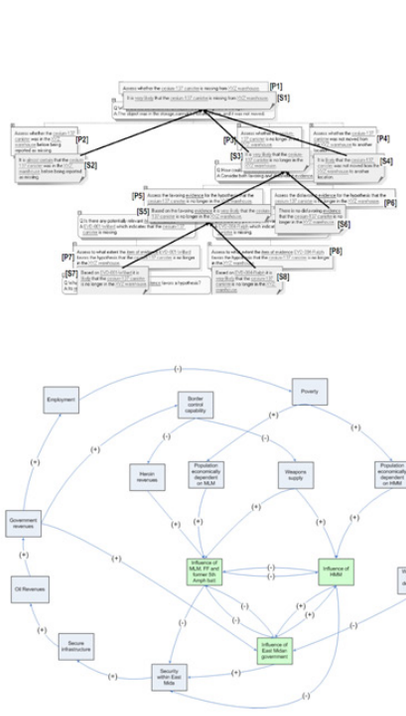
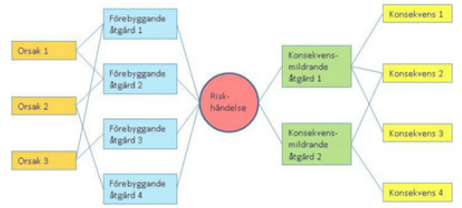
Analytiska verktyg

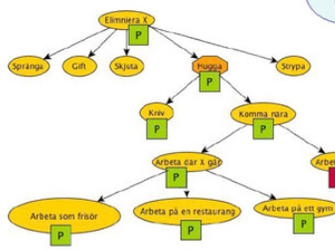
- en översikt av metoder och modeller för underrättelseanalys

TOVE GUSTAVI, FREDRIK JOHANSSON, RONNIE JOHANSSON,
MAGNUS JÄNDEL, LISA KAATI, CHRISTIAN MÅRTENSON, DANIEL OSKARSSON





	Brott	Olycka	Frivilligt försvinnande
Mobilsamtal	-	/	+
Upphittat hårspänne	/	/	?
Vittnesuppgifter	-	- -	+ +
Uppgifter från socialtjänsten	+	/	+



FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
Informationssystem
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se

FOI-R--3310--SE
ISSN 1650-1942

Användarrapport
December 2011

Informationssystem

Tove Gustavi, Fredrik Johansson, Ronnie Johansson, Magnus Jändel, Lisa Kaati, Christian Mårtenson, Daniel Oskarsson

Analytiska verktyg

- en översikt av metoder och modeller för underrättelseanalys

Titel	Analytiska verktyg – en översikt av metoder och modeller för underrättelseanalys
Title	Analytical techniques – an overview of methods and models for intelligence analysis
Rapportnr/Report no	FOI-R--3310--SE
Rapporttyp /Report Type	Användarrapport
Månad/Month	December
Utgivningsår/Year	2011
Reviderad/Revised	Feb 2012
Antal sidor/Pages	73 p
ISSN	ISSN 1650-1942
Kund/Customer	FM
Projektnr/Project no	E53200
Godkänd av/Approved by	Martin Rantzer

FOI, Totalförsvarets Forskningsinstitut
Avdelningen för Informationssystem

164 90 Stockholm

FOI, Swedish Defence Research Agency
Information Systems

SE-164 90 Stockholm

Sammanfattning

Det huvudsakliga syftet med denna rapport är att samla den kunskap om analytiska verktyg i form av metoder och modeller för underrättelseanalys som finns på FOI och att göra den tillgänglig i en lättförståelig och översiktlig form. Även om rapporten inte är heltäckande är förhoppningen att den dels ska ge läsaren en uppfattning om vilken sorts analytiska verktyg som finns, dels ska kunna användas i det praktiska underrättelsearbetet som ett stöd för att avgöra hur och när man ska använda de verktyg som presenteras i rapporten.

Nyckelord: analytiska metoder, underrättelseanalys, hypotesgenerering, hypotestestning, riskanalys

Summary

The main purpose of this report is to gather the knowledge of analytic tools for intelligence analysis that exists at FOI and to make this knowledge available in an easily accessible format. Even though the report does not cover all aspects it will hopefully give the reader an idea of the type of analytic tools that are available. Also, we hope that the report can be of help in the daily work when deciding how and when to use the tools described in this report.

Keywords: analytical methods, intelligence analysis, hypothesis generation, hypothesis testing, risk assessment

Innehållsförteckning

1 Introduktion

Med uttrycket ”analytiska verktyg” avses i denna rapport metoder och modeller som kan användas för att strukturera ett problem i syfte att skapa ökad problemförståelse och för att kunna generera och pröva hypoteser mot data/observationer. I de flesta fall består ett analytiskt verktyg av både en metod och en modell, där metoden beskriver hur man modellen tas fram och/eller hur modellen ska användas. På FOI används analytiska verktyg huvudsakligen i tre sammanhang; för analys, som underlag för metodforskning, samt som underlag för forskning om datorbaserade analysstödsystem. Erfarenheten på FOI av analytiska verktyg är utspridd mellan olika avdelningar och individer och det gör att den samlade kunskapen är svår att överblicka. Avsikten med den här rapporten har varit att samla den kunskap om analytiska verktyg som finns på FOI och att göra den tillgänglig i en lättförståelig och översiktlig form. I rapporten beskrivs ett antal analytiska verktyg. Dessa verktyg har två saker gemensamt:

1. Det finns praktisk eller teoretisk kunskap om dem inom FOI.
2. De har bedömts vara intressanta ur ett underrättelseperspektiv.

Inom underrättelseanalys är hypoteshantering och osäkerhetshantering särskilt viktiga områden och det speglas i rapporten genom att flertalet av de verktyg som finns beskrivna kan kopplas till antingen hypotesgenerering, hypotestestning eller riskhantering.

Rapporten består av tre delar: *Introduktion*, *Verktygsbeskrivningar* och *Diskussion*. Introduktionen innehåller bl.a. förklaringar av begrepp som återkommer senare i rapporten. Den centrala delen av rapporten utgörs av verktygsbeskrivningarna i kapitel 2. Kapitel 2 är ordnat så att beskrivningarna av de verktyg som används för hypotesgenerering kommer först, sedan följer beskrivningarna av de verktyg som används för hypotestestning. De verktyg som varken kan klassificeras som hypotesgenererande eller hypotestestande beskrivs sist. Varje beskrivning inleds av ett kort avsnitt som beskriver möjliga användningsområden och ger exempel på problem där modellen/metoden kan användas. Efter detta stycke följer ytterligare ett kort avsnitt där eventuella förutsättningar för att kunna tillämpa verktyget listas. Tanken är att de två första avsnitten i metodbeskrivningarna ska kunna användas för att avgöra om en modell/metod är lämplig att använda i en given situation. Efter dessa avsnitt följer i tur och ordning avsnitten *Beskrivning av metoden*, *Tillämpningar och erfarenheter* samt *Teknikstöd*. Rapportens tredje och avslutande del har fått rubriken *Diskussion*. I diskussionskapitlet flyttas fokus från enskilda verktyg till en övergripande systemnivå. I kapitlet beskrivs hur analysverktygen passar in i ett större sammanhang och hur hypoteshantering och informationshantering kan

kopplas till beslutsstöd. Ett avsnitt ägnas också åt att diskutera hur man kan gå från kvalitativ data till kvantitativ analys och vilken problematik detta medför.

Flera av de verktyg som beskrivs i rapporten bygger på matematiska modeller, men i denna rapport har de mer matematiska resonemangen medvetet utelämnats för att underlätta läsningen. Läsaren behöver alltså inga djupare kunskaper i matematik för att kunna ta till sig innehållet i rapporten. Den matematiskt intresserade läsaren hänvisas till referenslistan för respektive metod där det finns förslag på mer uttömmande läsning.

1.1 Underrättelseanalys

Underrättelsearbetet brukar traditionellt beskrivas av den så kallade underrättelsecykeln som delas upp i ett antal faser: planering, inhämtning, bearbetning och delgivning. I Underrättelsereglementet [1] delas bearbetningsfasen upp i *strukturerande* respektive *genererande* bearbetning. Den strukturerande bearbetningen omfattar hantering, registrering och sammanställning av data och informationselement. Den syftar till att urskilja och sortera relevant information samt göra den sökbar. Den genererande bearbetningen omfattar värdering, analys, syntes samt tolkning av data och informationselement. Den syftar till att göra informationen användbar genom att sätta in den i ett sammanhang där den kan användas till att upptäcka, värdera, förklara, förstå eller förutsäga ett fenomen eller en situation. Metoderna och modellerna i den här rapporten är anpassade för att i första hand stödja den genererande bearbetningen och i synnerhet analysdelen av denna process.

Analysen syftar till att skapa förståelse för ett fenomen genom att dela upp det i komponenter och klargöra respektive komponents betydelse och dess relationer till övriga komponenter. Analysen kan utgå antingen från data eller från en konceptuell modell, som utgörs av antaganden baserade på analytikerns erfarenhetsbaserade generella uppfattning av denna typ av fenomen. Oftast rör det sig dock om en kombination av dessa. I de fall där analysen huvudsakligen utförs manuellt får den konceptuella modellen ofta stort inflytande. Grundad teori (se kapitel 2.2 *Grundad teori*) utgör här ett undantag med sin extrema hållning att enbart data ska ligga till grund för analysen och all typ av förförståelse ska undertryckas. Vid ökat inslag av automatiskt stöd vid skapandet av analysmodeller får data naturligt större betydelse. Då man t.ex. använder maskininlärning för att automatiskt lära in kvantitativa parametrar i en analysmodell sätter tillgången till data upp begränsningar för hur korrekt modellen kan bli.

