrema organisationer med politiskt, etniskt eller religiöst syfte har blivit allt mer aktuella under senare år. En grogrund för sådana organisationer finns även i vårt land. Sådana organisationer kan alltså vara inhemska, men även agera med stöd utifrån. Såväl enklare sprängmedel som avancerade vapen och även B- och C- stridsmedel och radioaktiva ämnen skulle då kunna komma till användning. Syftet med en attack kan tänkas vara att protestera mot statsmakternas agerande mot minoriteten, att skada en motpart, att utöva utpressning eller att påverka vårt internationella agerande. Det sistnämnda syftet kan komma att accentueras eftersom Sverige alltmer kommer att delta i civila

och militära insatser utomlands. Mål för attackerna kan vara tekniska infrastruktursystem som el, tele och radio/TV, större folksamlingar, befolkningscentra och objekt som uppfattas som knutna till statsmakterna eller till utländska intressen.

Viktiga infrastruktursystem som el, tele och vattenförsörjningen är sårbara för sabotage via konventionella sprängmedel och även för olika typer av IT-attacker. Ledningsfunktionen måste vara beredd att hantera situationer efter sådana sabotage, och även utformas med hänsyn till att avbrott i sådana funktioner kan uppkomma på grund av sabotage.

Vår slutsats blir att ledningen och ledningssystemet måste vara berett på att hantera situationer som uppstått efter angrepp av terroristorganisationer med exempelvis politiska eller religiösa motiv. Bedömningen är också att det - med de modifieringar och reservationer som framgår nedan - är antagonistiska angrepp som bör vara dimensionerande hot för ledningsfunktionen. Beträffande elförsörjningen bedömd det nödvändigt att ledningsfunktionen dimensioneras för att klara ett allmänt el-avbrott på 6 till 12 timmar.

3.1.2 Icke-antagonistiska hot

De icke-antagonistiska hot som vi bedömer vara de som ledningsfunktionen bör ta störst hänsyn till är:

- avbrott i viktiga infrastruktursystem, samt beroenden dem emellan,
- naturrelaterade händelser med särskilt allvarliga konsekvenser (naturkatastrofer).

Andra händelser, som preliminärt bedömts vara sådana att de inte blir dimensionerande för ledningsfunktionen nämns också nedan.

3.1.3 Övriga icke antagonistiska hot

Tågolyckor med farligt gods inblandat inträffar med jämna mellanrum. Inom ramen för Hot- och riskutredningen [5] utarbetades ett scenario där en ammoniaklastad järnvägsvagn brister i en större stad [6]. I scenariot avlider 80 personer och 4-5000 personer tvingas söka vård på sjukhus och vårdcentraler. Scenariot ger en god beskrivning av konsekvenserna av en kemikalieolycka.

3.2 Avbrott i viktiga infrastruktursystem

Ett flertal studier och bedömningar har visat att den svenska elförsörjningen normalt är mycket pålitlig. De mest omfattande störningarna, sådana som berör flera län, inträffar som följd av avbrott i det s k storkraftnätet. Sådana avbrott är ovanliga och beror nästan alltid på en kombination av flera händelser, som t ex tekniska fel i kombination med felhandlingar. Dessa avbrott, liksom erfarenheter från liknande händelser utomlands, visar på systemens sårbarhet och på att en helt säker eltillförsel från storkraftnätet inte kan garanteras. Detta resonemang leder till att samtliga elanvändare måste kunna hantera ett el-avbrott under viss tid. Ledningsfunktionen måste dessutom kunna arbeta i en situation med avbrott i elförsörjningen. Vår bedömning är att det hot som denna typ av el-avbrott utgör, täcks in och kan hanteras via de åtgärder som vidtas med hänsyn till de antagonistiska hoten.

Telekommunikationerna är också ett av de viktigaste infrastruktursystemen. För sårbarhetsresonemang bör man inom telefunktionen skilja på det fasta telenätet och mobiltelefonin. Telias fasta telenät har mycket av inbyggd redundans och reserver och måste betraktas som tämligen säkert. Allvarliga avbrott är ovanliga. Mobiltelefonin är inget eget system, där finns basstatio-

ner som tar emot signaler från telefonerna, kopplingsstationer som överför signalerna till det fasta nätet, samt olika datoriserade styrsystem och register. Flera olika aktörer är verksamma inom mobiltelefonin. Var och en av dessa har egna stationer och register omfattar flera aktörer vilket leder till risk för redundans.

Utvecklingen på teleområdet går mycket snabbt, både beträffande författningar, organisationen (aktörerna) och den tekniska infrastrukturen. Utbyggnaden av mobiltelefoni, IP-telefoni och satellitförbindelser är uppenbara exempel på detta. Även inom den fasta telefonin sker en utveckling som karakteriseras av att flera aktörer bygger upp egna nät vid sidan av Telias nät. Allt detta innebär att hotbild och sårbarhet beträffande telekommunikationerna måste bedömmas och omprövas med täta mellanrum.

Även avbrott i vattendistributionen skulle på sikt leda till en svår påfrestning på samhället. Ett scenario med detta innehåll utarbetades inom Hot- och riskutredningen [3]. En förnyad analys av detta fall inom ramen för en huvudstudie kan vara lämplig.

Så gott som samtliga funktioner i samhället är beroende av eltillförsel, något som ofta påpekas i massmedia. Mellan el- och telefunktionerna finns ett ömsesidigt beroende. Telekommunikationerna är beroende av el till sina stationer och förbindelser. Inom elfunktionen överförs viktig styr- och övervakningsinformation via (ofta egna) teleförbindelser. För ledningsfunktionen har dessa beroenden framför allt betydelse när arbetsplatsen ska utformas. Det är då viktigt att analysera risken för el- respektive teleavbrott och vilka konsekvenserna kan bli.

3.3 Naturrelaterade händelser

I flera älvsystem finns stora kraftverksdammar med vattenmagasin. Ett genombrott i en sådan damm ter sig mycket osannolikt, men skulle om det verkligen inträffade medföra mycket stora skador nedströms. Ett genomarbetat översvämningsscenario ges i Räddningsverkets rapport [4] som beskriver ett dammgenombrott och dess följder.

Snöoväder som innebär isolering av enstaka bostäder under upp till några dygn inträffar nära nog årligen, och kan inte betraktas som en svår påfrestning för samhället. Större konsekvenser, med avstängning av större vägsystem och isolering av större städer, uppstår några gånger per århundrade.

4. Lednings- och skyddsfunktionen

Krishantering, räddningsinsatser och katastrofinsatser är komplexa dynamiska högriskaktiviteter i vilka många människor och tekniska system tillsammans utför uppgifter med extrema krav på rörlighet, effektivitet, vaksamhet och beslutsamhet. Taktiska enheter, organisationer och resurser är utspridda (distribuerade) över insatsområdet. Enheterna måste struktureras i distribuerade systemarkitekturer för att kunna lösa sina uppgifter samtidigt som säkerhet och effektivitet upprätthålls. De kan fungera självständigt under viss tid och inom vissa områden, men är oftast tvingade att koordinera sina handlingar mycket noggrant.

4.1 Insatsledning vid krishantering kräver kraftfullt ledningsstöd

Att utföra sådana komplexa riskfyllda operationer kräver många typer av stöd, bland annat i form av högkvalificerade ledningsfunktioner [12]. Ett ledningssystem för krishantering bör kunna hantera ett brett spektrum av allvarliga händelser som bl a karaktäriseras av brist på relevant och tillförlitlig information, osäkerhet om händelseförloppet och dess konsekvenser, tidspress, starkt offentligt och socialt tryck via medias uppmärksamhet samt behov av att samordna samhällsfunktioner som inte säkerställs genom spontan samverkan. Ledningssystemet bör bygga på ordinarie organisationsstruktur och befogenheter, men på grund av de karaktäristiska drag som ovan exemplifierats behöver ett ledningssystem som skall klara krishantering kompletteras med rutiner och arbetsformer som ger förutsättningar att verka under exceptionella omständigheter. Detta gäller både svåra påfrestningar på samhället i fredstid och andra allvarliga krissituationer.

Ett av de största problemen med att arbeta inom ett så vittomfattande problemområde är att uppfylla ett flertal fundamentalt olika, ofta starkt motstridiga krav på ett fullgott ledningssystem. En delmängd av dessa krav identifieras och formuleras av Foss [9], Wishart [11] och Worm [15] nedan:

- Chefer skall kunna överblicka, förstå och predicera (förutse) icke-linjära händelseförlopp. Detta kräver stöd för distribuerat dynamiskt beslutsfattande med ett kraftfullt simuleringsstöd för säkrare prediktion.
- Moderna ledningsprinciper kräver avancerade informationshanteringsresurser med mycket snabb och tillförlitlig manuell och automatiserad inhämtning och bearbetning av information för att kunna utvärdera och förstå händelseutvecklingen i insatsen samt för att kunna revidera målbilden i samverkan med stöd från andra enheter.
- Ledningssystemen arbetar i nära realtid på alla nivåer. Detta kräver robust och säker bredbandig kommunikation mellan insatsenheterna för att säkerställa förmågan att bevaka händelseutvecklingen.

Detta kräver i sin tur ett ledningssystem som kan åstadkomma ett kontinuerligt informationsflöde i alla riktningar, från den högsta ledningen till gruppen/teamet på den aktuella platsen. I vissa fall måste till och med individuella operatörer eller sensorsystem tillåtas att utan tidsfördröjning påverka en insatschefs beslut och handlingar. Detta kommer inte att vara möjligt om inte innovativa lösningar kan stödja människor och tekniska system i insatsenheterna.

Verksamheten har behov av information som kan förädlas med applikationer, vilka stöds av en teknisk infrastruktur. Informationens innebörd för den som inhämtar, bearbetar och delger är alltid föremål för tolkning hos mottagaren. Information hanteras i ett flertal olika format, t ex auditiv, textuell, visuell, formaterad, oformaterad, och kan överföras i både analog och digital form. Information som representerar kunskap hos avsändaren leder dock inte till motsvarande

kunskap hos mottagaren i fall inte denne också har insikt i det sammanhang, kontexten, som bestämmer ramverket inom vilket informationen kan vara relevant [17]. Insikt råder när någon uppnår en djupare förståelse av underliggande orsaker och samband. Färdigheter, d v s förmåga att utföra något i praktiken, uppstår som regel genom en kombination av kunskaper, insikter och erfarenheter. Däremot utgör information en möjlighet till kunskapsuppbyggnad hos mottagaren. För att informationen skall omvandlas till faktisk kunskap krävs att mottagaren vill och kan tolka informationen.

4.2 Aktionsstyrning

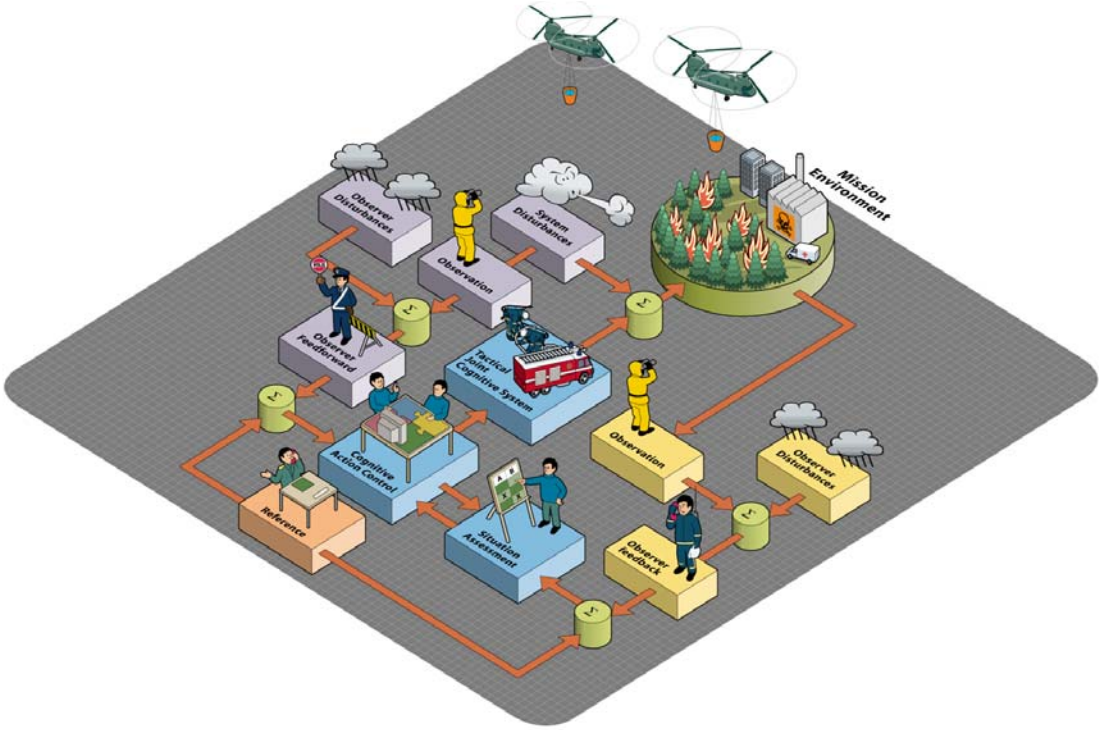
För att lösa ledningsproblem vid krisinsatser krävs banbrytande metoder. Taktik, teknik, metoder och utbildning måste ständigt sträva efter perfektion. Samtidigt är det svårt att peka på de viktigaste färdigheter och egenskaper som människor och system måste ha för att kunna ge sitt bästa i kritiska lägen. Det som är svårt att peka på är också svårt att förbättra. Det finns mycket att vinna med tvärvetenskapliga angreppssätt på solid klassisk och innovativ teoretisk grund. Det leder till heltäckande men ändå enkla, robusta och lätt modifierbara modeller som kan stödjas av avancerade experimentella, mättekniska och analytiska metoder. Den bärande principen är att samordna väletablerade vetenskapsgrenar till en ny forskningsinriktning: Aktionsstyrning (Eng: Action Control Theory, förkortn: ACT). Aktionsstyrning [13] har sin bas i forskningsområdena:

- kognitiv systemvetenskap (Eng: Cognitive Systems Engineering (CSE)),
- systemteori, reglerteori och cybernetik,
- beslutsteori, främst inom tidskritisk insatsledning i högriskmiljöer, och
- psykofysiologisk stressteori.

ACT medger empiriskt baserad modellering, analys och värdering av taktiska förenade kognitiva system i flera nivåer samt av deras tillstånd och tillståndsövergångar. En taktisk aktionsstyrningsmodell kan då utvecklas. Dess huvuddelar är insatsmiljön, insatsenheten, insatsuppföljningsfunktionen och den kognitiva aktionsstyrningsfunktionen. Nästa steg är att bygga upp den egentliga insatsledningsmodellen. Insatsenheten kan därmed också hantera systemstörningar och modellfel. Sista steget i modelleringen är att kombinera flera insatsledningsmodeller till en taktisk distribuerad insatsmodell med flera nivåer. Modellerna som utvecklats fångar de relevanta egenskaperna hos ett integrerat insatsledningssystem på taktisk nivå och är samtidigt så enkla att de möjliggör simulering, utvärdering och analys.

4.3 Empiriskt baserad analys och modellering av insatsledning

Fältförsök och studier av olika enhetstyper inom armén och räddningstjänsten har genomförts i syfte att studera ledning, informationsbehandling och beslutsfattande i olika taktiska exempel. Det visade sig vara nödvändigt att utveckla ett helt metodpaket, kallat Tactical Real-time Interaction in Distributed ENvironmenTs (TRIDENT) för att kunna genomföra en insatsanalys i sådana tillämpade situationer [13]. Det var av särskilt intresse att undersöka hur insatsenheternas förmåga att lösa sin uppgift varierar med ledningsfunktionens förmåga att leda insatsen [14], [15], [16]. Det var också av intresse att studera insatsenheternas förmåga att inhämta, bearbeta och utnyttja tillgänglig information, insatsledningens utnyttjande av insatsstyrkans tillgängliga resurser och slutligen insatseffektiviteten, som är insatsens utfall och effekt i förhållande till utnyttjade resurser. Låt oss studera ett exempel: en räddningsinsats vid en skogsbrand nära bebyggelse, se figur 2.



Figur 2. En insats vid en skogsbrand nära bebyggelse [13], [14].

4.3.1 Situationsbeskrivning

En större skogsbrand har rasat under två dagar. Räddningstjänsten har bekämpat branden sedan den bröt ut. Av den egna personalen har flera nyckelpersoner såsom rökdykarledare, brandmästare och specialfordonsförare råkat ut för skador, men de har efter omplåstring kunnat återgå i tjänst. Övrig personal börjar uppvisa tecken på allvarlig utmattning. Utrustningen har vid flera tillfällen visat sig vara otillräcklig för omfattande skogsbrandbekämpning. Detta har föranlett att tillkalla externa resurser enligt räddningstjänstlagen. Polis sköter omdirigering av trafik samt evakuering, övervakning och avspärrning av drabbade områden för att förhindra att boende i området skadas, samt för att förhindra plundring av ensligt belägna bostäder i området. Lokala frivilligbrandkårer och hemvärn assisterar i eftersläckningsarbete, och yrkesbrandkårer från andra distrikt understödjer släckning och avgränsning med brandgator i de områden där branden fortfarande rasar.

4.3.2 Insatsens avsedda sluttillstånd

Insatsledningens målbild är att efter ytterligare ett dygn skall branden ha begränsats så att den inte kan sprida sig ytterligare till tidigare förskonade områden. Därefter skall eftersläckning pågå tills faran för "återtändning" är över. Personalen kommer att behöva avlösning snarast och förberedelser skall påbörjas för överlämnande till pågående räddningsledningslag. Väderläget är gott, ostlig vind gör att insatsen kan koncentreras till den västra brandfronten. Eftersläckningsarbete kommer att ske i ytterligare 7 - 10 dagar beroende på markvegetationens beskaffenhet.

4.3.3 Prediktion, mental simulering och planering

Den största faran just nu är en plötslig vindkantring från ostlig till västlig (= en systemstörning). Det kommer att medföra ytterligare utbredning av brandområdet samt att bebyggelse hotas. I bebyggelsen finns bland annat en kemisk industri med stora mängder klorgas och tetra-

klormetan (lösningsmedel som bildar stridsgasen Fosgen vid upphettning!) samt intill denna ett svårutrymt större förortsområde med ca 20 000 invånare.
En sådan vindkantring kommer att kräva fullständig utrymning av förortsområdet samt omedelbara insatser av polis och räddningstjänst. Om kemikalierna kommer ut kommer bostadsområdet att behöva sanering av ett mycket stort antal kvalificerade keminsatsteam, fler än vad som finns att uppbringa. Om branden sprider sig till bostadsområdet kan endast delar av bebyggelsen räddas, en stor del av bebyggelsen måste utnyttjas som buffertzon vid brandbekämpningen och därmed offras.

4.3.4 Aktionsstyrning genom beslutsfattande, val av åtgärder och ordergivning

Exempel på hur aktionsstyrning genomförs följer nedan.

"Förbered helikoptersläckningsinsats i syfte att hindra brandens spridning till bebyggelsen. Kontakta helikopterflottiljen och samverka med dem. Insatsberedskap 30 min."
"Förbered evakuering av insatsområdet i syfte att begränsa personskador till ett minimum. Kalla in förstärkning från polis och 1. Stadsskyttebrigaden. Insatsberedskap 60 min."
"Kommunens informationskontor sprider upplysningar till de boende samt sköter kontakten med media."
"Gruppera 4 st keminsatsteam öster om insatsområdet i syfte att omgående medelst indikering inhämta och rapportera utbredning och spridning hos ev. utsläpp. Upprätta saneringsplatser och uppsamlingsplatser för skadade söder om och väster om bostadsområdet med övriga keminsatsteam, beredda assistera med kompletterande indikering och sanering av övriga insatsstyrkor."

4.3.5 Insatsuppföljning

Den faktiska händelseutvecklingen bevakas mot målbilden:
Övervaka avspärrningar och trafikläge, omfördela resurser mellan insatsområdets olika sektorer vid behov. Övervaka brandens utbredningsmönster och väderläget kontinuerligt, förändringar i vindriktning rapporteras omgående till räddningsledningen. Fortsätt med avgränsningsarbetet, fullfölj arbetet med brandgatorna. Därefter skall de gator som inte bedöms stoppa branden breddas. Se till att uttröttad personal avlöses och ges mat, vatten och vila. Skadad personal transporteras till uppsamlingsplatserna för vård.

Den predicerade händelseutvecklingen bevakas mot målbilden:
Händelseutvecklingen avgör hur situationen i insatsområdet skall bedömas över tiden. Om målbilden inte ser ut att kunna nås, måste resurser tillföras/omfördelas så att insatsen som helhet kan nå målet. Den aktuella händelseutvecklingen följs upp och jämförs med den predicerade. Avvikelser identifieras och används för att revidera situationsbeskrivningen. Förbrukade resurser relateras till insatsens verkan och grad av måluppfyllelse. Aktuella resurstillgångar jämförs med det predicerade behovet, och brister åtgärdas omgående genom omfördelning eller tillförsel.

4.3.6 Anpassning av målbild

Bevakningen av händelseutvecklingen återkopplas kontinuerligt till räddningsledningen. Situationsbeskrivningen revideras så snart nya verifierbara observationer rapporteras. Den uppdaterade situationsbeskrivningen används för att rekonstruera, klassificera, identifiera och tolka framtida observationer. Då insikt nås om att målbilden inte kommer att kunna uppnås, vidtar arbetet att revidera målbilden. Resultatet används för att i samverkan med andra berörda insat-

senheter och aktörer upprätta en ny målbild som motsvarar de faktiska förhållandena, med aktuellt resursläge och aktuell situationsbeskrivning.

4.3.7 Sammanfattning av typfallet

Det aktuella fallet är ett typexempel på något som kan kallas ett distribuerat komplext adaptivt system [7], som kan upprätthålla kontrollen över insatsen och insatsområdet genom fyra fundamentala förmågor:

1.Observation av händelser i insatsmiljön,
2. Prediktion av den framtida händelseutvecklingen,
3. Reglering för att nå nya jämviktstillstånd efterhand som insatsmiljön förändras,
4. Anpassning till de varierande förutsättningarna i insatsmiljön.