Om syftet med analysen är att enbart öka förståelsen för fenomenet som studeras kan det vara tillräckligt att skapa en analysmodell. Ofta vill man dock använda analysmodellen för att ta fram ett beslutsunderlag genom att skapa ett antal hypoteser och pröva dem mot observerad data. En hypotes kan vara av olika slag,

t.ex. en utsaga om en framtida händelseutveckling eller en möjlig förklaring till en observerad händelse. Förfarandet att utifrån en analysmodell försöka generera och identifiera den hypotes som bäst förklarar (matchar) de observationer som finns kallas *abduktion*. Abduktion är en central del av bearbetningens värdering och syntes och kan göras både kvalitativt som i Analys av konkurrerande hypoteser (se kapitel 2.6 *Analys av konkurrerande hypoteser*) och kvantitativt, t.ex. med hjälp av Bayesianska nätverk.

1.2 Användning av analytiska verktyg

Analytiska verktyg används idag i varierande grad inom svensk militär underrättelsetjänst, huvudsakligen inom ”bearbetning och analys”-delen av underrättelsecykeln [1]. Förutsättningarna för att kunna göra mer ingående och tidskrävande analyser är i regel bättre på strategisk än på taktisk och operativ nivå och därför är det också där som analytiska verktyg används mest. Det kan dock finnas tillfällen även på taktisk och operativ nivå då användning av analytiska verktyg är lämplig.

Användningen av analytiska verktyg inom underrättelseanalys är inte helt oproblematisk. Förutom att metoderna är mer eller mindre tidskrävande upplevs de ibland som illa anpassade till de praktiska problem som ska lösas och i vissa fall är det dessutom oklart om de ger något verkligt mervärde till analysen. Det är rimligt att anta att problemen åtminstone till viss del är en följd av bristande kunskaper om vilket verktyg som passar vid vilket tillfälle, men det ska också medges att analytiska verktyg inte alltid är lämpliga att använda. Problemet som ska analyseras bör vara av så stor vikt att det är värt att låta en enskild analytiker, eller ibland en hel grupp, lägga ner den arbetsinsats som krävs för att kunna använda verktyget på rätt sätt utan att det finns några garantier för att arbetet kommer att resultera i avgörande ny kunskap eller nya insikter.

Det kanske viktigaste skälet till att använda strukturerade analytiska metoder är att man minskar risken för att oönskade kognitiva faktorer ska påverka bearbetningen av information. Vid användandet av strukturerade metoder och väldefinierade modeller tvingas analytikern ofta ifrågasätta sina egna slutsatser och redovisa sina antaganden tydligare än annars vad som annars är fallet. Det blir då lättare för analytikern själv såväl som för kollegor och andra referenspersoner att upptäcka oredovisade antaganden och brister i ett resonemang. **Att använda analytiska verktyg kan alltså ses som ett sätt att - i den utsträckning det är möjligt - verifiera att alla bedömningar och slutsatser är baserade på saklig grund.**

Nedan följer exempel på kognitiva faktorer som, om man inte är uppmärksam på dem, riskerar att påverka bearbetningen av information [1]:

- *Tendensen att se mönster där det inte finns något*

Det är lätt att övertolka data och därför ska man vara försiktig med att dra slutsatser innan man har ett tillräckligt stort underlag att basera slutsatserna på.

- *Tendensen att söka efter bekräftande bevis*

  Människan tenderar att leta efter bevis som stödjer hennes hypotes snarare än bevis som motsäger egna och/eller andras hypoteser. I värsta fall kan detta leda till att man missar den riktiga hypotesen [2].

- *Fördomar genom vår förförståelse*

  Om man genom erfarenhet vet att något ofta förhåller sig på ett visst sätt så är det lätt att ta detta förhållande för givet utan att reflektera över att man därmed inför ett nytt antagande i analysen.

- *Gruppbeteende*

  Om man vet att t.ex. kollegor eller familjemedlemmar är av en viss åsikt eller gör en viss tolkning av fakta så är det troligt att ens egen bedömning omedvetet påverkas i samma riktning.

Andra skäl för att använda analytiska verktyg i underrättelsearbetet är:

- De kan användas som diskussionsunderlag och stöd för att få igång tankeprocessen i en arbetsgrupp, s.k. *facilitering*.
- Risken att missa viktiga aspekter i analysen minskar.
- De kan ge ett visst stöd vid bedömningen av hur mycket tilltro man ska ha till ett visst resultat (bl.a. baserat på informationskällornas tillförlitligheter och informationens sakriktighet).
- De kan användas som stöd vid dokumentation och redovisning av processen bakom ett beslut.

1.3 Tekniska hjälpmedel

De flesta av de verktyg som finns med i rapporten kräver inga tekniska hjälpmedel, men det underlättar ofta betydligt att ha tillgång till någon form av datorstöd. I vissa metoder och modeller hanteras så många informationselement och relationer mellan dessa att tekniskt stöd är mer eller mindre nödvändigt för att man ska kunna använda verktyget på ett effektivt sätt. I vissa fall finns analysprogram fritt tillgängliga på nätet, i vissa fall finns kommersiell programvara tillgänglig. För varje verktyg har vi försökt att ge en sammanfattning av idag tillgängligt (kommersiellt/fritt åtkomligt på nätet eller åtkomligt på annat sätt) tekniskt stöd. I viss mån har vi också föreslagit möjliga vidareutvecklingar/förbättringar av befintligt stöd.

1.4 Centrala begrepp

Några ord och uttryck återkommer på flera ställen i rapporten. För att undvika missförstånd definieras de viktigaste här.

Hypotes - Hypoteskonceptet är centralt inom underrättelseanalys. En hypotes betraktas inom underrättelseanalys som ”ett antagande för att förklara ett fenomen eller iakttagelse” [1]. En hypotes bör enligt Försvarsmaktens underrättelsereglemente vara:

- Motsägelsefri.
- Möjlig att pröva, d.v.s. det måste finnas något som går att observera och som kan knytas till om hypotesen är sann eller falsk.
- Rimlig (man bör dock vara försiktig med att utesluta hypoteser redan från början på basis av subjektiva bedömningar).

Indikator – En indikator är ”en observerbar faktor (händelse, företeelse, beteende eller liknande) som stöder eller motbevisar en hypotes. En indikator kan uttryckas i form av ting/objekt, händelse, förlopp, aktiviteter eller tillstånd” [1].

Evidens – En observation av en indikator kallas evidens.

1.5 Klassificering av metoder och modeller

Verktygen som ingår i den här rapporten är inte utvalda för att tillsammans kunna täcka behoven av analytiska verktyg i alla situationer. Trots detta bör det framgå av metodbeskrivningarna att verktygen till viss del kompletterar varandra på olika områden. För att läsaren ska få en bättre överblick över verktygens egenskaper, likheter och olikheter har alla verktyg i rapporten klassificerats utifrån:

1. Utgångspunkten för metoden
2. Vilken typ av information metoden arbetar med
3. Vilken typ av resultat metoden genererar

Klassificeringen har skett enligt följande definitioner.

Modelldriven/Datadriven: I modelldrivna metoder utgår analytikern från en konceptuell modell av verkligheten. Information och observationer tolkas sedan inom ramen för denna modell. I datadrivna metoder finns ingen sådan bakomliggande modell. Istället använder sig metoden av tillgängliga data för att *skapa* en modell, det kan t.ex. handla om att lära in en normalbild av en situation eller fenomen och identifiera avvikelser från denna. Datadrivna metoder ger utdata som ska vara tolkningsbara, men modellen i sig är inte alltid möjlig att

tolka utifrån vår vanliga begreppsvärld. Maskininlärning är ett exempel på en datadriven applikation.

Kvalitativ/Kvantitativ: Att en metod/modell är kvantitativ innebär att den arbetar med numeriska data, t.ex. numeriska mätvärden eller sannolikheter. Kvantitativa verktyg är baserade på matematiska modeller och ger alltså i någon mening objektiva resultat som är exakta och lätta att jämföra. Kvalitativa metoder/modeller är ”beskrivande” till sin natur och arbetar med ord och symboler snarare än med siffror. Klassificeringar av typen ”Bra”, ”Mindre bra” och ”Dåligt” är exempel på kvalitativa klassificeringar. Kvalitativa verktyg är till sin natur mer eller mindre subjektiva och öppna för tolkning. Kvalitativa data kan ibland göras kvantitativa genom att man med hjälp av någon strukturerad metod sätter siffror på omdömen och utsagor. Man måste emellertid vara mycket uppmärksam på hur detta sker så att resultatet kan tolkas på ett meningsfullt sätt utan att bli missvisande. Mer om detta finns att läsa i kapitel 3.2 *Från kvalitativt till kvantitativt – Att utvinna sannolikheter ur domänkunskap*.

Hypotesskapande/Hypotestestande: Hypotesskapande metoder producerar nya hypoteser utifrån någon form av underlag (erfarenhet, observationer, eller dylikt). Dessa nya hypoteser kan användas för att bredda ett beslutsunderlag eller utgöra material till hypotestestande metoder. Hypotestestande metoder förutsätter att det redan existerar ett antal hypoteser att arbeta med. Hypotestestande metoder har som mål att välja mellan hypoteser eller bedöma hypotesers giltighet.

Innan man använder ett analytiskt verktyg bör man tänka igenom vilka egenskaper verktyget har och om dessa egenskaper passar för det problem man vill tillämpa verktyget på. Hoppar man över detta steg är risken stor att man förlorar mycket tid på att försöka anpassa ett problem till ett verktyg som inte är avsett att producera den sorts resultat man efterfrågar.

En sammanfattning av egenskaperna hos de verktyg som beskrivs i rapporten finns i Tabell 7 i diskussionskapitlet efter verktygsbeskrivningarna. Notera att i vissa fall har verktygen inte kunnat klassificeras entydigt och i vissa fall har frågeställningen som en viss klassificering baseras på inte varit relevant för ett specifikt verktyg.