De parallella skeendena är uppenbara i detta exempel, hypotesen om vindkantringen belyser detta tydligt. Varje delaktivitet i insatsen måste kunna utföras samtidigt och med förmåga att skifta fokus från en aktivitet som verkar stabil för tillfället till en aktivitet som är på väg att gå överstyr. En distribuerad ledningsstruktur med flexibla och delvis överlappande förmågor till effektiv insatsuppföljning är det enda som kan bemästra denna insatstyp.

Det visade sig vara mycket effektivt att på detta sätt bygga en grund för analys och värdering av taktiska högriskinsatser. Det har varit komplicerat och arbetskrävande då strävan ständigt har varit att finna empirisk bevisning i det teoretiska arbetet. Det är möjligt att nyttja resultaten för att:

- Identifiera prestandabegränsande faktorer hos en specifik individ, enhet, system, process eller insats.
- Värdera graden av inflytande hos dessa faktorer på totala taktiska prestanda.
- Ta fram och implementera åtgärder för att förbättra otillräckliga förmågor och bidra till framgång i framtida insatser.
- Ge metodologiskt stöd åt framtida integrerade ledningssystem.
- Utveckla träningsstöd för taktiskt beslutsfattande och resurshantering i taktiska insatser.

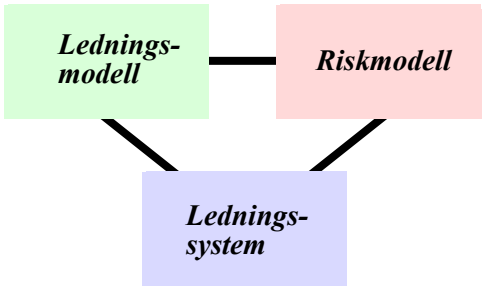
4.4 Principer för ledningssystemutveckling

En princip som tillämpas i de flesta verksamheter är att verksamheten och dess företrädare skall styra ledningssystemutvecklingen. Svårigheten ligger i att kunna göra entydiga ansvarskopplingar mellan verksamhet, som i många fall är decentraliserad och geografiskt spridd, samt den tekniska infrastrukturen, som alltmer blir koncerngemensam och centralstyrd. Verksamhetens behov är att på ett enkelt och effektivt sätt skapa och ha tillgång till den information, som behövs för att producera varor och tjänster samt att samverka med kunder och marknaden. Det är därför nödvändigt att verksamheten preciserar sitt behov och sina krav i termer av den information som behövs och hur denna skall kunna behandlas och kommuniceras [8]. Genom angivande av karakteristiska informationsflöden kan verksamheten ta ansvar för de stödsystem som behövs för att genomföra och utveckla verksamheten. Från den andra utgångspunkten kan de ansvariga för den tekniska infrastrukturen realisera denna från den samlade kravbild som olika verksamhetsföreträdare ställer. Vid konflikter i dessa sammanhang måste vissa bedömningsfrågor avgöras i den högsta företagsledningen. Samarbete i verksamheten förutsätter att de verksamhetsstödjande systemen kan samverka på ett enkelt sätt. En förutsättning för detta är tillgången till en formellt och informellt accepterad begreppsmängd.

För att uppnå effektiv insatsledning är det av avgörande betydelse att en tillräcklig mängd information når den avsedda beslutsfattaren i tid, och att han kan leda utan prestandanedsättande fördröjningar eller friktioner. Information betraktas som en resursklass som skiljer sig från andra klasser av resurser genom att den ej förbrukas eller förlorar sitt värde när den används. I princip kan information användas av ett godtyckligt antal användare och hur många gånger som helst utan att det påverkar värdet av densamma. Emellertid är värdet hos en informationsresurs ej nödvändigtvis beständigt. Information och underrättelser måste vara anpassade för insatsledning och skall därmed uppfylla strikta krav avseende tillförlitlighet, tillgänglighet, relevans, diagnosticitet och komplexitet [13]. Om informationen inte kan uppfylla dessa krav kontinuerligt och parallellt under insatsens planerings-, genomförande- och uppföljningsfaser förlorar den i betydelse för verksamhetens värdeskapande. Därmed minskar informationsresursernas värde. I ett annat fall kan informationsvärdet minska snabbt, när någon med fientlig avsikt kommer åt informationen och har möjlighet att manipulera den. Den ordinarie informationsanvändaren är i de flesta fall ej medveten om att informationen som används är felaktig i något avseende. Snabb tillgång till korrekt information är av strategisk betydelse. En konsekvens av detta är att resursklassen information måste ledas i såväl ett strategiskt, taktiskt som operativt perspektiv. Vidare behöver verksamhetens ledning och personal se information som en resurs med ett värde bestämt av dess potentiella nytta för verksamheten. Detta kräver kompetensutveckling med både bredd och djup för att använda information på ett effektivt och samtidigt säkert sätt. En konsekvens av informationens ökade betydelse är att hoten mot densamma också ökar, vilket leder till att informationssäkerheten måste byggas in från början och följas upp kontinuerligt.

5. Ramverk för preventiv och operativ ledning

Av speciellt intresse i detta sammanhang är att basera arbetet på en ledningsmodell som omfattar tekniker för datainsamling för att upptäcka, identifiera, bedöma och hantera olika typer av hot. Sådana hot skall med stöd av ledningssystemet genom analys kunna kopplas till andra existerande hot så att en sammanhängande hotbild kan byggas upp. Detta skall således kunna ske genom att hitta och bygga upp kedjor av potentiella hotfragment. Andra aspekter av intresse i detta sammanhang är t ex att övervaka olika typer av hot i preventivt syfte. Således, med utgångspunkt från ledningsmodellen bör det vara möjligt att beskriva och utveckla ett ledningssystem med dessa förmågor. Detta är emellertid inte tillräckligt. Systemet måste också kunna utnyttjas för ledning i operativt syfte vilket avser förmåga att på högre systemnivå kunna leda arbetet med att avvärja eller åtminstone begränsa kriser som brutit ut. För att möjliggöra detta kommer det att krävas metoder för samarbete och kommunikation mellan berörda myndigheter. Genomförandet av denna verksamhet kräver en modell för ledning och ett ledningssystem med tekniker för bl a IT-säkerhet till skydd för systemet samt olika beslutstöd.

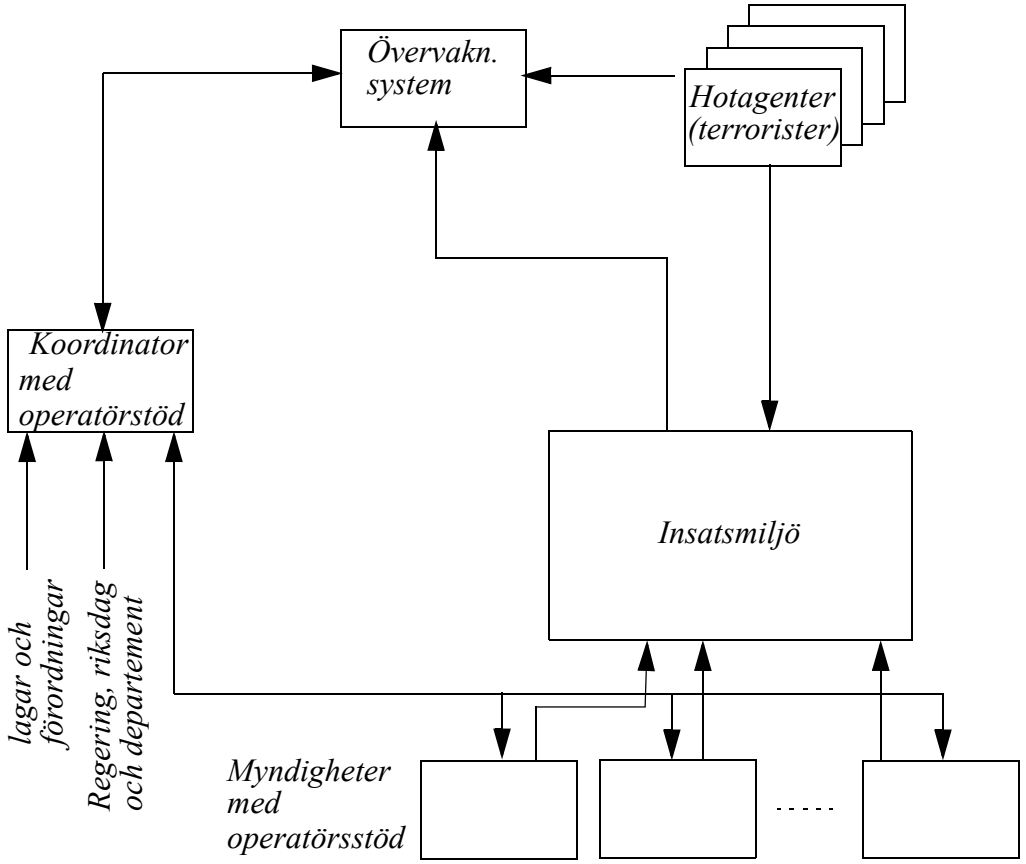


Figur 3. Sambandet mellan ledningsmodell, riskmodell samt ledningssystem.

Till den struktur, som kommer att krävas i ett ledningssystem för krishantering, kommer det också att krävas att en riskmodell hårt kopplas till ledningsmodellen och ledningssystemet, se figur 3. Det huvudsakliga syftet med riskmodellen är att ge stöd till ledningsfunktionen. Detta stöd är främst fokuserat mot olika sårbarheter, risker och för bedömning av hot. Till detta kommer också behovet av att kunna värdera olika former av motåtgärder i olika krissituationer.

5.1 Ledningsmodellen och ledningssystemet

För den ledningsmodell, vars övergripende struktur framgår av figur 4, som diskuteras här är huvudsyftet att den skall kunna realiseras i ett ledningssystem som i sin tur skall kunna användas vid både preventiv och operativ ledning. Av speciell vikt är härvid att hänsyn skall tas till att det föreligger ett antal olika grundläggande krav som måste vara uppfyllda. Till dessa krav kan man räkna samverkan med andra aktörer men även allmänheten skall kunna informeras via ledningssystemet. Emellertid kommer det också att ställas krav på en koordineringsfunktion med syftet att leda verksamheten. En sådan funktion kan givetvis bestå av en grupp av personer, t ex från länsstyrelse, kommun, räddningstjänst samt externa medlemmar som kan besitta expertkunskap nödvändig i ett givet läge. För att leda verksamheten i syfte att föra den pågående krisen till ett slut måste man kunna övervaka den aktuella insatsmiljön som dels kan utgöra centrum för en pågående kris eller bestå av ett eller flera skyddsvärda objekt. Av denna anledning behövs instrument för insamling av nödvändiga data. Dessa kan vara både sensorer och/eller meddelanden i form av både text och tal. För att göra ett system av detta slag till en fungerande enhet krävs också att man kan överföra information mellan de olika medverkande parterna samt att dessa kan kommunicera och att beslut kan överföras på ett tillfredställande och effektivt sätt. Av denna anledning kommer en nätverkslösning, som kan utgöra en del i den nätverksbaserade krishanteringen (NBK), att krävas. Med NBK avses en nätverksstruktur som kan användas för t ex krishantering och skydd av samhälle och individ.

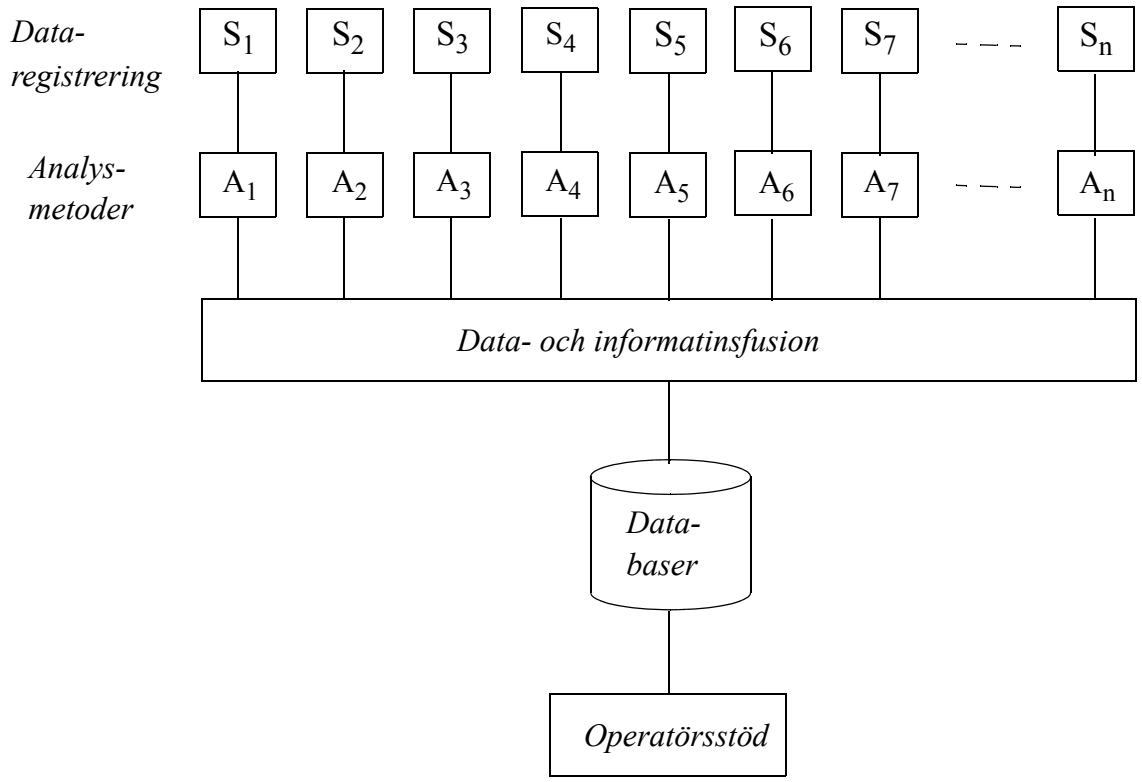


Figur 4. Den övergripande strukturen i ledningsmodellen.

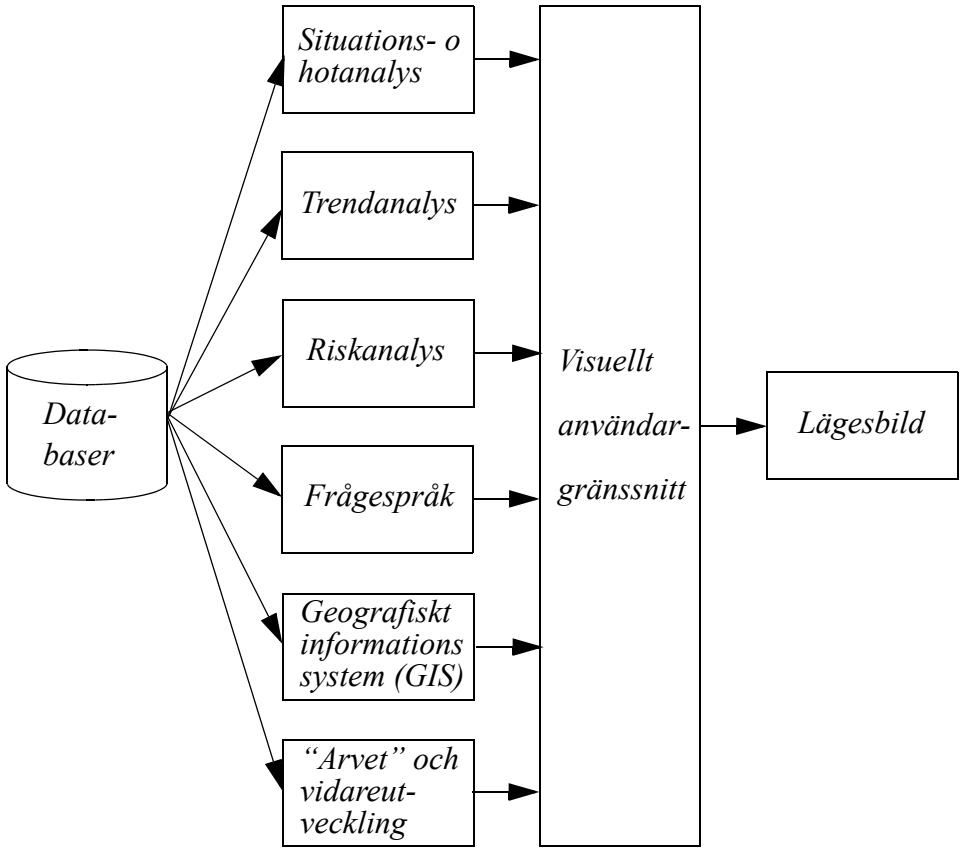
Det kommer emellertid inte att vara tillräckligt att övervaka enbart den miljö som är utsatt för den aktuella krisen utan det måste också, oftast i ett preventivt skede, vara möjligt att övervaka förekommande hotagenter. De preventiva aktiviter som kommer att bli nödvändiga kommer tvivels utan att vara omfattande och kräva speciella forskningsinsatser.

En funktionalitet i det slutliga ledningssystemet, som inte får förglömmas, är den återkoppling till insatsområdet som måste vara möjlig. I samband med detta kan man observera att de olika medverkande myndigheterna själva normalt har sina egna kanaler för detta ändamål in mot insatsområdet, t ex har såväl polis som räddningstjänst sina normala ansvarsområden och utrustning för att släcka bränder respektive bekämpning av brottslighet. Genom en stärkt förmåga till övervakning blir det möjligt att med denna ledningsmodell stödja de enskilda myndigheternas förmågor eftersom koordineringsfunktionen kommer att kunna stödja optimerade insatser så att olika kriser kan bekämpas effektivare.

I figur 5 framgår hur modellen till ett delsystem för övervakning kan tänkas vara uppbyggd. Principen är baserad på att i insatsmiljön kommer olika platser och skyddsvärda objekt att observeras av utsända observatörer eller av speciellt utplacerade sensorer. De data som registreras på dessa sätt svarar mot dataregisteringsenheterna i figur 5. Data som registrerats måste genomgå någon form av dataanalys, t ex bilder måste analyseras med avseende på sitt innehåll, text- och talmeddelanden måste på motsvarande vis analyseras för att tillgängliggöra informationsinnehållet. I vissa fall måste viss information också fusioneras. Den på detta sätt insamlade informationen skall slutligen lagras på ett adekvat sätt i en lämplig databas för att till sist bli tillgänglig för användaren i något lämpligt beslutsstöd.



Figur 5. Strukturen i övervakningssystemet i ledningsmodellen.



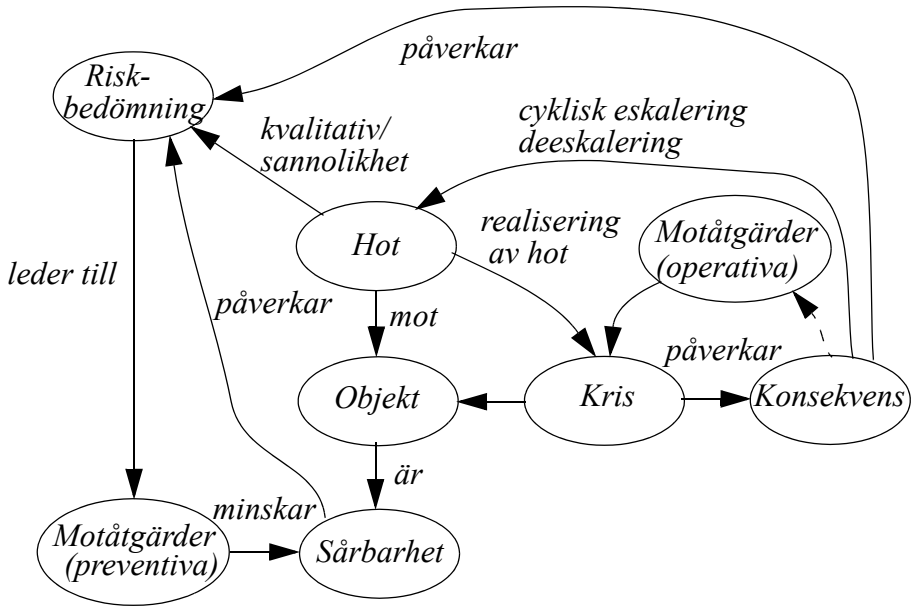
Figur 6. Strukturen i ledningsmodellens operatörsstöd med exempel på olika beslutsstöd.

Strukturen för ledningsmodellens operatörsstöd framgår av figur 6. Syftet med denna del av ledningsmodellen är väsentligen att ge ett adekvat stöd för beslutsfattandet samt för kommunikation mellan olika användarkategorier. I exemplet i figuren återfinns ett antal olika beslutstöd som kommer att vara tillgängliga för en viss användare. Dessa olika beslutstöd kan variera med avseende på vilka behov som olika användare kan komma att ha. Således behövs det en metodik för att knyta olika beslutstöd till det visuella användargränsnittet (VUI), dvs strukturen skall vara modulär. Knutet till detta användargränssnitt kommer det också att finnas en lägesbild som svarar mot det aktuella läget i den uppkomna krissituationen. Lägesbilden kommer inte med nödvändighet att vara gemensam för alla medverkande parter men måste däremot vara allt igenom konsistent eftersom den återspeglar en realitet på vars grund olika beslut skall fattas. Till systemet kommer det också att bli nödvändigt att knyta ett antal speciella databaser mot vilka de olika beslutsstöden skall kunna arbeta. Vissa av dessa databaser utgör mottagare av data från övervakningssystemet i figur 5.

En central del i detta delsystem är att det måste kunna hantera *arvet*, dvs redan existerande stödsystem. Vid sidan av detta måste det också bli möjligt att analysera informationen mot bakgrund av andra kunskaper samt att kunna hantera konflikter avseende motstridiga rapporter, etc.

5.2 Riskmodellen

Ett ledningssystem för preventiv och operativ krishantering måste baseras på en riskmodell, dvs en modell för att beskriva skyddsvärda objekt, vilka hot de är utsatta för, vilken risk dessa hot utgör samt vilka konsekvenser realisering av ett hot skulle innebära. Modellen måste även ta hänsyn till hur förebyggande åtgärder påverkar risken för att ett hot realiseras samt hur åtgärder minskar konsekvenserna av ett realiserat hot. Riskmodellen som beskrivs nedan skall ses som ett initialt steg mot att utveckla en sådan modell, men som behöver kompletteras och vidareutvecklas, se figur 7.



Figur 7. Riskmodellen med dess preventiva och operativa delar.

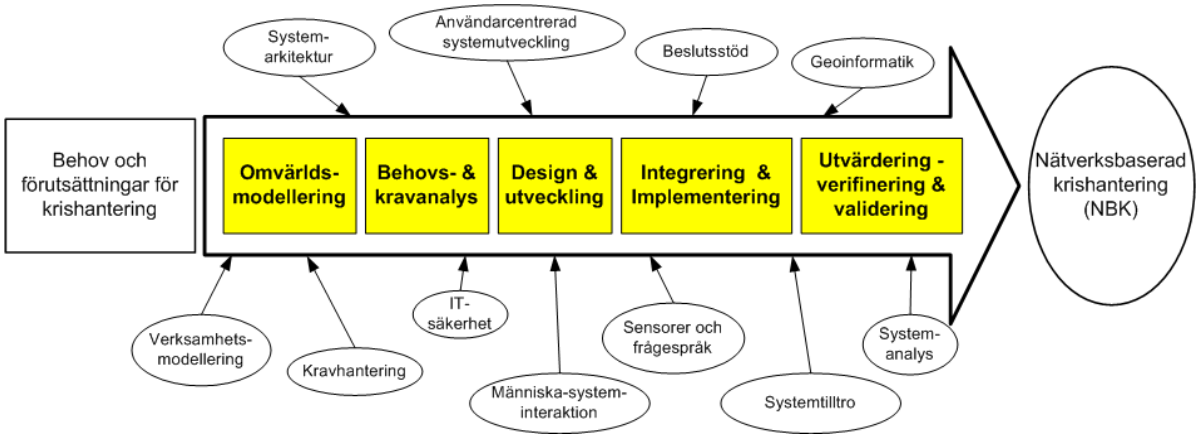
Mot ett objekt riktas en hotbild. För objekt och hot görs en riskbedömning baserat på objektets sårbarhet, sannolikhet för att ett hot realiseras samt vilka konsekvenser resultatet av en realisering av ett hot får. För att minska ett objekts sårbarhet genomförs preventiva motåtgärder (pre-

ventiv krishantering). Dessa åtgärder minskar objektets sårbarhet, men kan också minska den påverkan en realisering av ett hot skulle få.

Konsekvenserna av en realisering av ett hot inverkar såväl på objektet i sig, som dess omgivning. Det vill säga påverkan av ett objekt kan i sig utgöra ett hot mot andra objekt. Detta innebär att det kan uppstå kedjereaktioner av hot som realiseras, vars konsekvenser utgör realiseringen av nya hot mot andra objekt o s v. Denna kedjereaktion kan såväl eskalera som avta. För att minska påverkan och därmed konsekvenserna samt förhindra eskalerande kedjereaktioner
vidtas operativa motåtgärder. Lärdomar av konsekvenser, av realiserade alternativt simulerade realiseringar av hot, används som underlag för att göra bättre riskbedömningar framöver. En väl genomarbetad riskmodell kan används som grund för att simulera hot, dess konsekvenser och möjliga kedjereaktioner. Möjligheten att simulera ger ett bättre beslutsunderlag för riskbedömningar och utveckling av motåtgärder, såväl för preventiv som operativ krishantering.

6. Centrala forskningsområden

Ett stort antal olika forskningsområden berörs av problematiken kring utvecklingen av ett ledningssystem för krishantering, vilket redan har påpekats. I detta kapitel kommer flera av dessa områden att diskuteras i anslutning till de behov som kommer att uppstå i arbetet med att utveckla ett sådant system. I figur 8 framgår sambandet mellan de olika faserna i systemutveckingsprocessen och de aktuella forskningsområden.



Figur 8. Översikt över sambandet mellan olika aktuella forskningsområden och systemutvecklings processen.

6.1 Systemarkitektur

Alla system har en arkitektur, oavsett om den är formaliserad och medvetandegjord eller ej. Att tydliggöra och använda en arkitektur för att beskriva befintliga och tänkta system skapar förutsättningar för helhetssyn, flexibilitet, återanvändning och samverkan [99]. Detta gäller såväl vid utveckling av nya som vid modifiering av befintliga system. Att besera utveckingen av system på en arkitektur har i stor utsträckning använts vid konstruktion av hårdvara och mjuk-vara [100], [101]. Att nyttja en arkitekturansats gör det möjligt att återanvända befintliga sys-tem för att, eventuellt i kombination med nyutvecklade delar, åstadkomma helt nya system [102]. På senare tid har även möjligheten att använda arkitekturansats anammats för att erhålla liknande positiva effekter på komplexa system, som förutom informationsteknik, består av organisationsstruktur, processer och kompetens i form av personal [103], [104]. I samband med att den Amerikanska Försvarsmakten beslutade sig för att satsa på ett nätverksbaserat försvar, tog intresset för att använda en arkitekturansats vid verksamhetsutveckling fart på allvar [105]. Målet med att använda en arkitekturansats på verksamhetsnivå var att erhålla en organisation som snabbt och flexibelt kunde anpassas till de uppgifter som den ställdes inför.

Fundamentalt för nätverksbaserade organisationer är principen ”system-av-system” och nyttjandet av modern informationsteknologi. För att erhålla de positiva effekterna så som anpassningsförmåga, effektivt resursutnyttjade etc. som nätverksbaserade organisationer möjliggör ställs stora krav på förmågan att effektivt och kontinuerligt kunna utveckla olika typer av system. Dessa system måste också enkelt kunna integreras och fungera i den redan befintliga organisationen, det vill säga samverka med redan befintliga system. Detta ställer i sin tur krav på en förståelse för arkitektur och möjligheten att nyttja den som grundpelare för den kontinuerliga processen att skapa och avveckla system. Det är arkitekturen som måste utgöra grunden för samsynen när det gäller såväl systemutveckling som att säkerställa att systemen fungerar ihop. Det innebär att de system som skall ingå i organisationen måste konstrueras så att de är

kompatibla och att arkitekturramverket bör innehålla stöd för utveckling av system i enlighet med arkitekturen.

Många arkitekturer beskrivs idag som tjänstebaserade. Det finns dock ingen helt entydig definition av vad begreppet tjänst står för när det gäller arkitekturer, men oftast avses funktionalitet eller kapacitet. Tjänstebegreppet har blivit ett koncept för att beskriva vad ett system producerar utan att beskriva hur det åstadkoms. På så vis kan komplexitet och realisering döljas och fokus hamnar på systemets funktionalitet istället för dess struktur. Utifrån tjänstedefinitioner kan samverkan mellan system erhållas baserat på de prestationer de tillhandahåller. Detta medför att systems samverkan kan reduceras till ett beroende mellan de tjänster som de tillhandahåller och inte till systemen i sig. Detta skapar möjlighet till evolutionär utveckling, eftersom ett system kan förändras och bytas ut med en begränsad och förutsägbar inverkan på omgivande system. Tjänstekonceptet ger också möjlighet att återanvända befintliga tjänster för att utveckla nya tjänster. Detta genom att befintliga tjänster kombineras, eventuellt med inslag av nyutvecklade tjänster.
I likhet med den amerikanska och flertalet andra försvarsmakter, står den Svenska Försvarsmakten inför en omfattande omstrukturering och genomgripande förändring mot en nätverkscentrerad organisation, det Nätverksbaserade försvaret (NBF). Denna förändring skall resultera i en omställning från ett invasionsförsvar till ett flexibelt och kostnadseffektivt insatsförsvar med förbättrad styrning, kvalitet och spårbarhet i verksamhets- och resursutvecklingen. Men för att kunna realisera visionen av NBF i enlighet med uppsatta krav krävs en för hela Försvarsmakten gemensam och stabil arkitektur. Försvarsmakten driver utvecklingen av en sådan arkitektur, kallad *Försvarsmaktens arkitektur* (FMA) [106].

6.1.1 Försvarsmaktens arkitektur (FMA)

FMA är tänkt att utgöra ett verktyg för Försvarsmakten för att med korta ledtider kunna realisera och integrera teknik, information och kompetens i form av personal till fungerande system. Dessa system ska vidare kunna integreras till och samverka med andra system.
Ambitionen är att FMA skall utgöra en för Försvarsmakten övergripande och sammanhållen utvecklingsprocess samt ett gemensamt sätt att beskriva verksamhet och resurser. Till skillnad mot flertalet andra arkitekturansatser syftar FMA till att omfatta alla typer av system, allt från ren verksamhet (kompetens i form av människor och organisatorisk struktur och processer), till rent tekniska och mer komplexa system bestående av såväl verksamhetsdelar som teknik.

I FMA betraktas, beskrivs och hanteras Försvarsmakten som ett *system*. Detta system består av ett flertal andra system, som i sin tur består av ett flertal system. Det vill säga, FMA bygger på principerna för *system-av-system*. I FMA används sex perspektiv för att betrakta och beskriva system. Varje perspektiv speglar en viss del av ett system. Dessa perspektiv är: (1) systemperspektiv, (2) verksamhetsperspektiv, (3) organisationsperspektiv, (4) personalperspektiv, (5) informationsperspektiv och (6) teknikperspektiv. Systemperspektivet beskriver hur olika system förhåller sig till varandra genom att se system som system-av-system. Verksamhetsperspektivet beskriver de processer som tillsammans har till syfte att tillgodose en konsument med verksamhetens prestation. Organisationsperspektivet beskriver den organisatoriska strukturen, inklusive beslutsvägar. Personalperspektivet beskriver relationerna mellan roller, kompetenser och behörigheter. Informationsperspektivet beskriver vilka olika typer av information som behövs i samband med att en viss tjänst ska genomföras. Teknikperspektivet beskriver olika typer av teknologier, det vill säga kunskaper, som behövs inom organisationen.

FMA innehåller även en uppsättning dokument kallade *Generella design principer* som används för att dokumentera och formalisera kunskap gällande systemutveckling. Ett doku-

ment för detta upprättas inom ett område när det bedöms rationellt att skapa samordning och återbruk av kunskap och erfarenheter samt för att styra hur olika standarder och regelverk skall tillämpas.

Ett av de mest centrala koncepten i FMA är tjänstebegreppet [107]. I FMA är en tjänst *en abstraktion av hur en producent kan åstadkomma nytta för en konsument* utan att beskriva hur detta genomförs. Nytta åstadkoms genom att producenten levererar en *prestation* och prestationen ger en *effekt* hos/för konsumenten. Enligt FMA skall tjänster beskrivas oberoende av hur de implementeras. Det vill säga, en tjänstbeskrivning innefattar inte hur producenten producerar nytta, utan beskriver enbart hur konsumenten gör för att få tillgång till denna och vilka prestationer som produceras. En tjänst definieras alltså oberoende av om den implementeras manuellt, tekniskt eller genom en kombination av dessa. Flera producenter kan tillhandahålla en och samma tjänst men implementera dessa på olika sätt. Enligt FMA är också en tjänst *en standard som beskriver hur en konsument i samverkan med en producent kan få denne att leverera en prestation*.

Tjänster implementeras i *systemelement*, som var och ett tillhandahåller en eller flera tjänster. Det finns synkrona tjänster, där konsumenterna direkt får en effekt av tjänsten. Asynkrona tjänster beställs och konsumenten erhåller verkan fortlöpande tills dess att tjänsten avbeställs. Enligt FMA har en tjänst *egenskaper*, vilka skall vara de samma oberoende av realisering av en viss tjänst. Det är istället värden på dessa egenskaper som varierar beroende på realisering av tjänsten. Dessa värden ligger också till grund för att konsumenten kan identifiera just den tjänst som bäst motsvarar behovet utan att förstå hur den är realiserad. Enligt FMA skall tjänster definieras utifrån konsumentens synvinkel. I definitionen anges hur tjänsten skall användas och vad som presteras, men inte något implementeringsspecifikt. Dock skall den prestation som tjänsten tillhandahålla vara väl preciserad. Vidare skall tjänsten vara till nytta för många konsumenter som kan söka och välja tjänster baserat på dess egenskaper. En bra tjänst skall dessutom kunna kombineras med andra tjänster för att erhålla nya tjänster.

Utvecklingen av FMA har kommit relativt långt med en välutvecklad systemsyn och ett välutvecklat tjänstebegrepp. Vidare har ett flertal standarder lyfts in för att säkerställa framtida kompabilitet med andra ansatser. Det finns dock mycket arbete kvar. FMA behöver både testas ytterligare och anpassas till andra verksamheters förutsättningar och behov.

6.2 Systemutveckling

Systemutveckling är en process vars syfte är att skapa helt nya och/eller förändra befintliga system. Generellt kan dessa system vara rent teknikbaserade, verksamhetsbaserade eller en blandning av dessa. Ofta ses dock begreppet systemet som liktydigt med det rent tekniska systemet, vilket många gånger är en olämplig generalisering. Det är vid utveckling av större rent tekniska informationssystem sedan länge ett välkänt fenomen att om det tekniska systemet skall fungera väl och motsvara de behov som finns i den verksamhet som avses stödjas så måste det tekniska systemet harmonieras med de övriga delar i den verksamhet det är avsett att stödja. Det vill säga, teknikstöd, individernas kompetens, organisationens struktur och verksamhetens genomförande hänger intimt samman, där förändringar i en eller flera av dessa delar påverkar de övriga och systemets möjlighet att leva upp till ställda förväntningar. Den komplexa verksamhet som utveckling av system av denna typ innebär kräver kompetens från vitt skilda kunskapsområden, såväl tekniskt som beteendevetenskapligt orienterade. Komplexiteten i att utveckla *rätt system*, till *rätt pris* och i *rätt tid* har sedan länge uppmärksammats, men dessa har ännu inte lösts full ut[18], [19]. En grundläggande orsak till dessa svårigheter är avsaknaden av stöd för att skapa en förståelse för den omgivning (kontext) system skall fung-

era i, samt att hantera behov som finns i kontexten, överföra dessa till krav samt att realisera dessa krav i konkreta system [20], [22].

Inom systemutvecklingsområdet finns ett stort antal olika ansatser, allt från etnologiska ansatser där användningsmiljön särskådas till tekniska objektorienterade varianter [21]. Det är dock få av dessa ansatser som på ett tillfredställande sätt täcker samtliga delar av systemutvecklingsprocessen. En stor utmaning ligger nu i att lyckas integrera metodik, tekniker och kunskap från olika ansatser för att skapa mer heltäckande systemutvecklingsprocesser.

Det finns många olika sätt att beskriva och namnge aktiviteterna som ingår eller bör ingå i systemutveckling. En generell och generisk uppdelning av systemutvecklingsprocessen är i aktiviteterna *Modellering av kontext*, *Kravhantering*, *Design, Implementering* och *Utvärdering*. I modelleringen av kontexten skapas beskrivningar (modeller) av den omgivning som systemet skall fungera i, med syfte att erhålla en förståelse av denna. Dessa modeller kan senare användas som underlag för diskussioner mellan utvecklare, beställare och användare. På så sätt kan viktiga egenskaper, målsättningar, visioner och eventuella missförstånd mellan inblandade aktörer upptäckas och redas ut tidigt.

I kravhanteringsarbetet skall, ifrån bland annat diskussionerna kring den kontextuella modellen, utsagor identifieras som direkt eller indirekt innehåller information om krav på systemet. Syftet med kravhaneringen är att identifiera, beskriva och hantera de krav som ställs på systemet [24]. Brister i kravhanteringen anses vara den största orsak till misslyckanden i systemutveckling, där studier visat att ca 80% av defekterna i informationssystemen har sitt ursprung i specificeringen av kraven [23]. Samtidig är det välkänt att kostnaderna för att åtgärda misstag som görs i de tidiga faserna är väsentligt större än de som begås de senare [24]. Resultatet av kravhanteringen är någon form av kravspecifikation. Traditionellt så utgjordes denna kravspecifikation av rent textuella beskrivningar av krav, en mer modern syn är dock att dessa kan kompletteras med exempelvis prototyper, användningsfallsdiagram och scenariobeskrivningar.

I designen skapas lösningar som motsvarar de krav som identifierats i föregående steg. Viktigt att komma ihåg är att design kan exempelvis bestå av en designspecifikation av ett informationssystem, en beskrivning av en ny verksamhetsprocess, utbildning av personalen och/eller ny organisationsstruktur. Under implementeringen realiseras designen i faktiska lösningar. Ett datorsystem kan köpas in och integreras i verksamheten, en utbildning av personalen kan genomföras och så vidare. Det finns två grundläggande typer av utvärderingar av system, verifiering och validering. Verifiering innebär att systemet utvärderas mot de krav som ställts upp och som det avser uppfylla. Validering innebär att systemet jämförs med hur väl det motsvarar de behov som finns i verksamheten.

Varje aktivitet i denna grova beskrivning av systemutveckling är i många fall ett eget systemutvecklingsprojekt, där utvärderingar av delresultat som exempelvis kravspecifikationer kräver någon form av kvalitetssäkring. Vidare är systemutvecklingsprocessen i modern form inte något rent sekventiellt förlopp, där en aktivitet påbörjas när föregående avslutats. Tvärtom påtalas behovet av processer som är evolutionära, iterativa så väl i aktiviteterna som över hela processen och där inkrementella delar av system utvecklas.

6.2.1 Principer och ansatser

Några principer och ansatser som lyfts fram under senare tid är principer om spårbarhet, prioritering, iterativa, användbarhet, ISO-standarder samt ansatser som användningsfallsdrivna, användarcentrering och arkitekturcentrerad.

Spårbarhet
Att systemutvecklingsprocessen tillhandahåller spårbarhet mellan utsagor, behov, krav och design, till funktioner och egenskaper som implementeras är av största vikt [26]. Spårbarheten gör det möjligt att implementera det som kommer verksamheten till nytta, arbetet kan fokuseras på rätt ”saker”. Vidare ger spårbarhet pedagogiska vinster, när systemfunktionalitet skall motiveras och det skall visas hur behov i verksamheten är tänkta att mötas i realiseringen av ett system.

Prioritering
Allt som kan tänkas önskas av ett system varken kan eller skall implementeras. Enlig Paretoeffekten så motsvarar 20% av det som kan implementeras 80% av nyttan som erhålls. Att lägga resurser på att implementera funktionalitet och egenskaper som enbart ger begränsad nytta är både ett sätt att slösa bort resurser och att i många fall skapa en onödig komplexitet och därmed svåranvända lösningar[25]. Detta medför att det är nödvändigt att prioritera vad som skall implementeras eller inte, samt att välja vad som är viktigast och i vilken ordning funktionaliteten bör implementeras.

Iteration
Systemutveckling kan ske *sekventiellt* eller *iterativt*. Traditionell systemutveckling har ofta bedrivits sekventiellt, där varje aktivitet utförts avgränsat och endast levererat information som utgångspunkt för nästa aktivitet [20]. En rent sekventiell ansats är dock sällan särskilt lyckosam då förutsättningar och systemomgivningar sällan är stabila samt att chansen att lyckas fånga en helt korrekt kravbild i ett första försök sällan lyckas. Iterativ systemutveckling innebär att de olika faserna går i varandra och upprepas om nödvändigt [27],[28]. Iteration kan ske såväl i som över enskilda aktiviteter eller över hela utvecklingsprocessen. Med fördel tas synpunkter in emellan iterationerna genom utvärderingar med användare. De flesta modernare systemutvecklingsansatser har mer eller mindre inslag av iteration. Fördelar med en iterativ ansats är att genom att ta små steg framåt och utveckla systemet successivt gör det lättare och mindre kostsamt att göra om något som är felaktigt.

Användbarhet
Under senare år har vikten av att fokusera utvecklingsarbetet på att skapa system som har en hög grad av användbarhet betonats alltmer. Ett traditionellt sätt att se på begreppet användbarhet är att relatera till; hur enkelt ett system är att lära sig, hur effektivt ett system är att använda, hur enkelt ett system är att komma igång med, hur tilltalande ett system är och hur många fel användare begår vid användning av ett system [29]. Denna syn på användbarhet relaterar i huvudsak till interaktionen mellan användaren och systemets gränssnitt och på vilket sätt olika funktioner utförs. En mer modern och vidare syn på begreppet användbarhet är att det relaterar till den effekt och upplevda nyttan som användare upplever av ett system. Det innebär att även den funktionalitet som ett system ger anses som viktig att beakta. En iterativ systemutvecklingsprocess, användarmedverkan och att tidigt i utvecklingen använda prototyper ökar användbarheten av det resulterande systemet.

Användarcentrerad systemutveckling
Användarcentrerad systemutveckling är mer ett förhållningssätt till systemutveckling än en ansats, vilket innefattar olika angreppssätt, principer, metoder och tekniker. Inslag av både sekventiell och iterativ systemutveckling finns, även om iteration oftast betonas. I användarcentrerad systemutveckling uppmanas användare att aktivt medverka i arbetet eftersom de har kunskapen om sin domän, sina behov och restriktioner [30]. Vanligtvis sker arbetet i projektgrupper bestående av systemutvecklare, användarrepresentanter, och övriga intressenter och domänexperter av relevans för systemet under utveckling.

Användarcentrerad systemutveckling har en rad fördelar. Systemet bygger på användarnas verkliga behov utan att alltför tidigt binda upp sig vid tekniska lösningar, vilket gör att nyttan av systemet ökar. En högre acceptansgrad för systemet nås än om det hade utvecklats utan användarnas medverkan. Dessutom blir underhållskostnaderna lägre då kostsamma omarbetningar kan undvikas.

Det finns dock flera svårigheter med att tillämpa användarcentrerad systemutveckling. Till dessa hör rekrytering av representativa slutanvändare och att behålla deras motivation genom hela utvecklingsprocessen. Många systemutvecklare saknar också ofta språket att på ett enkelt och problemfritt sätt kunna kommunicera med användarna. Användarcentrerad systemutveckling tenderar även att kortsiktigt vara tids- och resurskrävande.