2 Verktygsbeskrivningar

2.1 Morfologisk analys

Modellegenskaper: Modelldriven, kvalitativ, hypotesskapande

2.1.1 Användningsområden

Morfologisk analys är en metod som används då man har ett behov av att konkretisera och analysera möjliga händelseutvecklingar eller hypoteser, typiskt i situationer där utfallsrummet är för stort för att enkelt kunna överblickas. Med hjälp av Morfologisk analys kan man på ett strukturerat sätt ta fram ett stort antal olika hypoteser, både mer och mindre realistiska. De mest relevanta av de genererade hypoteserna kan man sedan gå vidare med och analysera i större detalj.

Syftet med att använda Morfologisk analys är ofta att hitta händelseutvecklingar eller hypoteser som inte är uppenbara och som man därför lätt förbiser om man använder ett icke-metodiskt tillvägagångssätt. Metoden kan både användas som ett rent analysverktyg och som hjälpmedel vid facilitering.

Problem där Morfologisk analys kan användas

- **Hitta möjliga säkerhetsrisker**

  På t.ex. en militärbas eller en flygplats är det viktigt att ha beredskap för en stor mängd hot och säkerhetsrisker. Vid genomgång av säkerhetsrutinerna kan det vara nyttigt att använda Morfologisk analys för att på ett metodiskt sätt generera alternativa hotbilder och säkerhetsrisker. Detta minskar risken för att man vid den manuella genomgången av säkerhetsrisker ska ha förbisett något.

- **Konkretisera hypoteser för vidare analys**

  Vid t.ex. brottsutredningar händer det att man i brist på konkreta ledtrådar måste arbeta förutsättningslöst med en mängd alternativa hypoteser. Med hjälp av Morfologisk analys kan man generera en stor mängd hypoteser som förhoppningsvis är tillräckligt varierade för att tillsammans ge en god uppfattning om både troliga och mindre troliga alternativ. De genererade hypoteserna kan användas som utgångspunkt för utredningen och man kan fokusera arbetsinsatserna på att eliminera så många hypoteser som möjligt.

2.1.2 Nödvändiga förutsättningar

- **Möjliga scenarier/hypoteser får endast variera inom vissa ramar**

  Metoden för att ta fram olika scenarier bygger på att man varierar värdena på ett antal dimensioner som bedömts vara relevanta i sammanhanget. Exempel på dimensioner som kan vara av intresse vid en hotanalys är *Aktör*, *Motiv*, *Plats*, *Tidpunkt*, *Transportmedel*. Man kan se det som att de valda dimensionerna tillsammans utgör en mall som ska fungera för alla möjliga hypoteser/scenarier. Metoden kan alltså inte generera hypoteser som inte är konsistenta med mallen.

2.1.3 Beskrivning av metoden

Som analytiker hamnar man då och då i situationer där man måste ta med flera alternativa hypoteser eller scenarier i beräkningen. Ibland rör det sig om ett fåtal väldefinierade hypoteser/scenarier, men ibland är lösningsrummet öppet och svårt att överblicka som t.ex. om man ska analysera den politiska utvecklingen i ett land eller beredskapen för hot mot infrastrukturen i ett samhälle. Om problemet är svåröverskådligt kan det vara nödvändigt att försöka konkretisera de scenarier/hypoteser som behöver beaktas innan man går vidare med analysen. Det är företrädelsevis i sådana situationer som Morfologisk analys kommer till sin fulla rätt.

Tanken bakom Morfologisk analys är att man ska försöka hitta en gemensam struktur hos de lösningar/hypoteser/scenarier som är aktuella i ett visst problem (morfologi = formlära). Då man hittat en struktur som passar i sammanhanget kan man variera övriga parametrar i problemet och på så sätt generera en mängd mer eller mindre troliga hypoteser eller scenarier. Förhoppningsvis kan både modelleringsprocessen i sig och de genererade hypoteserna/scenarierna bidra till att ge analytikern eller analytikerna en bättre uppfattning om vilken sorts hypoteser/scenarier som kan behöva beaktas.

Då man ska använda Morfologisk analys börjar man i praktiken med att identifiera en uppsättning relevanta *dimensioner* som tillsammans definierar en händelseutveckling/hypotes. Dessa dimensioner utgör den gemensamma strukturen för alla möjliga lösningar. I en brottshypotes skulle man t.ex. kunna tänka sig att ha med dimensionerna *Gärningsman*, *Motiv* och *Brottsplats*. För att modellen ska hålla sig på en rimlig abstraktionsnivå och inte växa sig ohanterligt stor bör man försöka begränsa sig till att använda i storleksordningen 5-8 dimensioner. Detta riktmärke gäller i princip oavsett problemets karaktär och omfattning. Skulle det visa sig vara nödvändigt så går det dock att lägga till fler dimensioner i efterhand. Efter att dimensionerna fastställts listar man för varje dimension de värden som just den dimensionen kan anta. Möjliga värden för dimensionen *Transportmedel* skulle t.ex. kunna vara *Bil*, *MC*, *Cykel*, *Båt*, och

Tåg. Dimensionerna och deras möjliga värden förs ofta in i en tabell (se exempel nedan).

Genom att systematiskt gå igenom alla kombinationer av möjliga värden på de identifierade dimensionerna i tabellen får man nu enkelt fram en mängd hypoteser som kan analyseras vidare. Ett problem är dock att antalet möjliga hypoteser snabbt blir väldigt stort. Med *n* dimensioner och *m* olika möjliga värden för varje dimension uppgår det totala antalet olika hypoteser i modellen m^n. Ett effektivt sätt att minska antalet hypoteser är att betrakta dimensionerna parvis och identifiera kombinationer av värden som av någon anledning inte kan förekomma i samma hypotes. Alla hypoteser som innehåller icke-tillåtna kombinationer kan strykas. Denna teknik för att minska antalet hypoteser refereras ibland till som *the principle of contradiction and reduction* medan den på andra ställen i litteraturen kallas *cross-consistency assessment* [3]. Det räcker ofta med att identifiera ett par stycken otillåtna kombinationer för att minska antalet tillåtna hypoteser drastiskt. Vill man göra en heltäckande analys av alla parvisa kopplingar behöver man i regel använda någon form av datorstöd. Antalet parvisa kopplingar i modellen ökar visserligen inte alls lika snabbt som antalet hypoteser då man lägger till fler dimensioner, men trots detta blir antalet kopplingar lätt väldigt stort.

Morfologisk analys gör sig i allmänhet bäst som en interaktiv metod där flera personer får bidra med sina respektive kunskaper och erfarenheter. Genom att involvera människor med olika kompetenser minimerar man risken att missa viktiga aspekter av problemet i modelleringen. På många sätt är Morfologisk analys en svår analysmetod trots att den rent tekniskt är ganska enkel. För att få ett bra resultat krävs en känsla för hur man ska sätta upp sin modell, vad som bör ingå i modellen, vilken komplexitet som är lämplig, o.s.v. Av den orsaken rekommenderas ofta att någon med tidigare erfarenhet av Morfologisk analys leder, eller åtminstone deltar, i modelleringsprocessen.

Fördelar	Nackdelar
1. Metoden ställer få krav på egenskaperna hos det problem som ska modelleras	1. Antalet hypoteser växer oerhört snabbt och det är svårt att hantera alla möjliga hypoteser utan datorstöd (i vissa fall även med datorstöd) 2. Det kan vara svårt att få ut användbara resultat utan assistans av erfaren moderator

2.1.3.1 Exempel

I det här exemplet visar vi hur Morfologisk analys kan användas för att hitta säkerhetsrisker, i detta fall inför ett politiskt evenemang. Vi tänker oss ett scenario där en känd politiker ska delta i ett torgmöte. Politikern ifråga har välkända och tämligen kontroversiella åsikter i vissa känsliga frågor och lever därför med en ständig hotbild mot sig. Inför torgmötet gör man en rutinmässig genomgång av tänkbara hotscenarier för att verifiera att man inte missat viktiga aspekter i säkerhetsarrangemangen. Som stöd vid arbetet med att ta fram hotscenarier används Morfologisk analys.

För enkelhetens skull utgår vi i detta exempel från att en eventuell attack kommer att vara riktad direkt mot den aktuella politikern och inte mot tredje part (medhjälpare, arrangörer av torgmötet eller åhörare).

1. Välj dimensioner. Då man väljer vilka dimensioner som ska finnas med i modellen är det viktigt att hålla i minnet vad modellen ska användas till. I det här exemplet ska modellen ligga till grund för det förebyggande säkerhetsarbetet och därför är det viktigt att modellen fångar upp aspekter som är viktiga för det arbetet. T.ex. bör modellen innehålla dimensionen *Vapen/Tillhygge* eftersom den dimensionen är avgörande för vilka skyddsåtgärder som ska vidtas. Däremot är det inte uppenbart att man måste ha med dimensionen *Motiv*. Motivet för en attack är endast relevant för säkerhetsarbetet om det säger något om vem som planerar en attack eller om hur attacken kommer att ske.

I vårt förenklade exempel har vi nöjt oss med att välja ut fyra dimensioner: *Aktör*, *Plats för attacken*, *Placering av aktör* och *Tillhygge*.

Aktör	**Plats för attacken**	**Placering av aktör**	**Tillhygge**
Upprörd allmänhet (oorganiserad)	Flygplatsen	Bland flygpersonalen	Kniv
Aktivistgrupp (organiserad)	På väg till/från bil	Bland åhörarna på torgmötet	Obeväpnad attack
Ensam galning	Torgmötet	I hus med utsikt över torget	Tårta
Terrorist			Skjutvapen

Tabell 1. Morfologisk matris.

2. Identifiera värden. För varje dimension identifieras alla tänkbara värden som är relevanta i sammanhanget. Värdena förs in i en Morfologisk matris (Tabell 1). Man kan använda matrisen till att hitta möjliga scenarier genom att kombinera ett värde från varje kolumn. Ett scenario karaktäriseras t.ex. av följande sammansättning:

Ensam galning – Torgmötet – Bland åhörarna på torgmötet – Obeväpnad attack.

Modellen omfattar nu totalt 4*3*3*4=144 olika scenarier, men många av dem är inte intressanta att analysera vidare.

3. Cross-consistency-analys. Gå igenom cellerna i tabellen parvis och identifiera kombinationer av värden som inte är möjliga. Exempel på omöjliga kombinationer visas i Tabell 2 där dimensionerna *Placering av aktör* och *Tillhygge* ställs mot varandra. I det här fallet är det fysiskt omöjligt för en tänkt förövare som är placerad i ett hus i närheten av torget att gå till attack med en kniv eller en tårta eftersom det kräver att förövaren och offret befinner sig på samma plats. Genom att stryka alla scenarier som innehåller någon av de tre identifierade otillåtna kombinationerna minskar man i ett slag antalet tänkbara scenarier från 144 till 108.

En högst osannolik kombination som i praktiken också kan uteslutas är *Terrorist – Tårta*. Genom att identifiera motsägelser av det här slaget kan man reducera antalet aktiva hypoteser/scenarier ytterligare. I det här steget är datorstöd till stor hjälp.

4. Extrahera möjliga scenarier. Efter de föregående stegen är det nu möjligt att generera en mängd möjliga scenarier genom att gå igenom alla tillåtna kombinationer av attribut i den Morfologiska matrisen (Tabell 1).

Placering av aktör *vs.* Tillhygge	**Bland flygplatspersonalen**	**Bland åhörarna på torgmötet**	**I ett hus med utsikt över torget**
Kniv			Omöjlig
Obeväpnad attack			Omöjlig
Tårta			Omöjlig
Skjutvapen			

Tabell 2. Cross-consistency-analys av kombinationen *Placering av aktör* och *Tillhygge*.

2.1.4 Tillämpningar och erfarenhet

2.1.4.1 Allmänt

Morfologisk analys utvecklades av astrofysikern Fritz Zwicky. Han använde metoden för frågeställningar som rörde hans arbete inom astronomi och rymdforskning. Fritz Zwicky har bland annat skrivit om morfologisk analys i boken *Discovery, Invention, Research – Through the Morphological Approach* [4]. I Sverige var det dåvarande FOA-medarbetaren Tom Ritchey som började utveckla metoden i mitten av 1990-talet [5]. Voros ger en bra översikt över metodens tillämpningar [6].

2.1.4.1 På FOI

Det finns idag ett antal analytiker på FOI som använder morfologisk analys för problemstrukturering, scenarioutveckling och analys av komplexa problem inom olika sakområden. Metoden har sedan mitten av 1990-talet tillämpats i ett nittiotal projekt. I rapporten Morfologisk analys i grupp – en personlig handledning [7] beskrivs hur metoden tillämpas på FOI och ett antal exempel på morfologiska analyser som FOI har genomfört.

Hotscenarier har tagits fram med hjälp av morfologisk analys i såväl civila som militära sammanhang. Många av dessa studier är av förklarliga skäl inte öppet publicerade. Två öppna exempel är ett verktyg för att värdera räddningstjänstens beredskap för kemikalieolyckor [8] och analys av SKI:s beredskap [9]. Ett annat exempel på hur man kan bygga hotscenarier med hjälp av morfologisk analys finns i Johansens rapport [10].

Aktuella exempel på morfologisk analys där scenarier har tagits fram med FOI:s stöd är EU-projekten DEMASST[1] och ACRIMAS[2] samt SLU-projektet Framtidens lantbruk [11].

2.1.5 Teknikstöd

Morfologisk analys innebär att man genererar en stor mängd hypoteser. För att kunna hantera dem är det i de flesta fall nödvändigt att använda datorstöd. Under 1990-talet utvecklade FOI datorverktyget MA/Casper (Computer Aided Scenario and Problem Evaluation Routine). Det MA/Casper bidrar med är bland annat:

- Stöd för tankeprocessen i en grupp experter genom att man visualiserar modellen
- Hjälp att hitta tillåtna hypoteser med ett visst värde på en eller flera variabler

[1] www.foi.se/demasst
[2] www.acrimas.eu/

- Hjälp att spåra hur man kom fram till en lösning/hypotes
- Hjälp att lägga till ytterligare dimensioner och tillstånd under processens gång och i efterhand
- Hjälp att på ett strukturerat sätt gå igenom alla parvisa kombinationer av värden/attribut och analysera tillåtenheten (den ovan nämnda cross-consistency-analysen)

MA/Casper är inte tillgänglig kommersiellt utan används av FOI:s analytiker i olika uppdrag. Ansvaret för metoden och dess utveckling ligger på enheten för Strategi och policy inom FOI Försvarsanalys.

På FOI har även verktyget Optima utvecklats som stöd för att skapa scenarier med hjälp av morfologisk analys [12]. Optima baseras på optimering av utfallsrummet så att scenarierna ska bli så olika som möjligt.

I FOI-rapporten Collaborative Synchronization Management Tool, A User's Guide [13] beskrivs ett kompletterande verktyg för kvantitativ analys av parvisa kombinationer av attribut där attributen utgörs av olika alternativ att genomföra delaktiviteter i en militär operation. En viss utvidgning har skett i [14].

2.2 Grundad teori

Modellegenskaper: Datadriven, kvalitativ, hypotesskapande

2.2.1 Användningsområden

Grundad teori kan användas för att bilda sig en uppfattning om en situation innan man vet så mycket att man ens kan ha en hypotes om vad situationen handlar om. Metoden är ett strukturerat arbetssätt där man försöker undvika förutfattade meningar och istället skapar hypoteser genom analys av data. Främst tillämpas metoden för att förstå människors mål och motiv i olika sociala situationer.

Relaterat till beskrivningen av underrättelseanalys i Försvarsmaktens Underrättelsereglemente [1] är Grundad teori en form av datadriven kvalitativ analys som omfattar både induktion och deduktion. Användningsområdet är genererande bearbetning och då speciellt fenomenanalys och systemanalys.

Problem där Grundad teori kan användas

- Polisen hittar en svårt skadad laptop i vattenbrynet på Stora Essingen. Den verkar ha slängts ut från en bil på Essingeleden. Hårddisken är krypterad men polisens jäktade tekniker lyckas åtminstone få fram en lista på alla filnamn. En analytiker på SÄPO får listan och uppdraget att ta reda på något om vad laptopen användes till. Att beställa mer avkrypteringsjobb eller annan teknisk analys är inte att tänka på. I denna

situation finns det inte något speciellt som analytikern försöker bevisa eller motbevisa. Grundad teori kan därför vara användbart här.

I beskrivningen av metoden återkommer vi till ovanstående exempel.

2.2.2 Nödvändiga förutsättningar

- **Det måste finnas data eller möjligheter att ta fram data.**

  Med data menas här någon form av observationer av den mänskliga situation som vi vill undersöka. Data kan t.ex. bestå av textrapporter, intervjuer, videofiler, ljudfiler eller fotografier.

2.2.3 Beskrivning av metoden

Vi fortsätter först det inledande exemplet med den skadade laptopen för att illustrera hur en analytiker kan arbeta med Grundad teori.

Analytikern börjar med att skriva ut listan på filnamn så att den täcker den vänstra kolumnen av pappret. I den högra kolumnen skriver hon koder som sammanfattar vad filnamnen handlar om. Koder kan vara substantiv, verb eller adjektiv. Det finns ingen regel för hur koder generas utan analytikern använder sin intuition. Tabell 3 visar hur arket ser ut när ett antal filnamn har kodats.

Filnamn	Koder
Ase Utra ljuddämpare Rimfire .22 pistol	TYST VAPEN
täbybo-testade-el-i-badkar-teori	ELOLYCKA
Bromsslangen avskuren - expojkvän åtalas	BILOLYCKA, SABOTAGE

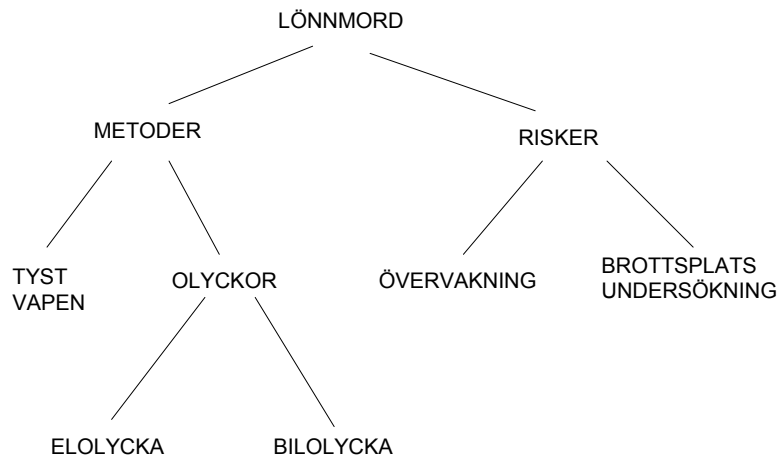
Tabell 3. Exempel på inledande ”öppen” kodning.

Efter att ha kodat ett antal filnamn börjar analytikern fundera på vilka begrepp som finns bland koderna och hur de är relaterade till varandra. Analytikern noterar att ELOLYCKA och BILOLYCKA båda tillhör kategorin OLYCKA. I övrigt framträder inte någon klar bild utan kodningsarbetet fortsätter enligt Tabell 4.

Filnamn	Koder
Polonium_ Poisoning_of_Alexander_Litvinenko	GIFT, LÖNNMORD
Säkerhetsteknik hjälper dig med kameraövervakning	ÖVERVAKNING
Forensic footwear evidence	BROTTSPLATSUNDERSÖKNING

Tabell 4. Fortsatt ”öppen” kodning.

Nu övergår analytikern till att återigen analysera de begrepp som finns med som koder. Som resultat ritas Figur 1.



Figur 1. Begreppsanalys där analytikern hittar kärnbegreppet LÖNNMORD.

Analytikern inser att LÖNNMORD är en mänsklig aktivitet som förklarar varför alla filerna är intressanta för laptopens användare. Denna kod kallas i fortsättningen för kärnbegreppet.