Användningsfallsdriven
Användningsfallsdriven systemutveckling bedrivs utifrån *användningsfall*, vilket är en beskrivning av hur användare önskar utföra uppgifter med systemet[31]. Det vill säga en beskrivning av en serie interaktioner mellan användare och system. Användningsfall härleds bland annat ur verksamhetsmodeller. Identifierade användningsfall sammanställs sedan i en *användningsfallsmodell* som beskriver systemets sammanlagda funktionalitet. I användningsfallsdriven systemutveckling drivs därmed processen framåt med utgångspunkt från användningsfallen. Användningsfallen utvecklas med fördel i samverkan mellan utvecklare och användare. Fördelar med användningsfallsdriven systemutveckling är att den ger en ökad förståelse för hur användare vill och har behov av att utnyttja systemet. Användningsfallen baseras på en enkel notation som inte innebär några större trösklar för användarna att lära sig, vilket ger ett gemensamt språk som underlättar kommunikation mellan systemutvecklare och användare. Användningsfallen stödjer grafisk och textuell modellering av systemet under utveckling, som kan användas för utvärdering och dokumentation.

Arkitekturcentrerad systemutveckling
Med *arkitekturcentrerad* systemutveckling avses en utvecklingsprocess som utgår ifrån systemets arkitektur, dess uppbyggnad utifrån ett helhetsperspektiv med avseende både på dess dynamiska och statiska egenskaper [32]. Att utnyttja det för utveckling av hård- respektive mjukvara är relativt vanligt, Det är däremot mindre vanligt att omfatta organisation, verksamhet och kompetens, även om detta nu verkar att öka kraftigt. En arkitektur för system skall konstrueras dels med utgångspunkt i de behov som finns i verksamheten, och dels med utgångspunkt i den teknik som är tänkt att användas. Arkitekturen utgör en översikt över designen, men innehåller inte detaljbeskrivningar av enskilda komponenter och funktioner. Arkitekturen innehåller systemet och dess övergripande struktur och form.

ISO standarder för systemutveckling

Det finns idag ett antal standarder framtagna för informationssystem, systemutveckling och användarcentrerad systemutveckling. Några som är av speciellt intresse är ISO 15288, ISO 13407 samt ISO 18529.

- *ISO 15288* är en standard för att hantera systems hela livscykel, från idé till dess avveckling [33]. En livscykel består av fyra processer indelade i ett antal subprocesser varav den *tekniska processen* omfattar systemutvecklingsprocessen.
- *ISO 13407* är en standard framtagen för användarcentrerad systemutveckling. Den är avsedd att vara en utgångspunkt vid genomförandet av användarcentrerade systemutvecklingsprojekt som kan modifieras utifrån projektets speciella kontext och förutsättningar [34]. ISO 13407 ser användarcentrerad systemutveckling som en process integrerad med den övergripande systemutvecklingsprocessen. Standarden betonar planering av såväl användarmedverkan som övrig utveckling som en fundamental förutsättning för ett projekts lyckade genomförande. ISO 13407 bygger på principer av *aktiv användarmedverkan och förståelse av användarens krav*, *en riktig allokering av resurser mellan människa och teknik*, *iteration av designlösningar* och ett *multidisciplinärt angreppssätt till systemutveckling*.
- ISO 18529 är en standard för användarcentrerad systemutveckling specifikt inriktad mot människa-systeminteraktion d v s hur användaren interagerar med systemet via ett gränssnitt [35]. ISO 18529 är en utveckling av ISO 13407

Rational Unified Process

Rational Unified Process (RUP) är en definierad systemutvecklingsprocess för mjukvaruintensiva system [32]. RUP är ursprungligen framtaget för utveckling av programvara, med starka rötter i objektorienterad utveckling. Detta har dock blivit allt mer spritt och en utveckling av grundkoncepten pågår kontinuerligt. RUP täcker hela *utvecklingscykeln* av ett system och är organiserad i två dimensioner. Den första dimensionen beskriver hur projektet genomförs över tiden. Projekt är enligt denna dimension en utvecklingscykel uppdelat på fyra *faser* som var och en är indelad i *iterationer*. Den andra dimension är uppdelad i de *discipliner* (arbetsuppgifter) som skall genomförs under projektet. Varje disciplin beskrivs som en mängd *aktiviteter* sammanlänkade i ett *arbetsflöde*. RUP är en kommersiell systemutvecklingsmetod som utan vidareutveckling inte på ett adekvat sätt täcker utvecklingen av verksamhets- och kompetensdelarna av system. Dessutom saknar det stöd för användarmedverkan.

Unified Modeling Language

Unified Modeling Language (UML) är ett standardiserat modelleringsspråk för visualisering, specificering, konstruktion och dokumentering av mjukvaruintensiva system [36]. Språket används av bland annat RUP och inkluderar en rad notationer och diagram för att beskriva såväl dynamik som statiska delar av system och dess omgivning. UML innehåller även möjligheter att skapa egna tillägg till notationerna vilket möjliggör anpassning av språkets syntax och semantik.

Verksamhetsutvecklingsmetoden för Ledningssystem
Vid Institutionen för systemutveckling och IT-säkerhet vid FOI har sedan ett flertal år ett antal systemutvecklingsprojekt drivits. Erfarenheter har samlats och finns nu beskrivna i form av en metodhandbok. Denna metod kallas *Verksamhetsutvecklingsmetoden för Ledningssystem* (VUM-LS) och bygger på bland annat på de principer och ansatser beskrivna ovan. VUM-LS bygger i grunden på RUP men är starkt influerat av principer och angreppssätt i användarcentrerad systemutveckling. Syftet med utvecklingen av metoden har varit att åstadkomma en mer heltäckande systemutvecklingsprocess, som även inbegriper utveckling av systemdelarna personal, organisation och verksamhet. I VUM-LS används en användningsfallsdriven, iterativ och arkitekturcentrerad ansats. UML används för att visualisera och stödja dokumentation. Dessutom följs standarderna ISO 15288, ISO 13407 och ISO 18529 på en övergripande nivå för att säkerhetsställa ett hänsynsstagande till alla ingående delar i processen. ISO standarder används dessutom som utgångspunkt för att täcka det praktiska genomförandet av VUM-LS som faller utanför de direkta arbetsflödena, t ex förstudiearbete och riskanalys.

6.3 Sensorer och andra datakällor

Frågan om vilka typer av datakällor som skall utnyttjas utgör en av grundbultarna i ett ledningsystem. Till detta kommer att aktuella datakällor kan vara av många olika typer. I de fall datakällorna utgörs av sensorer leder detta till speciella problem eftersom sensorer genererar data av olika slag och med olika säkerhet. Av denna anledning måste data kunna fusioneras för att få mer tillförlitlig information, uppnå högre mått av kunskap med vars hjälp man kan dra relevanta slutsatser och fatta korrekta beslut.

6.3.1 Sensorer

Det existerar många typer av sensorer, som levererar utdata av olika typ och kvalitet. Bildalstrande sensorer, såsom videokameror, IR-kameror och olika typer av radarsensorer, är en av de mest generiska typerna av sensorer, och ger rik utdata i form av bilder, som dock kan vara svårtolkade av ett system som använder sensorerna.

Inom forskningsområdena bildbehandling och datorseende utvecklas algoritmer för att extrahera relevant information ur bilder. Vilken information som är relevant bestäms av tillämpningsområdet. Det kan till exempel innebära att detektera, följa, känna igen eller klassificera objekt i bilderna. Extraktion av information är nödvändigt, både för att kunna representera bildinformationen på ett format som är användbart för ett autonomt system, och för att minska mängden data som ska lagras eller överföras till andra noder i ett nätverk – en digital bild kräver ett mycket stort utrymme. En introduktion till ämnet bildbehandling ges i [37].

Ett relativt väl utforskat område är detektion [38], klassificering och följning [39] av stela objekt i bildsekvenser. Stela objekt karakteriseras av att de olika delarna på objektet hela tiden har samma inbördes position. Exempel på sådana objekt är hus och bilar. Anledningen att detta problem är väldokumenterat är att det är relativt enkelt att göra datormodeller av stela objekt, eftersom deras position och orientering kan beskrivas med några få parametrar. För att passa ihop modellen med mönster i bilden eller bildsekvensen kan man variera parametrarna. Detta kan formuleras som ett optimeringsproblem eller som ett följningsproblem där parametrarna upprepade gånger ändras.

Det är också möjligt att med hjälp av statistiska metoder avgöra vilken typ av miljö som sensorn observerar. Exempelvis bildar träd andra slags mönster i bilden än inslag i en stadsmiljö. Bildstatistik diskuteras exempelvis i [37].

En allt vanligare tillämpning är detektion [40], följning och igenkänning av människor i bilder och bildsekvenser. Naturligtvis är det av central betydelse i system för övervakning och krishantering att kunna observera människor på ett autonomt sätt. Detta är dock ett mycket utmanande problem, av flera anledningar. Först och främst kommer en modell av en människa, hur den än ser ut, att ha många fler parametrar än en modell av till exempel en bil. Den snabba utvecklingen av beräkningskraft gör det dock möjligt att utföra mer och mer krävande beräkningar, vilket ju minskar omfattningen av detta problem. Ett mer grundläggande utmaning är att människors utseende och rörelsemönster skiljer sig mycket mellan individer. Det gör att det är svårt att formulera en modell av hur människor *i allmänhet* ser ut och rör sig som man kan använda för detektion och följning. En ytterligare svårighet introduceras om många människor, folkmassor, rör sig i bilden.

Sammanfattningsvis finns relativt väl fungerande metoder och system för att med bildsensorer inhämta information om stela objekt som bilar och hus samt om miljöer, medan metoderna för att observera människor och folkmassor är mycket outvecklade. Det kommer att kräva många års utvecklingsarbete för att ta fram effektiva och robusta metoder för detektion, följning och igenkänning av människor i bildsekvenser.

6.3.2 Sensornätverk för övervakning av skyddsobjekt

Ett sensornätverk är ett autonomt system som består av ett antal sensorer av samma eller varierande typ. Nätverkets sensorer ska placeras på ett sådant sätt att deras täckningsområden delvis överlappar och tillsammans täcker hela ytan inom det område där nätverket finns. Det måste dessutom finnas ett kommunikationssystem som gör det möjligt för sensorerna att utbyta data där det vanliga är att det sker i ett ad hoc-nätverk, se avsnitt 5.8. Vidare ska det finnas ett informationssystem som hanterar data, väljer vilka sensorer som ska användas i ett givet ögonblick och lägger samman (fusionerar) data från de valda sensorerna. Detta informationssystem bör normalt vara en del av ledningssystemet. Utdata från sensornätverket blir information, d v s en för människan tolkningsbar beskrivning av genererade data. Denna information utgör en fusion, se avsnitt 5.4.2, av data från de olika sensorerna, t ex ett fordons position, klass och hastighet.

En av fördelarna med att använda ett yttäckande nätverk av sensorer jämfört med enstaka punktsensorer är att det t ex går att låta nätverket analysera rörelsemönster. Det skulle kunna innebära att nätverket inte ger larm då en bil kör genom området på allmän väg, men att det larmar om bilen stannar längre stunder på ställen utmed vägen där den inte borde stanna eller om urlastning av något sker. Det är långt ifrån självklart att all ”onormal” aktivitet utgör ett hot, men antal möjliga hot (larm) som skall bedömas av en operatör kan minska kraftigt. En annan möjlighet är att använda sensorer som mäter på objekt från flera olika vinklar och kanske med olika sensormekanismer för att få en mer komplett bild av objektet utan att det krävs manuell klassificering.

Beroende på sensornätverkets storlek och syfte är det möjligt att fusionera data till olika nivåer. I vissa fall skulle det kunna vara intressant att studera avvikelser i trafikmönster (t.ex. att 20 fordon körde på en väg en natt där det i vanliga fall inte är någon trafik nattetid), vilket är en ganska hög nivå. I andra fall räcker det med att följa enstaka objekt i området och rapportera detta, vilket är en låg nivå av fusion.

Exempel på tillämpning är övervakning av flygplatser, hamnar och liknande större objekt som är känsliga för intrång. Eftersom det finns mycket normal aktivitet i dessa omgivningar går det

inte att ha en sensor som larmar varje gång ett fordon/människa rör sig i omgivningen. Istället kan ett sensornätverk bidra till att förbättra den information som skickas till användaren (t.ex. en övervakningscentral) genom att fusionera sensordata från flera sensorer för att uppnå säkrare klassificering av fordon/människa/djur, följning över större områden samt analys av rörelsemönster. Det är dock viktigt att komma ihåg att komplexiteten ökar ju högre nivå man vill nå, att klassificera och följa enstaka objekt är förmodligen genomförbart i närtid, medan analys av rörelsemönster inte kommer att kunna realiseras på flera år. Området finns belyst ytterligare i [42], [43] och [40].

6.3.3 Andra typer av datakällor

Övriga typer av datakällor kan vara existerande databaser av olika slag. Till sådana databaser kan räknas geografiska databaser för sammanhang där rumslig information är nödvändig. Olika typer av information med både rumslig och temporal information finns också. Exempel på sådan information kan vara larmmeddelanden till SOS-Alam eller andra larmcentraler.

6.4 Beslutsstödhjälpmedel och informationsfusion

Beslutsstödshjälpmedel som i många fall kan vara baserade på olika former av informationsfusion är nödvändiga element i ledningssystem med multipla datakällor. Beslutsstöd i ledningssystem är väsentliga med hänsyn till att de skall kunna bidra till insamling och sammanställning av den information som krävs för att en krisledningsgrupp skall kunna fatta nödvändiga och adekvata beslut i en krissituation. Antalet datakällor kommer i framtiden att vara stort och av denna anledning kommer behovet av att kunna fusionera denna information på ett adekvat sätt att öka. Denna process kallas vanligen informationsfusion. Integration av informationsfusion i beslutsstöd medför emellertid en ökande komplexitetsgrad som måste kunna hanteras. Ökning i komplexitet beror på ett flertal faktorer bland vilka kan nämnas den olika karaktären hos datakällorna samt den ökande datavolymen och osäkerheten i inkommande data. Alla dessa faktorer måste kunna hanteras i informationsfusionen.

6.4.1 Beslutsstödhjälpmedel

Beslutsstödshjälpmedel kommer alltid att vara i fokus i ledningssystem vare sig dessa är avsedda för militära eller civila tillämpningar. Självfallet kommer dessa hjälpmedel att vara av varieeande slag men av central betydelse är att de måste vara baserade på en för varje enskild tillämpning generell metodik. Man kan i huvudsak se två olika aspekter på beslutsstödsproblematiken, nämligen den logiskt/tekniska och den som associerar till MSI-aspekterna. Speciellt tas här hänsyn till de krav som kan komma att ställas i samband med nätverksbaserade lösningar.

De beslutsstöd som kommer att behöva utvecklas har som gemensam nämnare att de effektivt måste kunna hantera den information som extraherats ur de aktuella datakällorna, d v s primärt ur aktuella sensorer. Detta arbete omfattar inte enbart utveckling av de sensordataanalysprogram och de datafusionsmetoder som kommer att behövas, även om dessa kommer att utgöra en väsentlig del av de beslutsstöd som efter hand kommer att bli tillgängliga. Huvudsyftet med ett beslutsstöd är att förse användaren med ett redskap som gör det möjligt att mer eller mindre automatiskt samla in den information som krävs för att skapa det underlag som behövs för att användaren skall kunna fatta de beslut som löser de förelagda arbetsuppgifterna. Härvid skall man inte avkräva användaren någon omfattande teknisk kompetens d v s alla de hjälpmedel som kommer att behövas måste ge användaren möjlighet att lösa sina arbetsuppgifter utan att sådan teknisk kompetens behövs. Av denna anledning är det nödvändigt att man enkelt kan specificera de data som behöver samlas in, analyseras och fusioneras. För att göra detta möjligt

kommer det att krävas redskap med hög *generalitet*. Ett sådant redskap kommer också att kräva ett kraftfullt visuellt användargränssnitt. Inom ramen för detta utgör begreppet *tjänst* en central aspekt. Syftet med denna aspekt är att visa på alla de behov som kan tänkas föreligga och därmed också ge möjlighet till att generalisera informationsinhämtningen. En tjänst kan också ses som ett sätt att strukturera de olika delprocesserna/redskapen i ledningssystemet, t ex ett geografiskt informationssystem (GIS). Huvudsyftet är att i varje ögonblick förse de olika aktörerna med relevant information. Givetvis måste detta ske på ett användarvänligt och användbart sätt. För att uppnå önskvärd generalitet måste således redskap som uppfyller de olika funktionalitetskraven utvecklas. Man kan tänka sig flera olika ansatser för sådana redskap. Vid FOI i Linköping pågår sedan en tid utvecklingen av ett *frågespråk* för heterogena sensordatakällor [44].

6.4.2 Informationsfusion

Med informationsfusion [45] menas huvudsakligen en metodik som innebär att man på olika sätt hanterar information som är extraherad från multipla datakällor och på olika sätt väger samman denna information. Syftet med denna sammanvägning skall ge ett resultat som en användare kan känna större tilltro till än vad man kan ha enskilt för varje datakälla. Ett problem i detta sammanhang är att denna information oberoende av vilken källa den kommer från, alltid måste associera den med någon from av osäkerhet. Detta gäller både om datakällorna utgörs av sensorer eller av meddelanden från mänskliga observatörer. En väsentlig uppgift inom informationsfusionen är därför att hantera dessa osäkerheter inte bara vid källan utan också under hela processen d v s under hela sammanvägningsprocessen. Informationsfusion är med hänsyn till dessa osäkerheter vanligen baserad på olika sannolikhetsmodeller, t ex Baysianska nät [46] eller s k evidensmetoder där den mest kända går under namnet Dempster-Schafer [47].

Informationsfusion kan indelas i fyra huvudgrupper där sensorfusion utgör den lägsta nivån d v s närmast sensorerna. Exempel på operationer som äger rum på denna nivå är bestämning av observerade måltyper, deras position samt bestämning av deras färdvägar (eng. tracking). Nästa nivå är situationsanalys som innefattar operationer av typ aggregering samt associering d v s man analyserar vilka objekt som kan sammanföras till större grupper samt vilka observationer som gjorts av samma objekt. Den senare operationen avser således bestämning av huruvida flera observationer avser samma eller olika objekt. Associeringsproblematiken är ofta komplex till sin natur eftersom också den kräver en lösningsmetodik baserad på någon sannolikhetsmodell.

Det tredje steget i informationsfusionsprocessen utgörs av hotanalyssteget (eng. impact analysis). Detta steg utgör den högsta nivån i informationsfusionskedjan. Denna analys innefattar t ex hänsynstagande till eventuella strategier och doktriner som en eventuell motpart kan basera sina aktiviteter på. Denna del av informationsfusionen förekommer i stor utsträckning i militära tillämpningar men kan också komma till användning i vissa krissituationer grundade på t ex olika terroristaktiviteter. Målsättningen här är att bestämma motpartens förväntade aktiviteter, vilket är väsentligt vid riskbedömning.

Det som brukar kallas det fjärde steget i fusionsprocessen, d v s det adaptiva steget, är en återkoppling som kan äga rum på flera nivåer. Man kan enkelt sammanfatta detta steg som en förfiningsprocess.

Sammanfattningsvis kan man konstatera att informationsfusion spelar en central roll i ledningssystem där data från många olika typer av datakällor skall hanteras. Av denna anledning

finns det starka skäl att anse att informationsfusion också kan bli en betydande pusselbit också i ett ledningssystem för krishantering och att forskning inom detta område måste ingå.

6.5 Människa-systeminteraktion

Människa-systeminteraktion är ett multi-disciplinärt forskningsområde, som omfattar experimentell forskning och metodutveckling för värdering och utveckling av människa-maskin/ dator-system. Forskningen är inriktad mot samspelet mellan människa, teknik och de krav som omgivning och arbetsuppgifter ställer. Individens, gruppens och organisationens arbetssituation är i centrum [48].

Människa-systeminteraktion omfattar en stor bredd forskningsdiscipliner från humanvetenskaper som beteendevetenskap, psykologi, neuropsykologi, psykofysiologi, socialpsykologi, sociologi, organisationsutveckling, pedagogik, kognitionsvetenskap, ledningsvetenskap, ergonomi till ingenjörsvetenskaper som datavetenskap, lingvistik, systemteknik, medicinsk teknik, simulering, industriell arbetsmiljö. Även kunskaper inom t ex antropologi och konst efterfrågas.

De viktigaste kompetensområdena utgörs av gränssnittsutformning, informationspresentation, perception, kognition, beslutsfattande, mental och fysisk belastning, prestation, ledning, team work, kommunikation, automation, simulering, modellering, träning och utbildning.

6.5.1 Utvecklingstrender inom människa-systeminteraktion

Förmodligen ett av världens mest komplexa simulerade människa-maskinsystem eller prototypsystem för design av bemannade helikoptersystem inom armé, flyg och marin har utvecklats vid NASA Human Factors Research Laboratory. Utvecklingen av detta system, MIDAS (Man-machine Integration Design and Analysis System) [49] var närmast unik såtillvida att man redan i ett tidigt skede av designprocessen använde och utgick från modeller för mänskliga prestatationer snarare än tillämpningsspecifika guidelines, studier, eller vapensystem. Bakgrunden till framtagandet av detta simulerade människa-maskinsystem var en mängd växande operativa svårigheter och utbildningsproblem med nya system, som innebar krävande tekniska uppdrag med krav på effektivt användande av många delsystem och sensorer, som i sin tur medförde dramatiskt ökade krav på människan på såväl motoriska, perceptuella, och kognitiva funktioner och som inte minst medförde en alltför hög arbetsbelastning, vilket utgör den viktigaste bidragande orsaken till misslyckade uppdrag samt förlust av besättningar och flygplan. Projektet initierades då många av problemen visade sig gemensamma för alla flygplanstyper både inom militärt och civilt flyg. Hur komplexa och automatiserade system ska anpassas till mänskliga förmågor och färdigheter skapar ofta svåra problem. Ca 70 till 85% av livscykelkostnader för ett flygplan bestäms under ide´ -och konstruktionsstadiet. De höga initialkostnaderna samt de stora svårigheterna att modifiera begrepp och korrigera misstag i efterhand blev bestämmande för utvecklingen av MIDAS systemet, som gav möjlighet till tidig integrering och visualisering av principer för människa-systeminteraktion. I MIDAS ingår datamodeller baserade på experimentella data från många mänskliga funktioner. Modellen innehåller också en symbolisk aktörsmodell, som behandlar högsta nivå av abstraktion av mänskligt operativt agerande och som omfattar modeller för seende, perceptuell uppmärksamhet, omvärldsrepresentation, beslutsfattande, planering, arbetsbelastning [50] och motoriskt handlande. Karaktäristiskt för MIDAS är dess stöd vid realistisk dynamisk analys och dess simuleringskapacitet. MIDAS är ett illustrativt exempel på en prototyp, där principer och kunskaper om människa-systeminteraktion varit centrala och drivande i utvecklingen redan från början.