Analytikern fortsätter att koda men nu används kärnbegreppet och de koder som är kopplade till kärnbegreppet så mycket som möjligt. Syftet med den fortsatta

kodningen är att testa kärnbegreppets giltighet som förklaringsmodell – inte att skapa fler koder. Den fortsatta kodningen producerar Tabell 5.

Filnamn	Koder
Svenska Armborstunionen SAU	LÖNNMORD, METOD
DNA_analys_metoder	LÖNNMORD, RISK
Fallolyckor i hemmet	LÖNNMORD, METOD, OLYCKA

Tabell 5. ”Selektiv” kodning där kärnbegreppets förklaringskraft testas.

När fortsatt kodning inte gör att kärnbegreppet eller relaterade begrepp ändras är arbetet klart och analytikern har hittat en grundad teori för vad laptopens ägare är intresserad av.

Det inledande exemplet har förhoppningsvis gett läsaren en känsla för hur Grundad teori kan användas. Nu övergår vi till en mer systematisk beskrivning av Grundad teori och hur den kan användas vid underrättelseanalys.

Grundad teori är en av de mest använda kvalitativa forskningsmetoderna och används främst i beteendevetenskaper men även i ekonomisk vetenskap och sporadiskt i underrättelseanalys [15], [16]. Metoden uppfanns av de amerikanska sociologerna Barney Glaser och Anselm Strauss på 1960-talet. Senare utvecklade Glaser den klassiska grundade teorin som översiktligt beskrivs här medan Strauss tillsammans med Juliet Corbin skapade en alternativ metod som är mer systematisk och mindre intuitiv än Glasers metod. Skillnaden mellan skolorna är inte viktig i detta sammanhang men bidrar till att litteraturen i området framstår som svårgenomtränglig.

Vid användning av Grundad teori är målet att förstå människors beteende i det sammanhang som studeras. Man vill ha svar på frågor som ”Vilket är människornas problem och hur försöker de lösa det?”. Svaret är ofta en beskrivning av den viktigaste sociala processen i sammanhanget. En viktig förutsättning är att det inte från början finns någon hypotes som skall bekräftas, falsifieras eller sannolikhetsbedömas. Enligt Grundad teori skall man undvika att skapa hypoteser eller detaljerade forskningsfrågor genom egna gissningar eller litteratursökning. Analysprocessen går i stället ut på att skapa en hypotes genom att arbeta med data.

Det första steget i processen är att *datainsamling* t.ex. från intervjuer, fältanteckningar, och arkivsökningar. Data organiseras som diskreta block där ett datablock kan vara en textrad, en kort intervju eller en ljudfil. I vårt exempel var filnamnen datablock.

Nästa steg är *öppen kodning* där varje datablock annoteras med koder som anger viktiga saker, händelse eller egenskaper. Kodningen utförs intuitivt av analytikern själv och utvecklas kontinuerligt genom att analytikern efter hand jämför kodningen av det aktuella blocket med föregående kodningar och därmed ser nya samband och möjligheter till generaliseringar och specialiseringar. Under den öppna kodningen upptäcker analytikern de begrepp som är relevanta i sammanhanget.

Kodningen varvas med *begreppsanalys* där analytikern skriver s.k. *memon* som sammanfattar hur de begrepp som används vid kodningen förhåller sig till varandra. Här anges relationer mellan begrepp som t.ex. att BIL är en specialisering av FORDON, att BIL kan ha attributet FÄRG eller att RESA är en process där BIL kan användas. Vid begreppsanalysen byggs med andra ord en preliminär ontologi som använder de begrepp som upptäcks vid kodningen.

Genom att växla mellan öppen kodning och begreppsanalys upptäcker analytikern så småningom *kärnbegreppet* som typiskt identifierar den centrala sociala process som förklarar nästan allt som händer i sammanhanget. I vårt exempel ovan är LÖNNMORD kärnbegreppet. Kärnbegreppet skall väljas på så hög abstraktionsnivå att det hamnar i toppen av begreppshierarkin som byggs i begreppsanalysen. Därför väljs LÖNNMORD och inte OLYCKA i exemplet. Analytikern skall inte hitta på något som inte finns i data genom att specialisera onödigt mycket t.ex. genom att välja kärnbegreppet FÖRBEREDELSE FÖR LÖNNMORD. Datorn kanske ägs av en student i kriminologi som skriver uppsats om lönnmord. Analytikern skall inte heller välja en högre abstraktionsnivå än vad som behövs för att förklara data. De övriga begrepp som har skapats under den öppna kodningen relateras i en avslutande begreppsanalys så mycket som möjligt till kärnbegreppet. Vissa begrepp är inte relaterade till kärnbegreppet och används då inte i den fortsatta analysen.

Nu övergår analytikern till *selektiv kodning* där datablock bara annoteras med kärnbegreppet och begrepp som står i relation till kärnbegreppet t.ex. genom att specialisera kärnbegreppet eller vara attribut till kärnbegreppet. Under denna fas testas kärnbegreppets förmåga att förklara nya data. Den selektiva kodningen varvas med begreppsanalys där kärnbegreppet, relaterade begrepp och relationer kan modifieras.

När en följd av datablock har kodats selektivt utan att kärnbegreppet eller dess relaterade begrepp har förändrats har *teoretisk mättnad* uppnåtts. Analytikern har nu hittat hypotesen som är den grundade teorin. Kärnbegreppet är den sociala aktivitet som förklarar nästan allt som händer i det sammanhang som data beskriver. Det återstår nu bara att förfina och dokumentera resultatet. Under denna fas kan det vara relevant att ytterligare kartlägga relationerna mellan de centrala begreppen vilket ibland kan kräva kompletterande datainsamling. I denna *teoretiska fas* kan teorin även relateras till annan kunskap som t.ex. akademisk litteratur.

En intressant aspekt av metoden är att när ett datablock har kodats så används bara koderna i den fortsatta analysen. Metoden kan därför användas i situationer där data inte går att registrera permanent exempelvis då analytikern arbetar med intervjuer som inte får spelas in och det inte är praktiskt möjligt att göra omfattande anteckningar.

Grundad teori har inte som mål att hitta den ”sanna” förklaringen utan är till för att generera nya hypoteser om man inte har någon eller vill ha fler hypoteser. Om det behövs ett kvantitativt beslutsunderlag kan de hypoteser som skapas med Grundad teori underkastas statistisk analys t.ex. enligt någon av de hypotestestande metoder som beskrivs i denna rapport. För den som vill lära sig mer om Grundad teori med fokus på att använda metoden rekommenderas i första hand Hartmans bok [15].

Fördelar	Nackdelar
1. Metoden är mycket flexibel 2. Kräver ingen utbildning om teoretiska ramverk eller tekniska hjälpmedel 3. Begränsar ej vilka hypoteser analytikern kan komma fram till 4. Leder alltid till ett resultat	1. Metoden hittar bara en hypotes utan att kvantifiera hur väl data stöder hypotesen 2. Försöker inte kartlägga vilka olika hypoteser som har stöd av data. Olika analytiker kan komma fram till olika hypoteser utan att det med hjälp av metoden går att avgöra vilken hypotes som har bäst stöd av data 3. Även om metoden gör anspråk på att skapa hypoteser som är oberoende av förutfattade meningar går det inte att undvika att analytiker har ett omedvetet teoretiskt bagage som påverkar resultatet

2.2.4 Tillämpningar och erfarenheter

I litteraturen om Grundad teori påpekas ofta att analytikern måste frigöra sig från förutfattade meningar och inlärda teorier så att den grundade teorin kan formas av information som finns i data. Det är naturligtvis omöjligt att helt befria sig från teoretisk ballast. Även om analytikern följer alla råd och regler finns det

alltid undermedvetna tankemönster som påverkar processen. Olika analytiker som arbetar med samma data kommer därför ofta fram till olika grundade teorier.

Ett centralt antagande i Grundad teori är att det alltid finns ett kärnbegrepp – en social process som förklarar nästan allt som händer. Det är lätt att komma på exempel på situationer där flera sociala processer växelverkar. En by i ett konfliktområde kan samtidigt präglas av en klanfejd och av spänningar mellan lokalbefolkning och ett företag som utvinner olja. Om man ser Grundad teori som ett verktyg för att skapa hypoteser för vidare prövning så begränsar inte kravet på att identifiera ett kärnbegrepp analytikerns förmåga att förstå komplexa situationer.

I litteraturen framhävs att grundad teori bör resultera i hypoteser som är modifierbara d.v.s. kan anpassas så att den stämmer med nya data. Målet för underrättelseanalys är emellertid ofta att förutsäga framtida hot och möjligheter inte att hypotesen ska överleva konfrontation med verkligheten. En hypotes som smidigt kan anpassas till vilka nya data som helst saknar förmåga att peka ut en specifik framtida händelseutveckling – den stämmer ju med allt som kan hända. En hypotes som inte är modifierbar förutsäger däremot mycket specifika hot och möjligheter. Underrättelseanalytiker bör sträva efter att göra modeller som är så specifika som möjligt.

Litteraturen om grundad teori lider av en förvirrande terminologi, delvis för att det finns två konkurrerande fraktioner som använder olika begrepp. Kärnbegreppet kallas t.ex. ibland för kärnvariabeln. Begreppsanalys kallas ibland för axiell kodning. I denna beskrivning har vi försökt införa en lättbegriplig terminologi till priset av att vi inför några termer som inte är de normala i akademisk litteratur.

Kodningen och begreppsanalysen liknar mycket att bygga en ontologi från data. Kärnbegreppet med omgivande begrepp kan förstås som den minimala ontologi som behövs för att förklara det viktigaste händelseförloppet. Chou, Zahedi och Zhao använde Grundad teori för att skapa en ontologi för katastrofhantering [17]. En intressant forskningsmöjlighet är att undersöka om Grundad teori delvis kan automatiseras med hjälp av semantiska metoder och verktyg.