Med dagens allt komplexare system-av-system är det nödvändigt att i tidigt skede av utvecklingsprocessen införliva och optimalt integrera kunskap om mänskliga förmågor och färdigheter om användbara system ska kunna uppnås. Dessutom leder sådana satsningar till inte bara betydande förbättringar utan också stora kostnadsbesparingar, till uppskattningsvis upp till ca 50%-iga minskningar i totala livscykelkostnader. Satsningarna innebär sist men icke minst minskning av skador och olyckor inklusive de med dödlig utgång.

Människa-systeminteraktion (eng. human-system interaction, human factors m.m) växte fram som ett forskningsområde i USA under 1940-talet framförallt inom flyget i det amerikanska försvaret för att värna liv hos soldater och med framgång möta aktuella stridsuppgifter. Sedan denna tid har flyget, både det militära och det civila, fortsatt varit de starkaste pådrivarna av forskning och utvecklingen inom området människa-systeminteraktion. Flyget får också anses vara tidigt och på framkant i ett system-av-system tänkande. Inte minst haveriutredningar har banat vägen för ett sådant tänkesätt. Ett unikt och övergripande systemtänkande initierades av den amerikanska armén under 1980-talet genom projektet MANPRINT [52], [51]. Styrkan i MANPRINT är dess filosofi, metoder och tekniker, som kan tillämpas på alla produkter och system, som används av människor. MANPRINT omfattar organisations-och ledningsfrågor, användarcentrerad design, metoder för systemintegrering, komplexa omgivningsmodeller vid systemintegrering, metoder för analys av arbetsbelastning, prestationer, träning och utbildning av personal i komplexa system. Civilt har exempelvis International Standardisation Organisation (ISO) publicerat standardiserade riktlinjer för designprocessen vid systemutveckling utgående från människans behov och förutsättningar [53], [54].

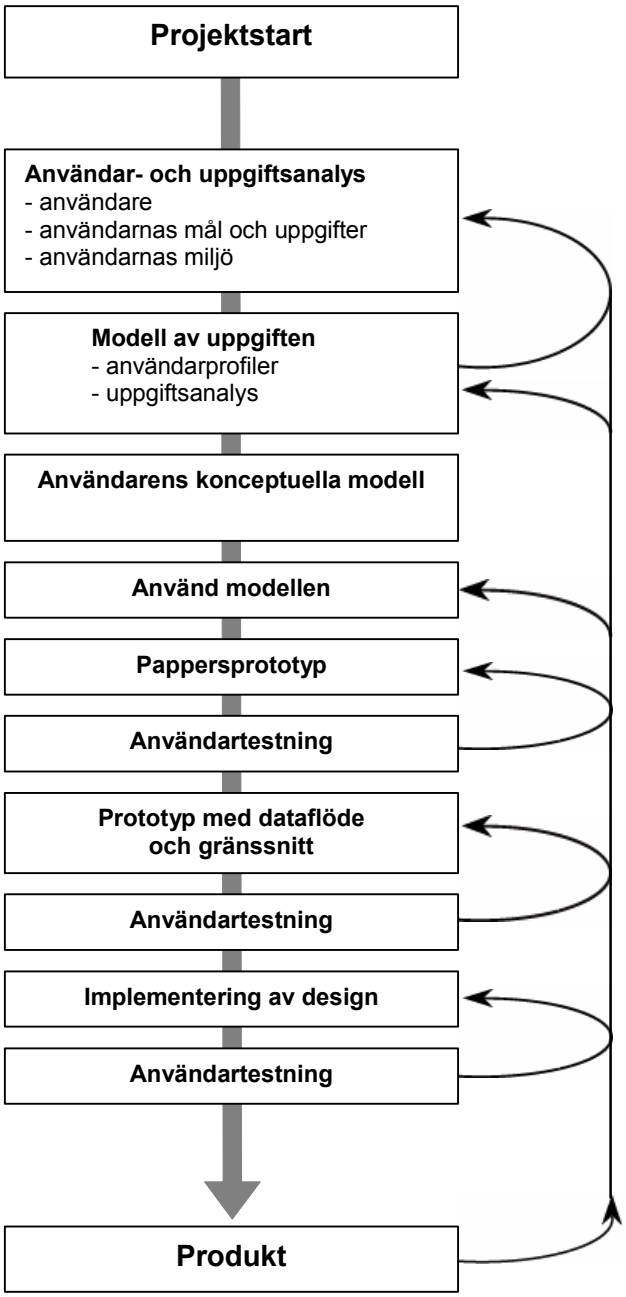
Med de kraftfulla datorernas framväxt under 1980-talet skapades stora förväntningar på datorn som möjligheter för interaktion, visualisering, avancerad datapresentation, artificiell intelligens, autonomt tänkande och fungerande etc. Användningen av den komplexa tekniken ledde även till många nya problem samt till mänskliga misslyckanden och frustrationer då man i avsaknad av kunskap och erfarenhet inte tillräckligt kunnat beakta människors beteenden och interaktioner med den nya tekniken vid designen av densamma. Ur behovet att få mer förståelse om hur människor och komplex teknik interagerar och ur behovet att skapa fungerande människa-datorsystem för människor i samverkan med den nya tekniken och med varandra växte ett nytt område fram i USA "Cognitive systems engineering" [55], [56], [57] ett multidisciplinärt forskningsfält och kunskapsområde med influenser från vitt skilda ämnesområden.

Från 1990-talet och framåt kan man skönja en ny trend inom området människa-systeminteraktion. Det räcker inte längre med att system är användbara i betydelsen möjliggör optimala prestationer under rimlig arbetsbelastning. System ska även befrämja motivation och möjliggöra känslomässigt engagemang. Kansei Engineering [58] är en ergonomisk konsumentinriktad metod för produktutveckling baserad på känslor och användarkrav. En databas av nyckelord som innehåller konsumenters beskrivningar av en produkt byggs upp. Det japanska ordet "Kansei" omfattar en persons helhetsintryck av ett föremål, eller situation, upplevt genom alla sinnen. Utvärderingen baseras i huvudsak på semantik, det vill säga "Kansei-ord", adjektiv som beskriver någons uppfattning om något. Genom Kansei Engineering kan konsumeters känslor överföras till designelement.

Emotioners och känslors grundläggande betydelse i allt mänskligt liv har Damasio beskrivit mycket tankeväckande [59].

6.5.2 Centrala människa-systeminteraktionsaspekter vid systemutveckling

Kunskap om människa-systeminteraktion har kommit att bli alltmer central för utvärdering vid systemutveckling för att skapa användbara system. "*Ett iterativt designförlopp för alla steg i en systemutveckling och med hänsyn till kunskap om människan illustreras enligt Hackos och Redish [60] i figur 9. Vikten av tidiga användar- och uppgiftsanalyser tydliggörs*" [61].



Figur 9. Schematisk beskrivning av designprocessens iterativa livscykel, med användaranalyser, uppgiftsanalyser och utvärderingar (anpassad efter [60]).

De olika stegen i figur 9 representerar olika forskningsområden, t ex metoder för uppgiftsanalys mentala processer som omfattar uppmärksamhet, varseblivning, informationshantering, minne, begreppsbildning, resonerande och problemlösning samt mentala modeller för situationsmedvetande, handlande, samverkan etc. Mentala modeller kan kortfattat beskrivas som "*förmågan att organisera minnen som behövs för att förstå specifika situationer. Används för*

att organisera erfarenheter av sig själv, andra människor, miljön och av de tekniska system man interagerar med ...” [61], sid 67.

Människa-systeminteraktion för komplex systemutveckling inbegriper förmågor hos enskilda individer, hos grupper och sociala system och en utvärdering måste därför ske med utgångspunkt från kunskap om såväl den enskilda individens kapacitet samt utifrån kunskap om individers och gruppers attityder, värderingar, motiv, beteenden och samverkan.

6.6 Systemtilltro

Tilltron till andra människor, samhällsfunktioner eller system i ett vidare begrepp, påverkas bl a av faktorer som förutsägbarhet, pålitlighet och övertygelse. Det innebär att tilltron till t ex ett ledningssystem påverkas dels av en historia med det specifika systemet men också av en föreställning om i vilken grad systemet är att lita på i framtiden. Systemtilltron får också olika underlag beroende på i vilket skede av ”kännedomsprocessen” med systemet man befinner sig i. Från ett rykte, via kännedom och senare kunskap, till slutligen erfarenhet av systemet byggs en grund för tilltron som, vid sidan av de rena kunskapsrelaterade förutsättningarna, starkt bidrar till hur ett system används och utnyttjas.

I en krissituation är det viktigt att deltagarna, både aktörer och utsatta, har förtroende för och tilltro till varandra och systemet. De drabbade i samhället känner förmodligen stor osäkerhet om vad som kommer att hända dem, sårbarheten är uppenbar och tilltron till det system som ska hantera situationen får en väsentlig och kanske avgörande betydelse [62]. Detta gäller naturligtvis i högsta grad även de som måste agera för att häva krisen eller mildra dess konsekvenser.

Ur ovanstående resonemang skulle några grupper i samhället kunna särskiljas med olika beroende och relation till krisledningsfunktionen/systemet, dels de direkt involverade i användandet av ledningssystemet och dels de som, på något sätt, drabbats av den uppkomna krisen:

användare; - ledning (myndighet, militär, räddn. tjänst, ARCC, MRCC osv.)
- utförare (personal inom räddningstjänst, civila)
drabbade; - direkt (skadade, anhöriga, organisatorisk tillhörighet osv.)
- indirekt (genom identifiering, samhörighetskänsla osv.)

Samverkan mellan användare och system är mycket viktigt om synergieffekter skall uppnås. Om användare inte litar på systemet utnyttjar de det inte till fullo eller ignorerar det och använder enbart egna bedömningar istället. Ett komplext tekniskt och socialt system som ett ledningssystem i form av t ex ett informationsnätverk kan inte förväntas få omedelbar tilltro. Användarna behöver tid och utbildning för att vinna tilltro till dessa nya verktyg. För de som kan räknas till de drabbade i en kris spelar en upplevd närhet och samhörighet med organisationen och systemet som hanterar krisen stor roll för att de ska känna tilltro och förtroende för ledningsfunktionen [63]. Om ledning och utförare, enligt definitionen ovan, har de drabbades förtroende/tilltro kan förmodligen arbetet med att mildra och häva krisens verkningar väsentligt underlättas. Det är alltså av största vikt att alla, både användare och drabbade, har haft tillfälle att, under normala förhållanden, skaffa sig adekvat kunskap om systemet och känner sig så bekanta med det att de även i en krissituation känner tilltro till systemet och dess förmåga.

De tre centrala och grundläggande principerna för ansvarsfördelning vid krishantering, se avsnitt 2.3; *ansvars-, likhets-* och *närhetsprincipen* ger goda förutsättningar för att ett ledningssystem för krishantering skall erhålla så hög grad av tilltro som möjligt utan att för den skull

överskattas. Genom att användare har samma ansvar under normala förhållanden som i ett krisläge, har de goda möjligheter att bygga sin systemtilltro på erfarenhet. Likhet i organisation och lokalisering ger alla, både användare och drabbade, goda möjligheter att ”känna igen sig” även i en krissituation. Slutligen kan hantering av krisen på lägsta möjliga samhällsnivå, enligt närhetsprincipen, ge goda förutsättningar även för tillfälligt sammansatta organisationer att erhålla tilltro genom att de byggs på kompetens, professionalism och engagemang [64].

Då systemtilltron påverkas av den uppfattning vi får av systemet redan genom rykten och kännedom är även marknadsföring och implementering av ett ledningssystem viktig för att alla skall ge systemet så stor och befogad tilltro det förtjänar. Det är alltså även viktigt att systemet inte ges för hög grad av tilltro, övertro, då detta också påverkar samverkan med systemet på ett negativt sätt.

6.6.1 Integritet

Ett ledningssystem med stort behov av information kan medföra omfattande övervakning av medborgarna i ett samhälle, vilket av många kan uppfattas som integritetskränkande. Med en hög förståelse för ledningssystemets funktion och dess avsikter ökar dock förutsättningarna för en stor systemtilltro och därmed bör även känslan av att den egna integriteten kränks minska eller rentav försvinna. Några punkter som borde underlätta de övervakades förståelse för ledningssystemets funktion kan vara att man;

- vet vem som övervakar
- sympatiserar med övervakaren
- känner till orsaken till övervakning
- gillar eller åtminstone accepterar orsaken till övervakning

Dessa punkter kan relateras till begrepp som starkt anknyter till systemtilltro såsom familjäritet, avsikt, begriplighet och ärlighet. Frågor om integritet verkar alltså ligga nära problemställningana man ställs inför när man försöker skapa en stor och befogad tilltro till ledningssystemet.

6.7 Informationssäkerhet, IT-säkerhet och driftsäkerhet

Säkerhet är en egenskap som är avgörande för existensen av såväl organisationer som system. Brist på säkerhet leder primärt till ekonomiska och materiella förluster samt, i värsta fall, till och med personskador. Sekundärt resulterar otillräcklig säkerhet i att tilltron skadas, vilket kan leda till att användningen minskar och, i extrema fall, att system kasseras eller organisationer upplöses. Ett exempel på system och organisationer vilka under senare år drabbats hårt av säkerhetsproblem är flygtrafiken respektive flygbolagen. Vidare finns det exempel på informationssystem vilka efter lång och omfattande utveckling helt har kasserats på grund av bristande säkerhet.

Låt oss en gång för alla slå fast att fullständig eller 100-procentig säkerhet inte existerar. För det första innehåller alla typer av system brister. För det andra så kan inte system konstrueras så att alla risker som orsakas av felaktigt användande elimineras, till exempel går det inte att hindra någon från att skriva upp bankomatkoden och förvara den tillsammans med kortet. För det tredje får inte säkerhetslösningarna bli så komplicerade att de uppfattas som störande av användarna. Det är oftast därför som dåliga lösenord tillåts, fast det går att införa begränsningar som stoppar användandet av sådana [80].

Att säkra korrekta data till rätt tid och till rätt aktör, är uppenbarligen viktigt i krishantering. (ett eller ett par klargörande krisexempel). Detta diskuteras, som i exempelvis [81], ofta i termer av datakvalitet, vilket både ur drift- och informationssäkerhetssynpunkt är av central betydelse att upprätthålla.

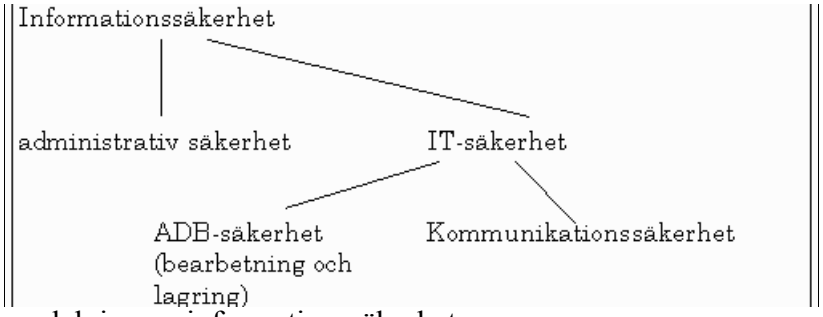
I detta avsnitt diskuteras två aspekter av säkerhet: informationssäkerhet och systemsäkerhet. Informationssäkerhet kan delas upp i olika delområden. När distribuerade informationssystem är i fokus framträder IT-säkerhet som en betydande del av informationssäkerhetsområdet.

Informationssamhället är beroende av väl fungerande informationssystem och -infrastruktur, vilket förutsätter en hög IT-säkerhetsnivå. Exempelvis förlitar sig många organisationer allt mer på Internet som informationsbärare. Att IT-säkerheten är kritisk för ett högteknologiskt samhälle förstärks av de resonemang som förs av bland andra Sårbarhets- och säkerhetsutredningen [82].

Ofta används katastrofscenarion för att motivera behovet av IT-säkerhet. Det finns argument mot dylika scenarion [83]. En mer relevant riskbild består av många begränsade IT-säkerhetsincidenter vilka tillsammans allvarligt kan skada hela organisationer och samhället. Detta ställer stora krav på att kontinuerligt och på alla nivåer (hos enskilda användare, organisationer och samhälle) kunna möta och hantera IT-säkerhetsproblem.

6.7.1 Informationssäkerhet och IT-säkerhet

Informationstekniska standardiseringen i Sverige, ITS, definierar informationssäkerhet som bestående av administrativ säkerhet och IT-säkerhet. IT-säkerhet, i sin tur, delas upp i ADB-säkerhet och kommunikationssäkerhet. Detta illustreras av Figur 10 från [84], vilken innehåller definitioner av de olika begreppen. Det kan noteras att termen ADB-säkerhet är synonym med datasäkerhet. Denna uppdelning anammades av Sårbarhets- och säkerhetsutredningen [82].



Figur 10. ITS uppdelning av informationssäkerhet.

Hallberg et al skriver [85]:

Informationssäkerhet består i att bevara någon eller flera av egenskaperna sekretess, tillförlitlighet och tillgänglighet för information, vilken på något sätt är kritisk för en given verksamhet. *IT-säkerhet* består i att bevara någon eller flera av egenskaperna sekretess, tillförlitlighet och tillgänglighet för information och tjänster som hanteras respektive tillhandahålls av informationssystem. *Administrativ säkerhet* rör rutiner och information vilken inte är en del av informationssystemet men påverkar dess säkerhet, såsom behörighetsadministration med mera. Således gäller informationssäkerhet all information i alla dess former medan IT-säkerhet endast avser information som hanteras av informationssystem (elektronisk information). Å andra sidan inkluderar IT-säkerhet de tjänster som informationssystem levererar.

Det finns ett starkt beroende mellan IT-säkerhet och administrativ säkerhet. Detta medför att båda dessa områden måste beaktas för att få en heltäckande bild av problematiken, d v s graden av säkerhet i distribuerade informationssystem. Däremot täcker de inte aspekter gällande information som inte hanteras med eller berör distribuerade informationssystem, vilka dock torde vara en del av informationssäkerheten. I fortsättningen diskuteras IT-säkerhet i en vidare bemärkelse, vilken inkluderar administrativ säkerhet.

6.7.2 Aktiv IT-säkerhet

Traditionellt har man tänkt sig IT-säkerhet som ett huvudsakligen passivt försvar. Den växande systemkomplexiteten leder dock till att helt passiva försvar blir allt mindre realistiska. Därför måste även aktiva komponenter beaktas. IT-säkerhet brukar delas upp i förmågorna att skydda, upptäcka och reagera (SUR). SUR-tanken relaterar till riskhantering. De sårbarheter som inte kan elimineras bör täckas in av mekanismer och rutiner för upptäckt, vilket också kräver en förmåga att reagera när säkerheten bryts. Reaktionsförmågan kan ha vitt skilda delar, vilka exempelvis syftar till återställning av system eller att begränsa angripares tillgång till systemet.

Ett aktivt upprätthållande av IT-säkerhet kräver dock vidare förmågor än SUR. Dessa förmågor relaterar till värdering, spaning, angrepp och ledning. Sammantaget utgör de resulterande fem förmågorna ett IT-försvar [85]. Förmågan IT-säkerhet innefattar de delar av förmågorna skydda, upptäcka och reagera som är begränsade till det egna systemet. De delar av förmågan upptäcka som baseras på kunskap om andra system ingår i IT-spaning och de delar av förmågan reagera som riktas mot andra system ingår i IT-angrepp. Ett effektivt IT-försvar kräver en ledningsförmåga. Dessutom behövs en förmåga till värdering, IT-försvarsvärdering, vilket framträder som en väsentlig och komplex förmåga. Den inbegriper nivåer på samtliga andra förmågor, i såväl egna som andras nuvarande och framtida system, samt möjliga effekter på system och omgivning.

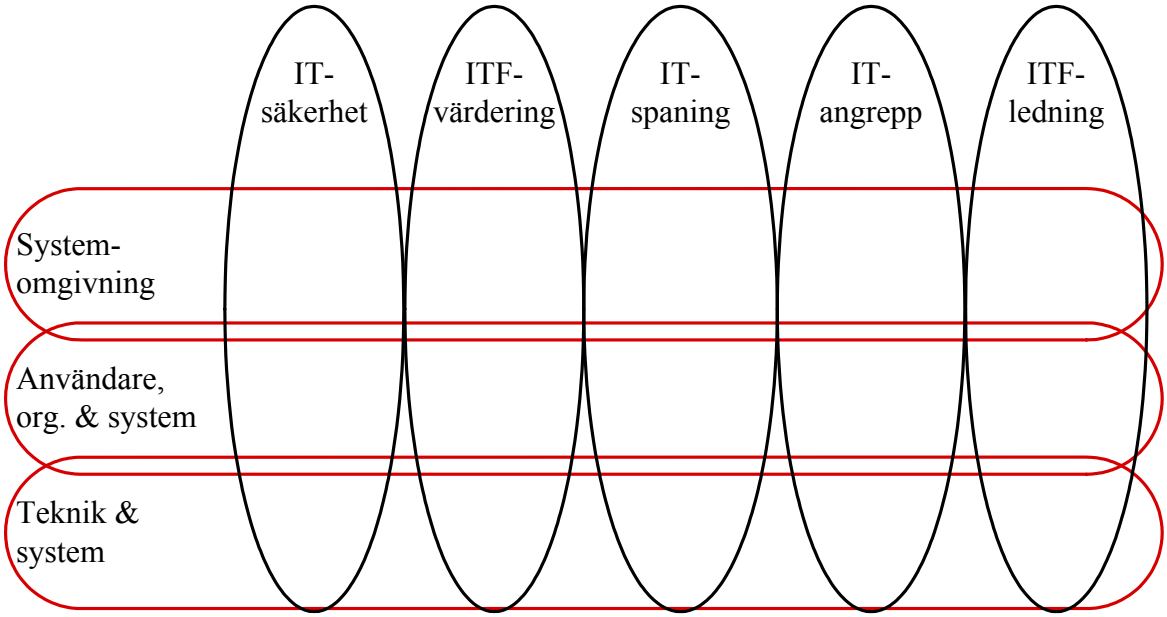
För att kunna uppnå en hög IT-säkerhetsnivå för ett informationssystem krävs att ett stort antal frågeställningar relaterade till IT-försvarsförmågorna besvaras. Dessa frågeställningar är av starkt varierande karaktär, gällande till exempel teknik, organisation eller policy. Dessa frågeställningarna kan kategoriseras med hjälp av de tre aspekterna Systemomgivning, Användare, organisation & system samt Teknik & system. Exempelvis inkluderar användarautentisering[1] frågor rörande teknik (användning av lösenord, aktiva kort eller biometri, lagring av verifieringsdata, etc.), användare och organisation (rimliga krav på och acceptans hos användare, administration av autentiseringssystemet, etc.) och omgivning (lagar och förordningar, allmän acceptans i samhället, etc.). En indelning av IT-försvarsfrågor i olika aspekter kan aldrig bli helt entydig utan resulterar i både överlapp och beroenden.