På FOI finns det inte någon stor erfarenhet av att använda Grundad teori förutom en kortfattad diskussion i Per Agrells avhandling från 1992 [18]. Per Wikberg använder Grundad teori för design av fallstudier vilket beskrivs i en kommande rapport.

Grundad teori används mycket inom samhällsvetenskaplig och psykologisk forskning men vi har i öppna källor hittat relativt få användningsexempel med anknytning till underrättelseanalys. Här följer några axplock. MacLeod använder Grundad teori tillsammans med andra metoder för att studera attacker på frivilligorganisationer i Afghanistan 2005-2006 [19]. Grundad teori användes i flera magisteruppsatser vid Naval Postgraduate School. Miller kartlägger t.ex.

behoven av underrättelsearbete inom ”Homeland Security” med hjälp av Grundad teori [20]. I en annan magisteruppsats använder Wineera Grundad teori för att analyser Nya Zeeländska erfarenheter av underrättelsearbete i fält [21].

2.2.5 Teknikstöd

Grundad teori utvecklades med tanke på forskare som arbetar utan teknikstöd. Den arbetsform som rekommenderas av metodens pionjärer bygger på kodning för hand i marginalen av utskrivna data och lättsorterade anteckningar på indexkort. Detta arbetssätt ligger väl i linje med den intuitiva arbetsstilen som vädjar till analytikerns kreativitet och förmåga till överblick. Det är inte uppenbart att ett datorbaserat arbetssätt är effektivare utan behovet av datorstöd bör bedömas för varje analysprojekt baserat på hur omfattande materialet är, behov av spårbarhet och hur många analytiker som är inblandade.

För den som önskar arbeta med datorstöd finns det många mjukvarupaket som stödjer kvalitativ dataanalys inklusive Grundad teori. CAQDAS är ett projekt som drivs av universitetet i Surrey med syfte att utveckla och informera om datorstöd för kvalitativ analys[3]. Bland annat tillhandahålls en online-guide för att välja mjukvara för kvalitativ analys. CAQDAS erbjuder också en jämförandet granskning av mjukvaror[4]. Koenig diskuterar programpaketens relation till forskningsmetoder och hävdar att Grundad teori ofta är vägledande för programmens funktion [22]. Ett annat mjukvarupaket som stödjer kvalitativ analys är Atlas.ti[5].

Som exempel på program som fokuserar på att stödja analys baserad på grundad teori kan vi nämna Kwalitan[6] och Atlas.ti [16]. Den mest användbara funktionen i Kwalitan verkar vara automatisk sökning och filtrering baserat på koder samt vyer som ger överblick över vilka koder som har använts. Frekvensanalys av koder och ord i dataunderlaget är också användbart vid kodning och analys. Atlas.ti erbjuder drag-and-drop kodning och ett grafiskt verktyg för att utforska relationer mellan koder.

[3] www.surrey.ac.uk/sociology/research/researchcentres/caqdas/
[4] www.restore.ac.uk/lboro/research/software/caqdas_comparison.php
[5] www.atlasti.com
[6] www.kwalitan.nl/engels/index.html

2.3 Attackträd

Modellegenskaper: Modelldriven, kvalitativ, hypotesskapande/hypotestestande

2.3.1 Användningsområden

Attackträd passar bra att använda när man har ett klart definierat mål och på ett strukturerat sätt vill analysera möjliga sätt att nå målet. Attackträdet används då för att identifiera så många olika sätt att nå målet som möjligt.

Attackträd har använts framför allt för att modellera säkerheten hos system. Detta sker genom att man försöker hitta alla möjliga tänkbara attacker mot systemet. Man kan med fördel använda attackträd som modell då man studerar säkerheten i ett nätverk, en banks datasystem eller i ett kryptosystem.

Problem där attackträd kan användas

1. När man vill identifiera möjliga attacker mot ett system.
2. För att analysera hur man ska använda motmedel mot attacker.

2.3.2 Nödvändiga förutsättningar

- För att kunna använda attackträd måste man ha god kännedom om olika sätt på vilka målet kan nås. Arbetet sker lämpligtvis i en grupp av experter.

2.3.3 Beskrivning av metoden

Attackträd används t.ex. då man på ett systematiskt sätt vill gå igenom olika möjliga händelseförlopp för att på så sätt kunna identifiera risker och svagheter i ett system. Attackträd är hierarkiska grafiska diagram och i likhet med många andra typer av trädmodeller (som t.ex. Wigmoreanska träd) är attackträd inverterade med en rotnod i toppen. Rotnoden representerar en potentiell angripares slutgiltiga mål. Trädets lövnoder är den lägsta nivå på aktivitet som angriparen kan utföra. Mellanliggande noder representerar delattacker.

Ett attackträd är en graf utan cykler (loopar). Det finns två typer av noder i ett attackträd: *och*-noder samt *eller*-noder. Att en nod är satisfierad betyder att antingen alla nodens barn är satisfierade (*och*-nod) eller att minst ett av nodens barn är satisfierad (*eller*-nod).

När man har skapat ett attackträd kan det analyseras för att ge mer information om säkerheten i systemet. Detta görs genom att olika attribut anges för

Fördelar	Nackdelar
1. Lättförståelig grafisk representation 2. Erbjuder ett strukturerat arbetssätt för att identifiera möjliga attacker mot ett givet mål 3. Möjlighet att resonera om attacker utifrån exempelvis deras kostnad eller svårighet att genomföra 4. Relativt enkla matematiska beräkningar	1. Hanterar inte cykler i den enklaste varianten 2. Omöjligt att veta om alla attacker identifierats 3. Kan bli stora och svåra att överblicka

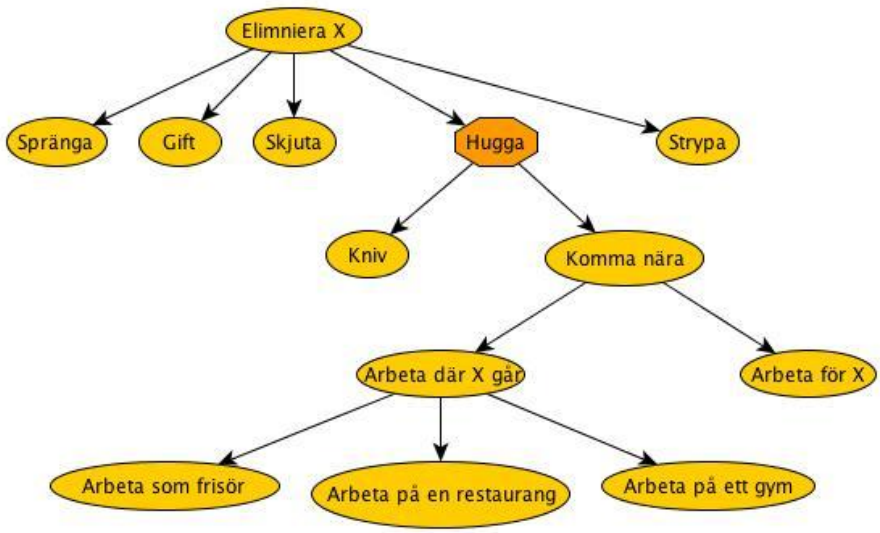
lövnoderna. Attributen kan vara kostnad för att utföra aktiviteten, kunskapsnivå för att utföra aktiviteten eller om det över huvud taget är möjligt att genomföra aktiviteten.

Genom relativt enkla beräkningar kan man svara på frågor som: är någon attack möjlig? Vad är den minsta kostnaden för att göra en attack? Vad är den minsta nivå på kunskap som behövs för att kunna utföra en attack?

2.3.3.1 Exempel

Figur 2 visar ett attackträd som modellerar olika sätt att eliminera person X. Syftet med attackträdet är att identifiera och därmed kunna förhindra så många möjliga attacker mot X som möjligt. En angripare kan eliminera X genom att antingen spränga X, få X att ta gift, skjuta X, hugga ihjäl X eller strypa X. För att kunna hugga ihjäl X måste angriparen emellertid ha en kniv och komma tillräckligt nära för att kunna använda kniven. För att kunna komma nära X (om vi antar att X är en person som står under ständig bevakning) måste angriparen antingen arbeta åt X eller arbeta på något ställe som X besöker. De enda ställen som X besöker är frisörer, restauranger och gym.

I Figur 3 analyseras om det är möjligt att eliminera X. Aktiviteterna ”arbeta som frisör”, ”arbeta på en restaurang” och ”arbeta på ett gym” anses som möjliga (”possible”) och har därför märkts med *P*. Aktiviteten ”Arbeta för X” har ansetts omöjlig (”impossible”) och har därför märkts med *I*. Eftersom vi kan komma nära X genom att ”arbeta där X går” märks noden ”Komma nära” med *P*. En kniv anses vara möjlig att införskaffa och således går *och*-noden ”hugga” också att satisfiera. Detta innebär att det finns en möjlig attack mot X:s säkerhet.



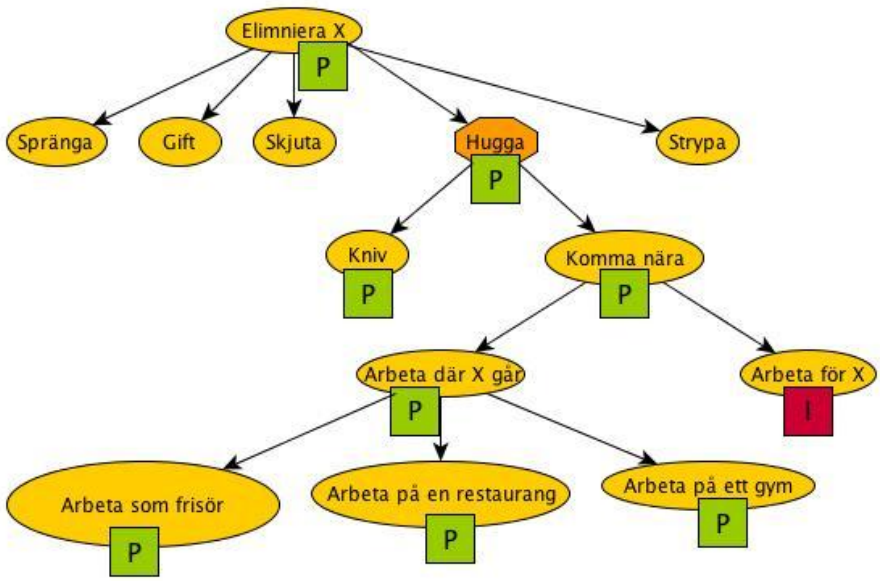
Figur 2. Ett (ofullständigt) attackträd som modellerar olika sätt att eliminera en person X. Alla noder är *eller*-noder förutom ”Hugga” som är en *och*-nod.