Figur 11 nedan beskriver hur IT-säkerhetsproblematiken spänner över olika förmågor[2] och aspekter. Därigenom tydliggörs områdets betydande omfattning. För att få med både förmå-

1. Användarautentisering syftar till att verifiera att användare är de som de utger sig för att vara.

2. Det faller sig naturligt att prioriteringen och utformningen av de olika IT-försvarsförmågorna är situations- och organisationsberoende. En klar skiljelinje kan tyckas finnas mellan dem som har som ambition att utnyttja de offensiva förmågorna strategiskt och dem som endast är intresserade av att försvara sig mot IT-hot. Varje effektivt försvar har dock offensiva förmågor. Därmed finns det ett behov av kunskap inom detta område för alla organisationer.

gorna och aspekterna i en figur förenklas bilden genom att överlappen mellan förmågorna samt mellan aspekterna Systemomgivning och Teknik & system tas bort.



Figur 11. Ett IT-försvar består av de fem förmågorna IT-angrepp, IT-säkerhet, IT-försvarsvärdering, IT-spaning och IT-försvarsledning. Dessa kan studeras ur de tre aspekterna Systemomgivning, Användare, organisation & system samt Teknik & system [85].

Hittills har forskning och utveckling inom IT-säkerhetsområdet i huvudsak varit fokuserad på tekniska aspekter och produkter samt övergripande studier, d v s inom aspekterna Teknik & system respektive Systemomgivning. Detta har delvis sin grund i att fysisk separation har varit ett faktum och tillsammans med fysisk säkerhet har kunnat utnyttjas för att uppnå tillräckligt hög IT-säkerhet. Den pågående integrationen av informationssystem omintetgör dock detta och tvingar fram ett nytänkande som beaktar såväl teknik som användar-, verksamhets- och organisationsfrågor. Exempelvis så har framtagandet av lösningar för distribution av öppna kryptonycklar, s k public-key infrastructures (PKI), fokuserat på de tekniska utmaningarna, vilket har resulterat i tekniskt fungerade system vilka dock har varit mycket svåra att få att fungera i sina organisatoriska sammanhang.

Områdets mognad samt insikter som att absolut säkerhet inte existerar och att säkerhet är en process, inte en produkt, [86] leder dock till att forskningen framöver mer kommer att inriktas på att ta fram lösningar vilka möjliggör en effektiv riskhantering.

6.7.3 Driftsäkerhet

Vad vi här omnämner som driftsäkerhet, innefattar säkerhetsfunktionalitet som normalt sett inte diskuteras i termer av informations-/IT-säkerhet. Exempelvis är kvalitet hos informationssystem och dess programvara av central säkerhetsmässig vikt, även där detta inte fullt ut beskrivs av IT-säkerhetens grundbegrepp sekretess, tillförlitlighet och tillgänglighet.

Driftssäkerhet är en sådan faktor av central vikt för den typ av ledningssystem vi föreslår. Det torde vara uppenbart att problem med att upprätthålla driften i ett sådant system i en krissituation vore katastrofalt. Samtidigt kan man observera att driftssäkerheten även har påverkan på IT-säkerheten, till exempel genom att bristfällig driftsäkerhet påverkar tillgängligheten. Behovet av gemensam begreppsbildning rörande driftsäkerhet diskuteras i [87]. I ett vidare arbete

kring ledningssystem för krishantering, är det av vikt att en sådan begreppsbildning tydligt influerar hur systemen byggs upp för att ge tillräcklig driftsäkerhet och informationssäkerhet.

6.8 Kommunikation/nätverk

Kommunikationsnätet utgör den nödvändiga infrastruktur som krävs för att information skall kunna transporteras på ett snabbt och säkert sätt i ett ledningssystem. En vanlig liknelse är att kommunikationsnätet motsvarar människans nervsystem. Tillförlitliga kommunikationer är nödvändiga för att exempelvis sprida sensorinformation (t ex från gas- och radiakdetektorer), ledningsinstruktioner, positionsangivelser etc inom ett ledningssystem. Kommunikationsnätet måste säkerställa höga krav på tillgänglighet, tålighet samt säkerhet ur olika perspektiv. Praktiska erfarenheter visar entydigt att ett ledningssystem som saknar säkra och robusta kommunikationsnät snabbt förlorar förmågan att leda insatser. Forskning inom krishantering visar att den initiala fasen av en kris ofta är mycket avgörande för hur krisen utvecklar sig och för hur väl man kan hantera konsekvenserna. Det är i detta sammanhang viktigt att snabbt kunna larma ut personal för att hantera akuta problem [89]. Detta förutsätter alltså tillgång till robusta och säkra kommunikationsnät. Ledning ute på fältet, olycksplatser, riskområden etc förutsätter tillgång till trådlösa kommunikationsnät eftersom rörlighet är ett grundläggande krav i dessa situationer. Under de s k Göteborgskravallerna 2001 konstaterades att ett av de stora problemen med att leda polisinsatsen orsakades av att polisens radiosamband inte fungerade störningsfritt. En av orsakerna till detta tros vara att anhängare till demonstranterna sände falska larmanrop som tidvis blockerade all annan trafik [92]. I tätbebyggda områden är ofta den allmänna elektromagnetiska bakgrundsmiljön gränssättande för med vilken kvalitet och säkerhet trådlös kommunikation kan användas. Av detta skäl är det av yttersta vikt att sårbarhetsanalyser kan göras av aktuella kommunikationssystem för ledning. I framtida nationella nätverksbaserade lösningar skall ett stort antal enheter med olika organisatoriska tillhörigheter kunna kommunicera. Dessutom förutsätts civila och militära resurser kunna samutnyttjas [90] vilket förutsätter delvis nya tekniker för trådlös kommunikation; dels måste kommunikationen kunna ske *sömlöst*, dels måste kommunikationsnäten vara av typen *mobila ad hoc-nät*.

Med *sömlös kommunikation* menas att användarna trots dynamiska förändringar i näten har tillgång till de ledningssystemtjänster de behöver, oavsett vilken terminal de använder, vilket delnät de har tillgång till och vilken organisationsenhet de tillhör. Dynamiska förändringar i näten kan bero på variationer i till exempel: trafiklaster, topologi och rörelsemönster. Ibland används ordet transparent som synonym till sömlöshet. Med det menas att användarna i näten inte ska märka av de tekniska lösningar som gör kommunikationen möjlig. Idag förväntas sömlös kommunikation kunna lösas genom få samtliga system att använda samma protokoll som används inom internet d v s IP (Internet Protokoll).

Ett *ad hoc-nät* är ett kommunikationsnät som fungerar utan förplanering, oberoende av fast infrastruktur. Nätet har inga specialiserade noder med centrala funktioner (som t ex en basstation). Noderna (radiostationerna) kan tillsammans organisera nätstyrningen oavsett vilken topologi nätet råkar ha. En följd av detta är att informationen reläas via mellanliggande radiostationer till sin destination. Ett *mobilt ad hoc-nät* är ett ad hoc-nät där alla ingående radiostationer (noder) kommunicerar trådlöst och kan röra sig godtyckligt i ett större område. I mobila ad hoc-nät kan topologin förändras hastigt efter hand som noderna förflyttas, men även i ett helt stillastående ad hoc-nät kan topologin förändras när noder slutar att fungera samt initialt när de placeras ut.

Kraven på sömlös kommunikation i mobila ad hoc-nät förutsätter ett kraftigt tekniklyft inom trådlös kommunikation. Dagens civila system som exempelvis GSM, 3G, TETRA uppfyller

inte dessa krav och det finns inte några kommersiella utvecklingsprojekt som tillgodoser samtliga dessa krav. Forskningsverksamheten inom ramen för 4G innehåller komponenter som kan möta en del av kraven. Idag ser den möjliga lösningen ut att ligga i så kallad mjukvarudefinierad radio som bygger på en öppen standard för mjukvaran i dessa kommunikationssystem (eng. software defined radio, SDR samt software communikations architecture, SCA). SDR under SCA går ut på att en generell hårdvara utrustas med mjukvara för varje kommunikationssystem som skall ingå i ett större nät. Varje kommunikationssystem representeras med en så kallad mjukvaruvågform. Strategin för aktörer inom området [91] går ut på att få internationella aktörer att enas om en öppen standardiserad arkitektur för mjukvaruvågformem i SDR-SCA. Det pågår forskningsprojekt som är inriktade på tekniken för mjukvaruradio, men den sannolikt svåraste frågan är att få fram regulativa bestämmelser för auktorisering av användning av mjukvarubaserade radiosystem. En annan olöst fråga är vilken öppen standardiserad arkitektur som de olika aktörerna kommer att enas om. Dessa båda frågeställningar bedöms inte kunna vara löst förrän tidigast inom 5-10 år.

6.9 Lägesbild

I ett framtida ledningsnätverk kommer det bli möjligt att presentera och sprida lägesbilder för en gemensam förståelse av läget till hela eller olika delar av nätverket, lokalt, regionalt och nationellt. Det kommer även att bli möjligt att skapa mer detaljerade men även mer ensade lägesbilder. En viktig fråga rör beslutsfattares behov av hur information och kunskap kan och ska representeras i lägesbilden för att funktionellt stödja gemensamma resonemang mellan aktörer från olika myndigheter i analysgrupper lokalt och regionalt? Vilka behov och krav kommer att ställas på lägesbilden för att underlätta beslutsfattares sätt att tänka, resonera och förstå i osäkra situationer samt ge dem bättre underlag för viljeinriktade beslut om åtgärder? Att fatta beslut innebär en mänsklig avsikt, en mänsklig intention. I och med detta är beslutsfattande en handling som förutom förnuftet omfattar vilja och känsla. Kognitiva uppgiftsanalyser av beslutsfattares behov och scenarier med olika typfall och målbilder kommer här att utgöra underlag och metodik samt hjälpmedel för utformning av lägesbilder för att stödja beslutsfattandet i alla dess ovan nämnda aspekter.

Skapandet av en gemensam lägesbild innebär ingen garanti för att olika betraktare, mottagare uppfattar eller tolkar lägesbilden på samma sätt. Ett vanligt hinder för en gemensam tolknig och förståelse är att olika aktörer inom olika domäner använder olika symbolspråk. Ett minsta gemensamt språk för utformning av symboler för lägespresentation är därför nödvändigt för ett ledningssystem där samverkan mellan olika myndigheter är ett krav.

Att erhålla en gemensam lägesbild för en viss situation är inte alltid eftersträvansvärt. Om vi alla har samma lägesbild, men den inte överensstämmer med verkligheten, så kan det snarast vara en belastning. Lägesbilden bör alltså vara riktig. Inte heller är det självklart att vi är betjänta av att ha en gemensam lägesbild om vi har olika uppgifter att utföra. Här uppstår en avvägning mellan att få reda på samma saker och att få reda på saker man är betjänt av för att optimera sina handlingar. Avvägningen är inte självklar, då kommunikationen mellan två befattningshavare kan underlättas av en gemensam referensram, men deras respektive agerande gentemot andra aktörer kan kräva en annan prioritering av vad som ska lyftas fram i lägesbilden. Lägesbilden bör alltså vara anpassad för den uppgift som ska utföras. Ibland kallar man detta för en rollbaserad lägesbild, ibland användaranpassad lägesbild och ibland situationsanpassad lägesbild, beroende på hur långt man har valt att gå med anpassningen.

En central insikt är att förstå att en lägesbild är objektiv i så måtto att data inte är något objektivt annat än att en lägesbild alltid har en tolkare. Hur väl en lägesbild förmedlas beror såväl på intentioner och förståelse hos tolkaren av lägesbilden samt hur kunskapsrepresentationen faktiskt utformas i lägesbilden. Det är, i strikt mening, inte möjligt att erhålla en gemensam lägesbild eftersom varje tolkare är skild från den andre. Det kan därför vara befogat att snarare tala om en konsistent lägesbild, då man avser en modell i en abstrakt beslutsrymd, som kan tjäna som underlag för beslutsfattande, agerande och kommunikation.

I grova termer kan man särskilja lägesbild från lägesuppfattning och lägesförståelse genom att karaktärisera lägesbilden som en ofullkomlig avbildning av verkligheten i tid och rum. Den innehåller objekt, relationer och aggregeringar, historia och kanske prediktering om framtiden. Lägesuppfattning kan betraktas som en tolkad lägesbild och kan innehålla värderingar, prioriteringar, och förväntningar samt prediktering om framtiden. Lägesförståelse föutsätter tidigare erfarenheter för att förstå läget. Det innebär vidare förståelse för orsakssamband, förmåga till resursvärdering och till hotvärdering. Lägesförståelse utgör underlag för agerande samt skapar förväntningar på resultat av olika aktioner.

6.9.1 Symbolers begriplighet

Hur lätt eller svårt det är att förstå en symbol och dess betydelse är beroende av vilken typ av symbol som används, men också av i vilket sammanhang symbolen används och vad symbolen representerar. Det sätt symbolen avbildas på kallas för symbolens representation. Preece m.fl. [67] anger följande huvudsakliga typer av symboler, som dock inte alltid är renodlade:

- Avbildande (ikoniska) symboler avbildar genom liknande bild med olika detaljeringsgrad t.ex. foto, skiss, schema. Ett typiskt exempel på avbildande symboler i insatsplaner är tecknet för nyckelskåp.
- Exemplifierande symboler, typiska exempel, t.ex. en kvinnosymbol för damtoalett eller uppställningsplats för brandfordon.
- Symboliska symboler, t.ex. ett glas för att symbolisera ömtåligt gods eller symbolen för brytpunkt.
- Arbiträra slumpmässiga symboler har inget utseendemässigt samband med det som representeras. Sambandet måste därför läras in, t.ex. vägmärket "lämna företräde" eller symbolen för brandpost.

Enligt Allwood och Andersen [68] kan man också tala om konventionella symboler som bygger på en gemensam uppfattning i social grupp. Storleken på sådana grupper kan vara mycket varierande och sträcka sig från mycket små grupper till mycket stora, som t.ex. hela den västerländska civilisationen. Detta kan vara problematiskt när gränssnitt skall användas i olika delar av världen, beroende på att objekt som symboler refererar till kan se olika ut i olika länder. Vanlig text kan enkelt översättas till ett annat språk, men för att översätta symboler finns det däremot ingen tradition Nielsen [69].

Införandet av nya symboler kan vara problematisk eftersom viss tid åtgår innan användaren lärt sig att använda och tolka dem på rätt sätt. Vid utveckling av datorprogram löses detta ofta genom att symboler förses med en förklarande text som visas först efter att pekaren hållits inaktiv över en symbol en viss tid. När symboler representerar abstrakta begrepp, som t.ex. varningsskyltar eller handlingar, är det svårt att skapa lättolkade avbildande ikoniska symboler, vilket medför att mer abstrakta typer av symboler måste användas. Det är lättare att minnas och

avkoda symboler när flera egenskaper (t ex färg, form, storlek, ljushet, linjelängd) skiljer dem åt.

Mycken forskning och utveckling bedrivs idag inom tredimensionell presentation. Denna presentationsform har befunnits mycket användbar för elektroniska kartor och speciellt har metodiken använts som navigeringshjälpmedel för att underlätta global översikt och planering under färd. Perspektivpresentation har dock inte befunnits lämplig för att ge uppfattning om exakt läge eller hur felaktigt läge bäst kan korrigeras [70], [71], [72].

Ett antal omgivnings- och situationsfaktorer (s.k. stressorer), faktorer, försämrar människans förmåga att bearbeta information. Sådana faktorer kan vara kan sömnbrist, trötthet, olämplig tid på dygnet, hot, rädsla, alltför hög lufttemperatur, otillräcklig syretillförsel, buller och tidsbrist. Stressorer kan påverka vakenheten ("arousal"), som i sin tur har en mycket central betydelse för perceptuell och tankemässig förmåga. För låg vakenhet sänker förmågan att uppfatta perceptuell information och snabbt reagera på den. För hög, å andra sidan, kan försämra förmågan att tänka logiskt, att analysera komplicerad information och att lösa problem. Människan har till en viss gräns en kompensatorisk förmåga och kan avhjälpa trötthet med ökad ansträngning och exaltation med fokusering, vilket kan leda till så kallat tunnelseende. Sedan länge har man känt till tunneleffekten, som innebär att höga stressnivåer kan "snäva in" den visuella uppmärksamhetsförmågan. Stress kan dels försämra synfältsbredden, vilket kan leda till att man inte varseblir perifer information. Stress kan också göra att visuell uppmärksamhet blir alltför mycket styrd av ytliga egenskaper (iögonfallande färg, form) och att mer subtila aspekter, som kan ha betydelse, inte bearbetas. Det är därför av avgörande betydelse att färg och symbolik i lägesbilden har en utformning, som samstämmer med innehållslig relevans.

6.9.2 Lägesbildens innehåll och funktionella betydelse

För en noggrann och seriös utformning och utvärdering av lägesbilden rekommenderas:

- uppgiftsanalys av de krav krishanteringssystemet ställer,
- uppgiftsanalys av samverkansansvarigas funktioner i ledningsystemet samt
- uppgiftsanalys av hur lägesbilden kan tänkas påverka de samverkansansvarigas beteenden och funktioner utifrån de krav krissituationen ställer.

Uppgiftsanalys [73] är en övergripande term för att identifiera och utvärdera uppgifter avsedda att utföras av människor i deras samverkan med tekniska system. Mer i detalj syftar en uppgiftsanalys till att beskriva alla de krav och uppgifter i termer av handlingar och kognitiva processer, som krävs för att en människa (operatör, flygförare, räddningsledare etc.) eller en grupp människor (operatörer, flygförare, räddningsledare etc.) ska uppnå de mål som systemet ställer. Med system i detta sammanhang avses allt från enkla till mycket komplexa människa- maskin/datorsystem. Litteraturen inom detta område är omfattande. För att identifiera de kritiska kognitiva elementen i arbetsuppgifter som kräver bedömningar, beslutsfattande och värderingar har olika metoder för "kognitiv uppgiftsanalys" utvecklats. Mest känd är kanske den sk ACTA-metoden (ACTA= Applied Cognitive Task Analysis) [74], [75], [76]. Studier av beslutsfattande hos militära chefer men även hos räddningsledare och kommunchefer har studerats under fältövningar, i ledningsträningsanläggningar, och i spel och studier [77]. Metoden har även använts vid design av nya ledningskoncept men även för att definiera utvärderingskriterier av militär taktisk ledning och kommunal räddningsledning [78], [79].

6.10 Databrytning

Både i ett operativt och ett preventivt skede kommer de flesta ledningssystem att tillföras stora datamängder. Man kan också vara säker på att utvecklingen kommer att resultera i ett över tiden ökande behov av data. Detta som en konsekvens av att fler och fler sensorer och andra datakällor kommer att anslutas till ledningssystemen samt att de ökande kraven i sin tur kommer att leda till behov av allt mer data. Härvid uppstår frågan om hur dessa data skall bearbetas och sammanställas så att användaren kan dra nödvändiga slutsatser ur den information som på detta sätt görs tillgänglig. I vissa fall är detta inte så svårt eftersom man har den nödvändiga kunskapen och vet sina behov. I andra sammanhang är bilden mindre klar eftersom den sökta informationen är mera spridd inom oklara informationsgränser där de data som behöver genomsökas är mycket omfattande och frågeställningarna oklara. Situationen kompliceras också av att det som man i första hand är intresserad av ligger dolt i olika trender vilka inte framgår explicit av materialet. Det som gör situationen än mer komplicerad är att dessa trender kan återspegla processer som förändras över tiden, vilket i sin tur medför att data som behöver berarbetas ökar ytterligare. Denna typ av trendförskjutningar är emellertid mycket intressanta och kan mycket väl innehålla informationsfragment av stor betydelse vid hotanalys. De tekniker som kommer till användning för att vaska fram denna typ av information kallas vanligen databrytning (eng data mining) [65]. Med databrytning menas att man med olika former av sökmotorer försöker hitta så kallade associationsregler med vars hjälp man kan identifiera olika mer eller mindre komplicerade samband som råder mellan olika objekt.

Situationer där databrytningsmetodiker kan komma till användning kan således vara i sammanhang där ett stor inflöde av data äger rum kontinuerligt. Dessa data kan emanera från datakällor av varierande slag. De kan också vara av heterogen typ och bestå av t ex tal, text eller bilder. Informationen kan också vara av varierande slag, såsom rumslig och/eller temporal information. Konsekvensen av att data kan vara av heterogen typ innebär att en mängd olika metoder för analys av inkommande data blir nödvändig för att i någon mån kunna homogenisera data. Detta för att göra det möjligt att effektivt kunna genomföra nödvändiga sökningar. Dessutom kommer det i slutändan också att bli nödvändigt att kunna fusionera data på lämpligt sätt.

Redan idag finns goda exempel på aktiviter där dataflödet är av en art som kan göra det angeläget att utnyttja metodik för databrytning. Exempel kan vara teletrafiken till SOS-Alarm och olika ledningscentraler, såväl polisiära som militära. Andra exempel kan avse centraler för trafikövervakning både till sjöss och i luften, men även på marken. Huvudsyftet måste i dessa fall vara preventivt och målsättningen att identifiera situationer som kan utgöra hot eller troligare fragment av hot som kan tolkas i skenet av andra fragment. Det kommer därför att bli nödvändigt att även hitta relationer och samband mellan olika fragment för att skapa längre kedjor som tydligare kan associeras till framväxande hot. Exempel på litteratur som belyser användningen av databrytning i anslutning till tillämpningar relaterade till operativa aspekter på såväl krishantering som säkerhet återfinns i [66]. Det är ganska entydigt att detta problemområde är komplext och innehåller många svårigheter som måste bli föremål för omfattande forskningsinsatser i anslutning till ett ledningssystem för krishantering.

6.11 Sensemaking

Sedan 11 September 2001 har begreppet *sensemaking* kommit att framstå som ett viktigt område för forskning inom krishantering trots att området inte är särskilt väl avgränsat. Sensemaking definieras som processen att skapa förståelse och situationsmedvetande i osäkra situationer. Sensemaking spänner över många forskningsområden. En stor del av forskningen inom

tillämpad psykologi relaterad till sensemaking har sina rötter i ”systems engineering” och ”human factors”.

Även före 11 september insåg man i USA att det nätverksbaserade försvaret kräver djupare kunskap och förståelse om vad som kan kallas sensemaking, en forskning man anser behövs som tillägg till den traditionella fokuseringen på informationsteknologin (med fokus på hur information kan insamlas, lagras och presenteras). Framförallt ansåg man sig behöva ha förståelse för hur sensemaking inom ledningssystem sker på både individ – och organisationsnivåer och för vad informationen innebär i förhållande till mänskliga målsättningar, kunskap, expertis, känslor, övertygelser, värderingar och kulturella erfarenheter.

Resultaten från studier av sensemaking i USA är visserligen preliminära men stöder argumenten att forskning inom ledningsområdet bör öka sin inriktning mot sensemaking. För att få förståelse för den roll sensemaking spelar för militära framsteg eller misslyckande utfördes en retrospektiv analys av 30 historiska militära slag, uppror, terroristattacker och andra incidenter, som innehöll 149 specifika beslutshändelser. Av dessa kunde 60 st relateras till militär seger och 89 till militära nederlag.

Genom att använda begreppsapparaten för sensemaking kunde man genom subjektiva analyser ta fram nio grupper av faktorer av betydelse för hur beslut togs och som var starkt relaterade till sensemaking:

1. *Information system input* (were the right data collected and correlated, placed in context, and put in a form that facilitated awareness?)
2. *Situational awareness* (was situation awareness developed and shared?)
3. *Cognitive factors* (were emotions, beliefs, cognitive factors, prior knowledge, and mental models used or taken into account?)
4. *Understanding* (was shared awareness of situation correctly understood?)
5. *Sensemaking* (was sense made of the situation?)
6. *Decision effectiveness* (was a workable decision made?)
7. *Command intent* (was command intent developed collaboratively?)
8. *Plan* (was a quality plan developed?)
9. *Execution* (were the decisions and driving factors shared, and was the plan executed effectively?)

Analys av data visade att beslutsfattarna i allmänhet presterade väl i informationsdomänen men att mest avgörande för hur besluten fattades i de lyckade uppdragen var om förståelse och medvetenhet uppnåtts och detta var faktorer förknippade med sensemaking, dvs kognitiva faktorer [75].

6.12 Logistik

Forskning avseende informationssystem för logistiktillämpningar måste i första hand vara inriktade på utveckling av den grundläggande funktionaliteten i systemet. Till sådan funktionalitet måste även här metodik för insamling, analys, lagring samt hantering av data från olika datakällor räknas. I stor utsträckning kommer dessa datakällor att bestå av sensorer av många olika typer. Vidare kommer beslutsstödshjälpmedel att behöva utvecklas för olika användarkategorier på olika nivåer i systemet. Detta eftersom vi här diskuterar en metodik som kan arbeta på flera olika organisatoriska/logiska nivåer och med varierande upplösning. Av vikt är

också att man integrerar beskrivningar av de objekt som skall hanteras av informationssystemet, t ex fordon, etc. Detta kan ske på flera olika sätt men i detta förslag tänker vi oss användning av någon form av ontologi, se nedan. Emellertid kommer givetvis andra typer av mer eller mindre komplexa delsystem att behöva integreras för att erhålla ett kraftfullt och välfungerande system.

Moderna IT-system för logistiktillämpningar måste innefatta olika former av beslutsstödshjälpmedel med vars hjälp användaren kan lösa olika arbetsuppgifter. Till systemet måste olika typer av heterogena datakällor och databaser kunna anslutas. Till stöd för detta kan en ontologi, kompletterad med ett regelbaserat kunskapssystem, utnyttjas. En ontologi utgör en struktur som kan användas för att beskriva objekt som skall hanteras i systemet. Vid sidan av dessa beskrivningar kan även deras egenskaper och relationer beskrivas. Generellt sett består ontologier av hierarkiska strukturer som kännetecknas av att egenskaper som är gemensamma på olika nivåer i hierarkin kan ärvas av objekt på lägre nivåer. En ontologi kan således vara mycket komplex. Trots sin komplexitet kan en ontologi ändå vara en lämplig struktur för att beskriva objekt som skall hanteras i ett logistiksystem. Detta därför att logistik för tillämpningar relaterade till krishantering omfattar ett mycket stort antal både enkla och komplexa objekt. Av denna anledning måste det finnas metoder som kan hantera dessa objekt på ett adekvat sätt.

Ofta krävs det i logistik tillämpningar att man kan hantera lägesbunden information. För dessa ändamål används oftast geografiska informationssystem (GIS). GIS är nödvändiga i de flesta logistiktillämpningar. Detta har sin grund i att man i dessa tillämpningar måste kunna hantera både rumslig och temporal information.

Simulering av logistikstödet kan komma att bli nödvändigt när komplexa tillämpningar är för handen. Speciellt om ett mer fullödigt system anpassat för nätverksmiljö skall utvecklas.

6.13 Träning och utvärdering

"Grunden för samhällets förmåga att hantera kriser av skilda slag är att det finns välutbildade och motiverade människor som kan och vill genomföra insatser." [97]

En viktig del i förmågan att hantera kriser och svåra belastningar är att ha möjlighet att träna, kunna utnyttja och lära av de erfarenheter som erhålls. Att få ut ett så stort mervärde som möjligt av de erfarenheter som införskaffas av personalen, både då det gäller verkliga insatser och kontrollerade övningar, är centralt för att kontinuerligt förbättra och effektivisera verksamheten. Krishantering innefattar dock situationer som är svåra att överblicka och i efterhand analysera. Detta gäller speciellt vid skarpa insatser, men även vid övningar. Frågor som behöver besvaras är; vilka var de kritiska momenten, var och när ägde de rum, samt vem som gjorde vad och varför?

Vid Institutionen för systemutveckling och IT-säkerhet vid FOI har en metod kallad MIND-metoden [67] tagits fram för att kunna stödja uppföljning av distribuerade taktiska insatser. Metoden syftar till att rekonstruera och utforska de komplexa händelseförlopp som insatsen utgör. Rekonstruktionen innefattar en domänanalys för att fastslå de frågeställningar som skall undersökas och som ger en modell över de objekt, händelser och aktörer som är centrala för frågeställningarna. Utifrån modellen sker en instrumentering för att sätta upp de metoder och tekniker som behövs för att samla in data. Det sista steget i rekonstruktionen är datainsamlingen då all data inhämtas enligt instrumenteringen och infogas i den framtagna modellen. Ett

stort antal olika datakällor kan används: observationsprotokoll, kommenterade fotografier och video, positioner och förflyttningar, radio- och datakommunikation, skadeflöde etc.

I utforskningsskedet används ett ramverk, datorstöd, för att presentera insatsmodellens data. Insatsmodellen är händelsedriven, tidssynkroniserad, uppspelningsbar och multimedial. Presentationsramverket innehåller ett flertal vyer som kan presentera olika typer av data från de olika källorna. Dessa vyer syftar till att ge en gripbar bild över insatsen som ett underlag för analys. Analysen stöds dessutom av olika verktyg som kan filtrera, navigera bland och på andra vis hantera data. Användare av datorstödet kan bland annat titta på speciella sekvenser, snabbspela moment, zooma in på detaljer och ställa frågor genom direktmanipulation. Analysprodukter, som till exempel uppkomna frågor, reflektioner eller hypoteser, återförs också till datamodellen och är spårbart kopplade till de specifika situationer de upptäcktes i.

Denna metod har använts både för att analysera övningar och skarpa situationer, för att utvinna kunskap för att öka förståelsen av insatser och därigenom erhålla ökad effektivitet. Nya komponenter till presentationsramverket tas fram kontinuerligt allteftersom nya frågeställningar och domäner tillkommer. Denna utbyggbarhet är central i MIND-metoden.

6.14 Geoinformatik

Geoinformatik omfattar metoder för hantering av både rumslig och temporal information som oftast kommer till användning i geografiska informationssystem. I ett ledningssystem för krishantering framstår det klart att användning av denna typ av information kommer att vara väsentlig och att metoder för analys av rumslig information kommer att utgöra en central del vid krishantering. Emellertid kommer detta inte att medföra att man inom ramen för ett forskningsprojekt av den typ som diskuteras här kommer att behöva utveckla ett speciellt GIS. Däremot kommer olika metoder för analys av både rumslig och temporal information att behöva utvecklas med hjälp av redan existerande system. Användning av geografisk information kommer med stor säkerhet också att behöva kombineras med andra typer av rumslig information såsom t ex sensordata. I ett ledningssystem för krishantering måste det därför vara möjligt att hantera geografisk information för en mängd olika tillämpningar. Till exempel har redan logistik diskuterats ur detta perspektiv. Således kommer ett beslutsstöd med en rumslig temporal förmåga att spela en central roll vid ledning i samband med krishantering.

7 Förslag till ledningsfunktion för krishantering i lokalsamhället

Det huvudsakliga syftet i detta kapitel är att ge en kort beskrivning av en lämplig tillämpning för det förslag till ledningsfunktion för krishantering som varit målsättningen med denna förstudie. I detta sammanhang har studiegruppen enats kring följande grundläggande antagande som måste utgöra grunden för den fortsatta forskningsverksamheten:

- För att en ledningsfunktion skall vara nyttig bör den kunna användas även då kris inte råder.
- Av denna anledning måste ledningsfunktionen kunna anpassas till den dagliga verksamheten.
- Ledningsfunktionen måste ha kapacitet för hantering av extraordinära händelser.
- Människan måste spela en central roll i ledningsfunktionen.

Ytterligare några andra aspekter är att man redan från början av själva utvecklingen av ledningssystemet *måste* ta hänsyn till en mängd olika faktorer såsom *IT-säkerhet, beslutsstödsfunktioner, systemstrukturfrågor, systemarkitekturer*. Detta med hänsyn till den höga komplexitets- och generaliseringsgraden som gäller.

FOI har stor erfarenhet av att bedriva breda forskningsprojekt och är väl rustat för att bedriva forskning syftande till att utveckla ett system för en så omfattande tillämpning.Vidare ligger det också resultatmässigt ett *mervärde* i forskningsprojekt med bred inriktning d v s projekt med multidisciplinära inslag.

7.1 Tillämpningsförslag

Området ledningsfunktion för krishantering är i sig mycket omfattande och i ett forskningsprojekt med denna inriktning kommer flera relativt omfattande begränsningar att bli nödvändiga för att projektet inte skall svälla ut till en omfattning som blir omöjlig att hantera. Å den andra sidan kan inte dessa begränsningar vara för snäva eftersom detta då kan leda till alltför triviala frågeställningar. Mot denna bakgrund har projektgruppen beslutat att det är lämpligt att primärt studera vad som valts att kallas *det lokala samhället.* Med detta begrepp avses den del av samhället som kan omfatta en eller möjligen ett fåtal kommuner. I dessa kommuner skall det finnas några viktiga skyddsvärda objekt som kan knytas till den aktuella tillämpningen. För att genomföra ett projekt med sådan omfattning kommer kontakter med en eller två kommuner, samt med ansvarig länsstyrelse, att bli nödvändiga. Dessa organisationer kan härvid agera som referensgrupp och på andra sätt bidra till att göra det möjligt att genomföra tester och demonstrationer som kan vara av intresse även för Krisberedskapsmyndigheten. Vid sidan av dessa intressenter finns naturligtvis även andra verk och myndigheter som kan komma att delta; detta beroende på vilka skyddsvärda objekt som kan bli aktuella. Lokal industri med intressen för den angivna problematiken kan på sikt också bli viktiga partner till FOI. Dessutom kan det bli nödvändigt att även knyta andra forskningsorganisationer (främst universitet och högskolor, men även speciella forskningsinstitut kan komma i fråga) med speciell kompetens till projektet.

Enligt vad som nämnts ovan är det av stor betydelse att ledningsfunktionen skall fungera även under normala omständigheter för att sedan vid behov omvandlas till ett mer kraftfullt instrument för ledning när en kris inträffar. Det huvudsakliga motivet för ett sådant synsätt är självklart att man vill att olika användare skall besitta tillräckligt stor vana vid systemet så att det

blir naturligt för dem att använda det när en kris inträffar. Exempel på områden som lämpar sig för detta kan vara:

- sjukdomar; registrering och övervakning (t ex virussjukdomar),
- miljöfaktorer (t ex luftkvaliteten),
- transporter av farligt gods; kontroll och övervakning,
- kriminella aktiviteter,
- bränder.

De flesta exemplen ovan har potential för att både enskilt och i kombination med någon av de övriga kunna utvecklas till olika typer av kriser.

I anslutning till bekämpning av kriser i ett operativt sammanhang behövs också studeras den preventiva aspekten. Detta kan göras som en del av övervakningsprocesserna för något eller några skyddsvärda objekt. Exempel på skyddsvärda objekt som skulle kunna hanteras här är:

- flygplatser (extern och/eller intern övervakning),
- hamnar (extern och/eller intern övervakning),
- kärnkraftverk (extern övervakning),
- infrastrukturer, t ex för el-överföring.

En lämplig region för den föreslagna inriktningen skulle kunna vara Östergötlands län, t ex i anslutning till Linköpings och/eller Norrköpings kommun.

7.2 Primära forskningsfrågor

I detta avsnitt diskuteras forskningsfrågor av speciell vikt för den föreslagna inriktningen som framgår av avsnitt 7.1.

7.2.1 Arkitektur som grund för nätverksbaserad krishantering

Kriser är företeelser som i mycket hög utsträckning är nästintill omöjliga att förutse, gällande såväl typ kris som när och exakt var de kommer att drabba ett samhälle samt dess konsekvenser. Men tanke på att samhällets resurser inte är obegränsade finns inte förutsättningarna att bygga ett enda monolitiskt storsystem för att hantera alla tänkbara varianter av kriser. I stället behövs ett flexibelt system som vid behov kan sättas samman av befintliga resurser och verksamheter och som kan anpassas till krisens art och omfattning. Detta kräver ett systemtänkande, där system kan integreras med andra system. För att dessa system ska kunna fungera enskilt och tillsammans med andra system krävs en gemensam arkitektur. En etablerad arkitektur för krishantering skapar förutsättningar för flexibilitet och möjlighet att anpassa verksamheten efter behov och förutsättningar. Den ökar även förutsättningarna för en mer friktionsfri interorganisatorisk samverkan, där många aktörer från bl a räddningstjänst, polis och hälso- och sjukvård ingår.

I det föreskrivna projektet avses en arkitektur för krishantering att utvecklas. Denna arkitektur skall omfatta samtliga former av system, såväl tekniska som organisatoriska. En utgångspunkt skall tas i de koncept framtagna inom FMA [75], som bedöms vara väl genomarbetade. Detta inkluderar tjänstebegreppet, principen system-av-system och de sex initiala systemperspektiven. Arkitekturen kommer under hela projektet att utvärderas mot nya forskningsrön och empiriska tillämpningar. Dessa utvärderingar kommer att ligga till grund för den vidareutveckling och de kompletteringar av arkitekturen som kommer att genomföras. Målet är också att

skapa underlag för en nationell arkitektur, som underlättar och möjliggör en ökad samverkan mellan olika myndigheter, verksamheter och andra organisationer i samhället.
Forskningsfråga: Hur skall en generell och heltäckande arkitektur för krishantering se ut? Den skall skapa förutsättningar för att integrera samhällets resurser flexibelt så att dessa genom samverkan kan nyttjas som en välanpassad insats vid krissituationer. Arkitekturen skall även stödja nyutveckling av enskilda nätverksbaserade system och integrationen av redan befintliga system så att dessa blir kompatibla med övriga system i den nätverksbaserade krishanteringen. Ett led i utformningen av denna arkitektur är att identifiera de krav som kommer att ställas på en sådan arkitektur. Detta kräver en förståelse för de system som ingår i krishanteringen. Arkitekturen måste utvecklas på ett sådant sätt att den blir funktionell för samtliga berörda aktörer.

7.2.2 Systemutvecklingsmodell för nätverksbaserad krishantering

Arkitekturen skall inte enbart ligga till grund för att beskriva befintliga system, utan nya system som följer principerna givna i arkitekturen skall också kunna skapas. För att utveckla nya och vidareutveckla befintliga system i enlighet med arkitekturen krävs en modell för systemutveckling. Denna systemutvecklingsmodell måste vara generell nog att passa samtliga inblandade intressenters syften och förutsättningar, samtidigt som den måste vara enkel och entydig att använda. Utgångspunkten för denna modell tas i det arbete som under en längre tid drivits vid FOI med att integrera ett flertal standarder, teorier, metoder och ”best-practice” till en modell, VUM-LS. Modellen kommer under projektet kontinuerligt att förfinas och utvecklas. Initialt kommer modellen att användas för att skapa grunden för en nätverksbaserad krishantering, men under projektet kommer den att anpassa till en metod som kontinuerligt används för att skapa och integrera nya förbättrade system.

*Forksningsfråga***:** Hur skall en modell för systemutveckling inom krishantering se ut?

7.2.3 IT-säkerhet

Omfattande informationssystem som innehåller känslig information fordrar väl genomarbetade säkerhetslösningar. I enlighet med resonemang i *avsnitt 6.2 Systemutveckling* kräver detta förståelse för systemens omgivning, i vilket exempelvis ingår legala förutsättningar och systemägare, samt samordning mellan kravhantering och IT-säkerhetsfunktioner. Detta är en förutsättning för kostnadseffektiva säkerhetslösningar av hög kvalité och i förlängningen för att uppnå tilltro till system.

För att nå fram till dessa mål ser vi ett tydligt behov av säkringsbara system, d v s system som kan säkras under drift. Design av säkringsbara system kan delas upp i tre huvudprocesser:

- kontextuell modellering,
- hantering av säkerhetskrav, och
- implementering av säkerhetskrav.

Alla tre huvudprocesserna löper under hela systemets livscykel och det finns beroenden och överlapp mellan dem. Detta ger en dynamisk design, vilket torde vara en fördel för dynamiska och anpassningsbara system med höga säkerhetskrav. Samtliga huvudprocesser inrymmer också ett antal relevanta forskningsfrågor, vilka kräver adekvata lösningar för att uppnå den nivå av informations- och IT-säkerhet man bedömer som rimlig.

Ur informations- och IT-säkerhetssynvinkel speciellt viktiga forskningsfrågor:

Hur skall metoder för hantering av säkerhetskrav utvecklas?
Hur interagerar dessa med motsvarande metoder för andra systemkrav, d v s systemutvecklingsprocessen i stort?
På vilket sätt påverkar IT-säkerheten, eller systemets IT-säkerhetsnivå, tilltron till systemet och vice versa?
Hur bör risk- och ledningsmodell påverka modellering av informations- och IT-säkerhet i ledningssystem för krishantering och vice versa?

7.2.4 Beslutsstöd

Olika typer av beslutsstöd kommer att spela en central roll i den ledningsfunktion som har skisserats här. Ett relativt stort antal varianter kommer att behöva utvecklas för att göra det möjligt att lösa några av de ur forskningssynpunkt viktigaste uppgifterna som uppstår i samband med krishantering. Mot denna bakgrund måste frågan resas om vilka av dessa som kommer att bli primärt nödvändiga. Dessutom måste man på något sätt göra de flesta av dessa delsystem så generella att de kan användas för flera olika problem och situationer. I detta sammanhang gäller speciellt att ett stort antal problemområden kommer att behöva hantera rumslig/temporal information av geografisk natur. Detta innebär att de flesta beslutsstöd måste ha stöd av någon typ av GIS. Till detta kommer att data från de flesta indatakällor, förutom att de kommer att utgöras av rumslig och i många fall också av temporal information, kommer att kräva ett stort antal metoder för analys och fusion. Det senare kommer naturligtvis att öka komplexiteten i systemen samtidigt som kraven på hög effektivitet kommer att vara stort. Sammanfattningsvis, forskningsinsatserna inom detta delområde kommer att bli omfattande. På ett mer konkret plan kan ett antal olika instrument för stöd till beslutsfattare identifieras och som kan komma att spela en viktig roll sedan lämpliga avgränsningar gjorts i anslutning till detta projektförslag. Till dessa hör frågespråk, stöd för databrytning etc.

7.2.5 Användargränssnitt

I anslutning till ledningsmodellen och dess funktionalitet ligger också frågan om hur det visuella användargränssnittet och den till detta delsystem anslutna lägesbilden skall vara designad. Detta problemområde kräver givetvis speciella forskningsinsatser och bör utredas speciellt och i kombination med ledningsmodellen och dess struktur.