2.3.3.2 Relaterade modeller

Felträd är en grafisk modell som är nära relaterad till både attackträd och Wigmoreanska träd (se kapitel 2.4 *Wigmoreanska träd*). Precis som attackträd har felträd *och*-noder samt *eller*-noder. Vid varje lövnod anges en *a priori*-sannolikhet (i förväg uppskattad, baserad på redan existerande kunskap) för att den händelsen ska inträffa. När man analyserar felträd beräknar man sannolikheten för att en attack ska inträffa. I attackträd används traditionellt sett andra typer av mått för att värdera attacker. Detta beror på att attackträden skapats för att användas inom områden där man inte har tillgång till a priori-sannolikheter för händelser och där man alltså inte kan göra någon initial bedömning av sannolikheten.

Felträd lämpar sig för system med ett flertal komponenter där man har statistik över hur troligt det är att en enskild komponent går sönder. Felträd används bland annat för analys av säkerheten i kärnkraftverk och flygplan. Typiska händelser som är lämpliga att analysera med felträd är ”explosion i systemet” och ”utebliven produktion”. Lövnoderna motsvarar då aktiviteter som exempelvis ”radiator går sönder”, ”läcka i rör” och ”temperatur kan inte kontrolleras”.

Händelseträd (*Event trees*) är en annan grafisk modell som är nära besläktad med attackträd. I ett händelseträd utgår man från en händelse och identifierar och kvantifierar sedan möjliga händelseförlopp.



Figur 3. Ett attackträd där aktiviteterna har märkts med *P* om de anses vara möjliga och *I* om de anses vara omöjliga. För att svara på frågan ”Är det möjligt att eliminera X?” analyseras varje stig i attackträdet. Beroende på vilken fråga som ställs, vilka attribut som används och vilken typ noden har beräknas ett värde för varje enskild nod.

2.3.4 Tillämpningar och erfarenheter

2.3.4.1 Allmänt

Attackträd introducerades av Bruce Schneier [23] och formaliserades av Mauw och Oostdijk [24].

2.3.4.2 På FOI

På FOI har vi arbetat med en utökning av attackträd som kallas attackdjungler (attack jungle) [25]. Denna formalism tillåter träden att ha multipla rötter (flera mål), cykler och återanvändbara (reusable) noder. En nod som är återanvändbar kan användas i flera attacker. Ett exempel på en återanvändbar nod är en hemlig kryptografisk nyckel som kan återanvändas i ett flertal attacker eftersom man i vissa fall både kan läsa krypterade meddelanden och skicka krypterade meddelanden om man har en hemlig nyckel.

En mer ingående beskrivning av hur attackträd kan användas för underrättelsearbete finns beskrivet i [26].

2.3.5 Teknikstöd

Ett flertal kommersiella verktyg för attackträd finns på marknaden. Ett är AttackTree+ från Isograph[7], ett annat är SecurITree från Amenaza Technologies[8].

2.4 Wigmoreanska träd

Modellegenskaper: Modelldriven, delvis kvantitativ, hypotestestande

2.4.1 Användningsområden

Wigmoreanska träd, ibland även kallade pyramidmodeller, används för att på ett strukturerat sätt bryta ned komplexa hypoteser i mindre delhypoteser. Genom denna typ av nedbrytning får analytikern stöd i att välja ut indikatorer vars tillstånd ska inhämtas eller bedömas. Metoden kan även användas för att göra enklare kvantitativa bedömningar av de ingående hypoteserna. Det finns flera olika analytiska metoder som fokuserar på nedbrytning och är mycket lika den som beskrivs här. Ett sådant exempel är Strukturerad argumentation [27], som används i analysverktyget High SEAS.

Problem där Wigmoreanska träd kan användas

1. Sannolikheten för att en viss komplex hypotes ska inträffa (eller har inträffat) ska bedömas och analytikern behöver stöd för att resonera om denna. Exempel på sådana komplexa hypoteser/påståenden kan vara att:
    a. ”det kommer att ske en attack mot president X” eller
    b. ”al Qaeda har tillgång till kärnvapen”.
2. Inhämtningsplanering för att kunna svara på ett informationsbehov eller en RFI[9]. Wigmoreanska träd kan användas för att avgöra vilka indikatorer det är mest angeläget att samla in information om.

2.4.2 Nödvändiga förutsättningar

1. Hypoteser ska kunna brytas ned i mindre delhypoteser

Denna form av nedbrytning bygger på så kallad ”divide and conquer”-metodik (söndra och härska). Ett sådant reduktionistiskt synsätt är lämpligt att använda då hypotes eller ett system kan brytas ned i och

[7] www.isograph-software.com
[8] www.amenaza.com
[9] RFI – Request For Information; Informationsförfrågan

förklaras av sina beståndsdelar. Det är dock viktigt att vara uppmärksam på att mer holistiska synsätt kan krävas för andra typer av hypoteser (där ”summan är större än de enskilda delarna”).

2. **Sannolikheten för en hypotes ska kunna beskrivas som en funktion av tillståndet av de delhypoteser som denna kan brytas ned i.**

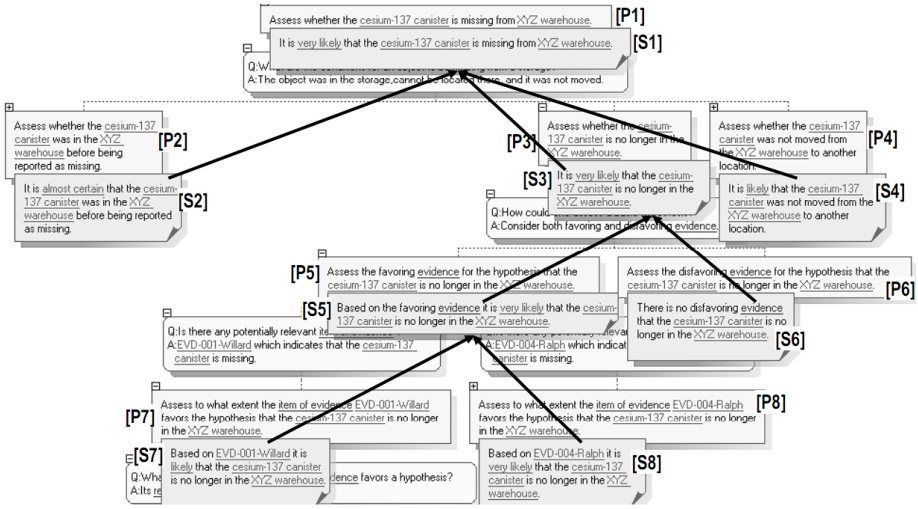
   För att kunna använda Wigmoreanska träd fullt ut ska sannolikheten för att en hypotes H_1 inträffat eller kommer att inträffa kunna beskrivas som en enkel matematisk funktion av dess delhypoteser H_{11}, H_{12}, …, H_{1n}. Vanligtvis används funktioner så som MAX, MIN eller medelvärde (AVG), det vill säga att tillståndet för en hypotes bestäms utifrån den delhypotes som talar mest för (MAX) eller mest emot (MIN) hypotesen, alternativt som ett medelvärde av de ingående delhypoteserna (se kapitel 2.4.3 *Beskrivning av metoden* nedan för en mer utförlig förklaring). Wigmoreanska träd kan dock vara mycket användbara även utan att kvantitativa aspekter tas med; istället använder man den som en rent kvalitativ modell.

3. **Alla faktorer som talar för respektive emot en hypotes ska kunna identifieras och modelleras.**

   Det är viktigt att analytikern tar sig tid att tänka igenom och skapa en så korrekt och heltäckande modell som möjligt, eftersom det annars finns en risk att modellen begränsar analysen.

2.4.3 Beskrivning av metoden

Wigmoreanska träd används för att bedöma troligheten (sannolikheten) för en viss hypotes. För att kunna bedöma troligheten för hypotesen bryter analytikern ner denna i ett antal mindre delhypoteser eller delproblem. Nedbrytningen pågår till dess att man når delhypoteser som kan utgöra indikatorer, dvs. sådana som man direkt kan bedöma troligheten på alternativt inhämta evidens för eller emot. För varje inhämtad evidens bedöms dess relevans och tillförlitlighet utifrån den typ av underrättelsekälla som evidensen härstammar ifrån. I nästa steg vägs evidens för och emot en indikator samman, så att en trolighet för indikatorn baserad på tillgänglig evidens räknas fram. Detta upprepas för alla indikatorer, varpå dessa vägs samman för att bedöma troligheten av de ovanliggande delhypoteserna, osv., ända tills att en trolighet för den ursprungliga hypotesen erhållits. Sammanvägningen kan ske på ett antal olika sätt och det är upp till analytikern att modellera hur denna typ av sammanvägning ska göras. Generellt sett används dock bara, vilket nämnts ovan, ett antal enkla matematiska funktioner så som MIN, MAX och medelvärde (AVG), det vill säga att tillståndet för en hypotes bestäms utifrån den delhypotes som talar mest för eller mest emot



Figur 4. Exempel på ett Wigmoreanskt träd (från [31])

hypotesen, alternativt som ett medelvärde av de ingående delhypoteserna. En vidare förklaring av vad detta innebär kan erhållas genom att studera Figur 4. I detta exempel har den komplexa hypotesen P1, om huruvida en dosa med radioaktivt Cesium-137 försvunnit från ett lager, brutits ned i delproblemen P2, P3 och P4. P3 har brutits ned i P5 (evidens som talar för P3) samt P6 (evidens som talar emot P3). Två evidens som talar för P3 har identifierats, så P5 bryts ned i P7 samt P8, vilka består i delproblemen med att bedöma i vilken grad dessa talar för hypotes P3. Analytikern gör efter analys av dessa evidens bedömningen att de indikerar att det är ”troligt” respektive ”mycket troligt” att P3 är sann (S7 respektive S8). Dessa fusioneras samman genom användandet av en MAX-funktion som analytikern valt, vilket gör att S5 antar det högsta värdet av ”troligt” och ”mycket troligt”, det vill säga att den får värdet ”mycket troligt”. För P6 hittas ingen evidens som talar emot hypotesen, varför S3 får samma värde som S5. Samma typ av resonemang förs för P2 respektive P4 (ej synliga i figuren), vilket gör att S2 antar värdet ”nästan säkert” och att S4 antar värdet ”troligt”. Dessa fusioneras slutligen ihop med hjälp av en AVG-funktion, vilket gör att S1 antar medelvärdet ”väldigt troligt”.