8 Relaterad forskningsverksamhet

En litteratur studie med ansikten att undersöka om det pågår någon verksamhet på internationell nivå som berör utveckling av ledningssystem för krishantering har också genomförts. I detta sammanhang exkluderas emellertid alla typer av ansatser syftande till utveckling av militära ledningsystem. Det visar sig att det för närvarande inte pågår någon mer omfattande forskningsverksamhet med denna inriktning. Anledningen till detta kan troligen hänföras till att man på skilda håll inte ännu kommit igång med denna typ av forskning i någon större omfattning. Troligt är dock att man inom några få år kommer att kunna se en ökad aktivitet med denna inriktning.

I ett arbete av Graser m fl [108] beskrivs ett system kallat ENCOMPASS där huvudsyftet är att stödja beslutsfattare som befinner sig i ledande position vid krissituationer, t ex vid terrorist attacker. I detta system får användaren stöd av typen kartbaserad situationsanalys, checklistor för stöd i situationsanalysen och epidemiologisk övervakning. Detta arbete har finansierats av DARPA.

Ett annat arbete av intresse beskrivs av Rodrigues m fl [109]. I detta arbete utvecklas ett system som kallas Mercury. Även i detta system är huvudsyftet att ge stöd till beslutsfattare och att i detta sammanhang också integrera data från andra system som kan vara olika typer av kriskontrollcentra. Detta system har ett militärt ursprung. En av de centrala forskningsaspekterna utgör arbetet med att utveckla en lämplig arkitektur för ledning vid krishantering.

Modrik [110] beskriver i sitt arbete ett system kallat PRESTO. Detta system är av något äldre datum än de både ovanstående och går tillbaka till tiden före den 11 september. I PRESTO fokuserar man på de mänskliga aspekterna i ett distribuerat system för ledning i krishantering där samverkan spelar en central roll. Även i detta arbete är en huvudinriktning att ta fram en passande arkitektur där också olika typer av multimedial information skall kunna hanteras.

En faktor som kan nämnas i detta sammanhang, och som inte diskuteras i något av de ovan nämnda arbetena, utgör problem relaterade till data- och IT-säkerhet. En annan aspekt som inte heller berörs är t ex hantering av olika datakällor, t ex sensorer. Bland andra arbeten med delvis gemensam inriktning kan nämnas [111] som diskuterar modellbaserad planering för stöd till ledning. I [112] diskuteras ett grafiskt användargränssnitt som primärt utvecklats för militära ledningssystem men med tillräcklig generalitet för att kunna användas även för andra tillämpningar.Wohlever m fl [113] beskriver ett ledningssystem för realtidstillämpningar. Slutligen finns också ledningssystemarbeten inriktade mot katastrofhantering som har viss släktskap med ledningsystem i krishantering; exempel på ett sådant arbete är [114] som fokuserar mot ett s k C^3-system dvs ett system för *command, control and communication*.

Referenser

[1] Fortsatt förnyelse av totalförsvaret, Prop 2001/02:10.

[2] Samhällets säkerhet och beredskap, Prop 2001/02:158.

[3] Staden på vattnet utan vatten, Delbetänkande inom Hot- och riskutredningen, SOU 1995:21.

[4] Störtflod i Dalälven, Räddningsverket, 1996.

[5] Ett säkrare samhälle. Huvudbetänkande från Hot- och riskutredningen, SOU 1995:19.

[6] Gasmoln lamslår Uppsala, Delbetänkande inom Hot- och riskutredningen, SOU 1995:24.

[7] Comfort, L. K., *Complex Systems in Crisis: Managing response to Extreme Events*, Proceedings of the International Emergency Management Society 9th Annual Conference, 2002, Universuty of Waterloo, Canada, sid. 565-579.

[8] Eriksson, Ö., *Ledning av informationsförsörjning - en allt viktigare uppgift i framtiden*, KKrVAHT, 1999, 5: sid, 23-31.

[9] Foss, J.W., *Command*, Military Review, (January-February), 1997, sid. 65-70.

[10] Försvarsberedningen, *Ny struktur för ökad säkerhet: nätverksförsvar och krishantering*, Försvarspolitisk rapport från Försvarsberedningen, 2001.

[11] Wishart, L.P., *Leader development and command and control*, Military Review, 1997(January-February): sid. 62-65.

[12] Worm, A., Jenvald, J. and Morin, M., *Mission Efficiency Analysis: Evaluating and Improving Tactical Mission Performance in High-Risk*, Time-Critical Operations, Safety Science, Vol. 30, Nos. 1/2, 1998, Elsevier Science B.V., The Netherlands, pp.79-98.

[13] Worm, A., *On Control and Interaction in Complex Distributed Systems and Environments*, Linkoping Studies in Science and Technology, Dissertation No. 664, Linkoping University, Linkoping, Sweden, 2000.

[14] Worm, A., *Skogsbrand eller militär operation - sättet att leda är ofta detsamma*, FOA-tidningen nr 5, november 2000, sid. 28 - 30.

[15] Worm, A., *On Systems Analysis and Performance Assessment in Complex, High-risk Work Environments*, Int. J. Risk Assessment and Management, Vol. 2, Nos. 3/4, 2001, pp.276-287. Inderscience, United Kingdom.

[16] Worm, A., *Rätt information viktig vid katastrofsituationer*, Vetenskapsrådets tidning Vetskap, 103 78 Stockholm, 2001.

[17] Worm, A., *An Integrated Framework for Information-Centered Human-Machine Systems Analysis*, Int. J. Emergency Management, Vol. 1, No. 2, 2002, Inderscience, United Kingdom, pp.125-143.

[18] Brooks, F. P. Jr. (1995). The Mythical Man-Month: Essays on Software Engineering. Addison-Wesley.

[19] Chaos (Måste kola upp denna)

[20] Hallberg, N. (1999) *Incorporating User Values in the Design of Information Systems and Services in the Public Sector*, Linköping Studies in Science and Technology, Dissertation No. 596.

[21] Sommerville, I. (2001) *Software engineering*, 6. ed. Harlow : Addison-Wesley.

[22] Kotonya, G. & Sommerville, I. (1998) *Requirements Engineering. Processes and Techniques*, John Wiley & Sons, Wichester.

[23] Young, R. (2001) Effective Requirements Engineering. Addison-Wesley.

[24] Hofmann, H. F. & Lehner, F. (2001) Requirements Engineering as a Success Factor in Software Projects, *Software*, IEEE, Vol. 18, July-Aug. Issue, s. 58-66.

[25] Karlsson, J., Wohlin, C., & Regnell, B. (1998). An Evaluation of Methods for Prioritizing Software Requirements, *Information and Software Technology*, 39, 939-947.

[26] Avison, D. E. & Fitzgerald, G. (1995) *Information Systems Development: Methodologies, Techniques and Tools*, The McGraw-Hill Companies.
[27] Bosson, E & Svensson, E (2001) *Krav på användbarhet – Att relatera användbarhet till funktionalitet vid kravspecificering*, FOI-R—0252, SE, Linköping.
[28] Kotonya, G. & Sommerville, I. (1998) *Requirements Engineering. Processes and Techniques*, John Wiley & Sons, Wichester.
[29] Nielsen, J. (1993) *Usability Engineering*, Academic Press, Boston, MA.
[30] Gulliksen, J. & Göransson, B. (2002) *Användarcentrerad systemdesign*, Studentlitteratur, Lund.
[31] Cockburn, A. (2001) *Writing Effective Use Cases*, Addison Wesley, Reading, MA
[32] Jacobson, I., Booch, G. & Rumbaugh, J. (1998) *The Unified Software Development Process*, Addison Wesley, Reading Massachusetts.
[33] ISO/IEC 15288 (2002) *System Engineering – System Life Cycle Processes, ISO/IEC CD 15288 FCDIS*, Version 4.
[34] ISO/IEC 13407 (1999) *Human-centered Design Processes for Interactive Systems*, International Standard
[35] ISO 18529 (2000) *Ergonomics – Ergonomics of Human-system Interaction – Human-centred Lifecycle Process Descriptions*, Technical Report.
[36] *OMG Unified Modeling Language Specification* (2001), Version 1.4.
[37] R. C. Gonzalez and R. E. Woods. *Digital Image Processing*. Addison-Wesley, 2002.
[38] J. Karlholm, M. Ulvklo, S. Nyberg, A. Lauberts, and A. Linderhed. A survey of methods for detection of extended ground targets in EO/IR imagery. FOI Scientific Report FOI-R—0892—SE, 2003.
[39] J. Karlholm, M. Ulvklo, J Nygårds, M. Karlsson, S. Nyberg, M. Bengtsson, L. Klasén, A. Linderhed, and M. Elmqvist. The target detection and tracking processing chain. FOA User Report FOA-R—00-01767-408,616—SE, 2000.
[40] H. Sidenbladh. Detecting Human Motion with Support Vector Machines. Submitted to *IAPR International Conference on Pattern Recognition*, 2004.
[41] Feng Zhao and Leonidas Guibas, editors. Proc. Second Int. Workshop on Information Processing in Sensor Networks (IPSN 2003), Palo Alto, California, 22-23 April, 2003.
[42] Special Issue on Sensor Networks and Applications, Proceedings of the IEEE, 91(8), August 2003.
[43] Special Issue on Collaborative Signal and Information Processing in Microsensor Networks, IEEE Signal Processing Magazine, March 2002.
[44] Erland Jungert et al., *From Sensors to Decision - Towards improved awareness in a network centric defence*, FOI-R--1041--SE, December 2003.
[45] Hall, D.L., & Llinas, J. (Eds.)., *Handbook of Multisensor Data Fusion*, CRC Press, New York, 2001.
[46] Jensen, F. V., *An Introduction to Bayesian Networks*, Springer Verlag, New York, 1996.
[47] Yager, R., Fedrizzi, M., & J. Kacprzyk (Eds.), *Advances in Dempster-Schafer Theory of Evidence*, John Wiley and Sons, New York, 1994.
[48] Salvendy, G. (Ed.), *Handbook of human factors and ergonomics* (2nd ed) New York: Wiley, 1997.
[49] Derefeldt, G.., Swartling, T., *Armstrong Lab, NASA Ames Research Center, Electronic Imaging: Science & technology - En reserapport*, FOA-R-94-00049-5.2-SE. Stockholm, Försvarets Forskningsanstalt, 1994.
[50] GARTEUR (Group for Aeronautical Research and Technology in Europe), Final Report for GARTEUR Flight Mechanics Action Group FM AG 13, GARTEUR Handbook of Mental Workload Measuremet, GARTEUR Action Group FM AG 13, 2003.

[51] Booher, H. R. (Ed.), *MANPRINT - An Approach to Systems Integration*, New York, Van Nostrand Reinhold, 1990.
[52] *MANPRINT in acquisition: A handbook,* Prepared by office of the deputy chief of staff for personnel. Personnel Technologies Directorate 300 Army Pentagon, Washington DC, 2000, URL:http://www.manprint.army.mil/manprint/references/handbookacquis/handbookacq.htm (2000-10-19).
[53] ISO 13407, *Human-centred design processes for interactive systems*, Geneve, ISO, 1999.
[54] ISO 9241 - 11, *Ergonomics requirements for office work with visual display terminals (VDTs)*, - Part 11, Guidance of usability, 1998.
[55] Woods, D. D., Roth, E. M., *Cognitive engineering: Human problem solving with tools*, Human Factors, 30(4), 1988, pp 415-430.
[56] Woods, D. D., *The cognitive engineering of problem represenation*. In Weir, G.R., Alty, J. L. (Eds.), Human-Computer Interaction and Complex Systems, London, Academic Press, 1991.
[57] Woods, D. D., Watts, J. C., Graham, J., Kindwell, D. L., & Smith, P. J., *Teachingcognitive systems engineering*, Proceedings of the human factors and ergonomics society 40th annual meeting, Santa Monica, California: The Human Factors andErgonomics Society, 1996, pp. 259-263.
[58] Nagamachi, M., *Kansei Engineering: A new ergonomic consumer-oriented technology for product development*, International Journal of Industrial Ergonomics, 15, 1995, pp 3-11.
[59] Damasio, A., *Looking for Spinoza. Joy, Sorrow, and the Feeling Brain*, New York: Harcourt, Inc, 2003.
[60] Hackos, J. T., & Redish, J. C., *User and task analysis for interface design*, New York: Wiley, 1998.
[61] Oskarsson, P.-A., *Översikt över metodik för MSI-utvärdering vid systemutveckling*, FOI-R--0583-SE. Totalförsvarets Forskningsinstitut, Avdelningen för Ledningssystem, SE- 581 11 Linköping, 2002.
[62] Mishra, A.K., *Organizational responses to crisis: The centrality of trust*, in *Trust in organizations: Frontiers of theory and research*, R.M. Kramer and T.R. Tyler, Editors. 1996, Sage: Thousand Oaks, CA. p. 261-287.
[63] Österman, T., *Förtroende*. 1999, The National Board of Psychological Defence (SPF): Stockholm. p. 45.
[64] Meyerson, D., K.E. Weick, and R.M. Kramer, *Swift trust and temporary groups*, in *Trust in Organizations: Frontiers of Theory and Research*, R.M. Kramer and T.R. Tyler, Editors. 1996, Sage Publications: London. p. 166-195.
[65] Zhengxin Chen, *Data Mining and Uncertain Reasoning: An Integrated Approach,* John Wiley and Sons, New York, 2001.
[66] Mena, J. *Investigative Data Mining for security and Criminal Detection,* Elsevier Science (USA), Burlington, MA, 2003.
[67] Preece, J., Rogers, Y., Sharp, H., Benyon, D., Simon, H., & Tom, C. *Human- Computer Interaction*. Wokingham: Addison-Wessley, 1994.
[68] Allwood , J., & Andersen, L.-G., *Semantik* (12:e upplagan). Göteborg, 1993.
[69] Nielsen, J., *Usability engineering*. Boston: Academic Press, Inc, 1993.
[70] Wickens, C. D., Todd, S., & Seidler, K. S., *Three-dimensional displays: Perception, implementation and applications.* CSERIAC--State of the Art Report, CSERIAC SOAR #89-001, 1989, Wright-Patterson AFB: Crew System Ergonomics Information Analysis Center.
[71] Wickens, C. D., & Prevett, T., *Exploring the dimensions of egocentricity in aircraft navigation displays: Influences on local guidance and global situation awareness*, Journal of Experimental Psychology: Applied, 1(2), 1995, pp 110-135.

[72] Wickens, C. D., & Carswell, C. M., *Information processing*, Chapter 4 in Salvendy, G. (Ed.) Handbook of Human Factors and Ergonomics, New York, John Wiley & Sons, Inc, 1997.
[73] Kirwan, B., & Ainsworth, L. K., *A guide to task analysis.* London: Taylor & Francis, 1993.
[74] Klein, G. A., Orasanu, J., Calderwood, R., & Zsambok, C. E. (Eds.), *Decision making in action: Models and methods.* Norwood, NJ: Ablex Publishing Corp, 1993.
[75] Cannon-Bowers, J. A., Salas, E., & Pruitt, J. S., *Establishing the boundaries of a paradigm for decision-making research*, Human Factors, 38(2), 1996, pp 193-205.
[76] Militello, L. G., & Hutton, R. J. B., *Applied Cognitive Task Analysis (ACTA): A practitioners´s toolkit for understanding cognitive task demands*. Ergonomics, 41(11), 1998, pp 1618-1641.
[77] Kylesten, B, *En referensram för att beskriva dynamiskt beslutsfattande i en ledningsträningsanläggning*, FOI-R-0340-SE, Linköping, Totalförsvarets Forskningsinstitut, 2001.
[78] Wikberg, P., & Modéer, B., *Modellering av operativ ledningsenhet. Visuell modellering som metod för problemanalys och operationalisering av begrepp i komplexa system*, FOA-R-99-01372-505-SE. Linköping, Försvarets Forskningsanstalt, 1999.
[79] Wikberg, P., Söderberg, H., & Worm, A., *Modellbaserad utvärdering: datainsamling i distribuerade ledningssystem med hjälp av förbandsinstruktörer.* FOA-R-00-01462-505-SE, Linköping, Försvarets Forskningsanstalt, 1999.
[80] Hallberg, J., ”IT-säkerhet för idealister–användarnas roll i att säkra system” i IT för idealister, Bilda Idé och Kommunikation, 2003.
[81] Wadströmer, N. Data quality, Linköping studies in science and technology, Thesis 363, Linköping University, 1993.
[82] Sårbarhets- och säkerhetsutredningen, Säkerhet i en ny tid, SOU 2001:41, maj 2001.
[83] Cohen, F. Cyber-Risks and Critical Infrastructures. all.net/journal/ntb/infrastruc.html. 2003.
[84] ITS, Informationstekniska standardiseringen i Sverige, Terminologi för Informationssäkerhet, Rapport ITS 6, mars 1994.
[85] [Hallberg, J., Hunstad, A., Eriksson, E. A. & Palmgren, S. Områdesanalys: IT-försvar. Användarrapport, FOI-R-0469-SE, FOI. Januari 2002.
[86] Schneier B, Secrets & Lies - Digital Security in a Networked World, John Wiley & Sons, 2000.
[87] Jonsson, E. *An integrated framework for security and dependability*, Proceedings of the New security paradigms workshop, Charlottesville, Virginia, USA, pp 22-29.
[88] workshop, Charlottesville, Virginia, United States, pp. 22 - 29, 1998.
[89] FOI yttrande över betänkandet ”Trygga medborgare - säker kommunikation. Förslag till gemensamt radiokommunikationssystem för skydd och säkerhet” (SOU2003:10). FOI regnr 03-140:2
[90] Årsrapport från perspektivplaneringen 2002-2003; Målbildsinriktningar inför Försvarsbeslut 2004 – rapport 7, HKV 23 210:63 128, 2003-02-28
[91] http://www.sdrforum.org
[92] Betänkande av Göteborgskommittén, SOU 2002:122
[93] Krishanteringssystemet, http://www.krisberedskapsmyndigheten.se/verksamhet/kommunal/kommunpaketet/krishanteringssystemet.pdf (2003-01-19)
[94] SOU 2003:11 *System för samordnad krisinformation*.
[95] *Planeringsinriktning för samhällets krisberedskap 2004*. ISBN: 91-85053-00-7, Edita Norstedts tryckeri AB, Stockholm 2002.

[96] Ryghammar L., Ekebjär G., och Nilsson A., *Lokal ledning och samverkan inför och under kris och krig*. Några exempel på lednings- och samverkanslösningar. (FOA-R--99-01131-505--SE) Stockholm, FOA 1999.

[97] Morin, M., Jenvald, J., and Thorstensson, M. (Red.) (2003) Utvecklingsmetoder fo"r samha"llsfo"rsvaret. FOI-R--1064--SE, ISSN 1650-1942.

[98] Morin, M. (2001) MIND - methods and tools for visualization of rescue operations. In: Proceedings of The International Emergency Management Society's Eighth Annual Conference (TIEMS 2001).

[99] Maier M. W. & Rechtin, E. (2002) *The art of systems architecting*. CRC Press.

[100] Garlan, D., Allen R., & Ockerbloom, J. (1995) Architectural mismatch: why reuse is so hard. *IEEE Software*, 12(6):17—26.

[101] Mills, J. A, A pragmatic view of the system architect, Communications of ACM, vol. 28, nr 7, 1995

[102] Muller, J.K., (1995) Integrating architectural design into the development process. In *Proceedings of the 1995 International Symposium and Workshop on Systems Engineering of Computer Based Systems*, pp. 114 -121.

[103] Dave, B. (1998) Teamwork constructs in architectural design. In *Proceedings of Computer Human Interaction Conference*, Australasian, pp.

[104] Rechtin, E. (1999) *System architecting of organizations: Why Eagles can't swim*. CRC Press.

[105] Alberts, D. S., Garstaka, J. J., & Stein, F. P. (2000). *Network Centric Warfare: Developing and leveraging Information Superiority.* CCRP publication series.

[106] FMA (2002), FMA 2.0 M5 (cd-rom), Försvarsmaktens arkitektur, FMV.

[107] Jönsson, PG (2003) FMA AR Tjänstekonceptet M5, ver. 2.1, Funktion 09100:54976/02, FMV.

[108] Graser, T., Barber, K. S., Williams, B., Saghir, F., Henry, K. A., *Advanced consequence management program: challenges and recent real-world implementations*, Proceedings of the SPIE conference on Sensors and Command, Control, Communications and Intelligence (C^3I) Technologies for Homeland Defence and Law Enforcement, Orlando, FL, USA, April 1-5, 2002, pp 324-333.

[109] Rodrigues Nt, J.A.; Ulm de G. Lima, V.M.; Lima, G.M.P.S.; Ferreira, M.C.; Alves de Almeida, J.C.; de Oliveira e Cruz, S.; Cerqueira, R.F.G.; Martins, C.B., *A command and control support system using CORBA*, Proceedings 21st International Conference on Distributed Computing Systems, Mesa, AZ, USA, April 16-19, 2001, p 735-738.

[110] Modrick, J. A., *PRESTO: multi-media distributed network for collaborative work in command and control*, Proceedings of 40th Annual Meeting of the Human Factors and Ergonomics Society, Philadelphia, PA, USA, 1996, pp 758-761.

[111] Sutherland, J.W., *Model-base structures to support adaptive planning in command/control systems*, IEEE Transactions on Systems, Man and Cybernetics, vol. 20, no. 1, Jan.-Feb. 1990, p 18-32.

[112] Braim, S.P., Hepworth, N., *A fully-featured human computer interface for intelligence and command and control applications,* International Conference on Information-Decision-Action Systems in Complex Organisations (Conf. Publ. No.353), 6-8 April, 1992 , Oxford, UK, p 149-52.

[113] Wohlever, S., Fay-Wolfe, V.; Freedman, R.; Maurer, J., *Building adaptable real-time command and control systems using CORBA*, Fourth International Workshop on Object-Oriented Real-Time Dependable Systems, 27-29 Jan. 1999 , Santa Barbara, CA, USA, p 117-22.

[114] Bammidi, P., Moore, K.L., *Emergency management systems: a systems approach,* 1994 IEEE International Conference on Systems, Man, and Cybernetics. Humans, Information and Technlogy, 2-5 Oct. 1994 , San Antonio, TX, USA , pt. 2, p 1565-70 vol. 2.