2.4.3.1 Exempel

För att exemplifiera metoden kan vi tänka oss att en analytiker vill testa hypotesen: ”En självmordsattack kommer att ske mot en polisstation i Mazar-e Sharif i Afghanistan”. Analytikern får då fundera igenom vilka faktorer som ska vägas in för att bedöma detta. De framkomna svaren blir till delproblem (t.ex. ”Analysera om någon har motiv att utföra en självmordsattack mot en polisstation i Mazar-e Sharif”, ”Analysera om någon har förmåga att utföra en

Fördelar	Nackdelar
1. Lättförståelig grafisk representation 2. Erbjuder ett strukturerat arbetssätt för nedbrytning av hypoteser i mindre problem eller delhypoteser 3. Inte matematiskt komplex 4. Väldigt låg beräkningskomplexitet	1. De enkla matematiska funktionerna som erbjuds gör att metoden svårligen lämpar sig för automatiskt beslutsstöd 2. Endast relativt grova modeller kan byggas med hjälp av Wigmoreanska träd, jämfört med exempelvis Bayesianska nätverk

självmordsattack mot en polisstation i Mazar-e Sharif", etc.). När ett problem inte kan brytas ner längre så ska analytikern koppla samman evidens som talar för respektive emot indikatorerna, samt utvärdera källans pålitlighet samt evidensens relevans. Utifrån denna information bedöms troligheten hos ovanliggande delhypoteser, vilka i sin tur används för att bedöma troligheten hos den ursprungliga hypotesen. På detta sätt "tvingas" analytikern arbeta på ett strukturerat sätt och man får även spårbarhet i varför en viss bedömning gjorts.

2.4.4 Tillämpningar och erfarenheter

2.4.4.1 Allmänt

Det finns flera publikationer som beskriver användningen av Wigmoreanska träd för underrättelseanalys. Många av författarna tillhör Gheorghe Tecuci's forskargrupp på George Mason University och publikationerna beskriver systemen Disciple-LTA och TIACRITIS (se kapitel 2.4.5 *Teknikstöd* nedan). Ett urval av de aktuella publikationerna ges av referenserna [31]-[34].

2.4.4.2 På FOI

På FOI har erfarenhet av Wigmoreanska träd (pyramidmodeller) erhållits genom en del av det arbete som utförts med FOI-verktyget Impactorium [35]. Även om Impactorium har funktionalitet som gör det möjligt att arbeta med mer avancerade modeller (Bayesianska nätverk) så har Wigmoreanska träd i många sammanhang visat sig vara mer praktiskt användbara.

Vid en intern FOI-workshop 2010 genomfördes ett test där två olika grupper fick i uppgift att skapa var sin hotmodell utifrån ett givet scenario. Den ena gruppen fick använda Bayesianska nätverk, medan den andra gruppen använde Wigmoreanska träd. Studien var för liten för att kunna dra några generella slutsatser, men gruppernas gemensamma intryck var att det för personer med

begränsad träning är enklare att skapa ett Wigmoreanskt träd än ett Bayesianskt nätverk. Vid hypoteser vars trolighet ska prövas en enda gång ansågs det gå betydligt snabbare och smidigare att skapa ett Wigmoreanskt träd, däremot sågs den större detaljeringsnivån hos det Bayesianska nätverket som en positiv egenskap för fall där en framtagen hotmodell kunde återanvändas vid flera tillfällen.

2.4.5 Teknikstöd

I Impactorium [35] finns stöd för att manuellt skapa hotmodeller i form av Wigmoreanska träd. Användaren måste själv göra nedbrytningen och framtagandet av modellen, men Impactorium gör det lätt att lägga till nya noder, välja vilken funktion för sammanvägning som ska användas och utföra beräkningarna.

Wigmoreanska träd har av forskare vid George Mason University (ledda av professor Gheorghe Tecuci) implementerats i systemen TIACRITIS och Disciple-LTA som används både för att lära ut underrättelseanalys till nya analytiker och som stödsystem av mer erfarna analytiker. Utöver att göra själva beräkningarna av hur troliga olika hypoteser är sett i ljuset av insamlat underlag så erbjuder systemen även viss funktionalitet för att semi-automatiskt hjälpa till med själva nedbrytningen av hypoteser i mindre delhypoteser, samt att identifiera relevanta informationsobjekt.

2.5 Bayesianska nätverk

Modellegenskaper: Modelldriven (finns även som datadriven variant där modellen lärs in från data), kvantitativ (och till viss del kvalitativ), hypotestestande

2.5.1 Användningsområden

Ett Bayesianskt nätverk är en matematisk modell med grafisk tolkning som beskriver hur olika variabler påverkar varandra genom sekvenser av *kausala samband* (se förklaring nedan). Bayesianska nätverk används för att skatta sannolikheten för hypoteser, tillstånd eller händelser utgående från tillgänglig information om relaterade fenomen.

Problem där Bayesianska nätverk kan användas

1. Bayesianska nätverk kan användas för att söka troliga förklaringar till händelser och observationer. T.ex. har Bayesianska nätverk använts för att stödja felsökning av exempelvis datorskrivare och bilar. Felsökningsprocessen börjar med att man modellerar hur möjliga felkällor i det aktuella systemet via långa eller korta händelsekedjor kan

resultera i olika observerbara symptom. Genom att ställa upp modellen som ett Bayesianskt nätverk kan man direkt utnyttja den till att beräkna vilken felkälla som är mest trolig att orsaka exakt de fel som observerats. Kunskap om att en viss del av systemet fungerar kan matas in i nätverket för att uppdatera sannolikheterna för fel i någon annan del [36].

2. Bayesianska nätverk kan också användas för att skatta sannolikheten för framtida händelser eller händelseförlopp, som t.ex. sannolikheten för att en konflikt i ett insatsland ska eskalera (se exempel i avsnitt 2.5.3.1).

2.5.2 Nödvändiga förutsättningar

1. Tillstånd kan modelleras som stokastiska variabler

Problemet som ska behandlas måste vara uppställt så att varje händelse eller tillstånd av intresse representeras grafiskt som en nod i det Bayesianska nätverket (se exempel på ett Bayesianskt nätverk i Figur 5). Varje nod måste i sin tur kunna knytas till en variabel som talar om vilket tillstånd noden har.

Exempel: *En nod som representerar en viss händelse är knuten till variabeln X. X är en binär variabel som kan anta ett av två möjliga värden. X=true betyder att händelsen inträffar, X=false betyder att händelsen inte inträffar.*

Tillståndsvariabler i Bayesianska nätverk är s.k. *stokastiska variabler*, d.v.s. i den matematiska representationen av nätverket associeras varje tillståndsvariabel med en sannolikhetsfunktion (se beskrivning nedan) som tilldelar en viss sannolikhet till varje tänkbart tillstånd noden kan anta.

2. Kausala samband mellan noderna

Noderna i ett Bayesianskt nätverk kan påverka varandra. Alla samband mellan noder är *kausala*, d.v.s. de har en riktning och beskriver orsak-verkan-samband av typen ”tillståndet i nod A påverkar tillståndet i nod B med sannolikhet x”. Om en nod påverkar en annan nod visas detta i den grafiska modellen med en pil.

3. Inga cykler i nätverket

Beräkningar med Bayesianska nätverk kan inte utföras om det finns cykler, ”rundgång”, av beroenden mellan noderna, såsom att nod 1 påverkar nod 2 som påverkar nod 3 som i sin tur påverkar nod 1.

2.5.3 Beskrivning av metoden

Ett Bayesianskt nätverk kan betraktas som en grafisk modell med en underliggande matematisk representation. I den grafiska modellen används noder för att representera tillstånd/händelser, medan pilar används för att visa hur dessa händelser och tillstånd påverkar varandra. Den påverkan en nod har på en annan nod är förknippad med en viss osäkerhet. Denna typ av osäkerhet hanteras i Bayesianska nätverk med hjälp av kända statistiska samband. I den här rapporten kommer vi inte att förklara de fullständiga matematiska detaljerna utan vi nöjer oss med att beskriva översiktligt hur ett Bayesianskt nätverk fungerar. Trots detta kräver beskrivningen ett visst matematiskt kunnande, men förhoppningen är att principerna ändå ska kunna förstås av alla läsare. För en fullständig redogörelse av matematiken bakom modellen hänvisas läsaren till [37]. Som en ytterligare förenkling har vi valt att endast betrakta nätverk vars noder har diskreta (icke-kontinuerliga) tillstånd.

Innan vi beskriver hur ett Bayesianskt nätverk fungerar måste vi förklara några grundläggande statistiska begrepp.

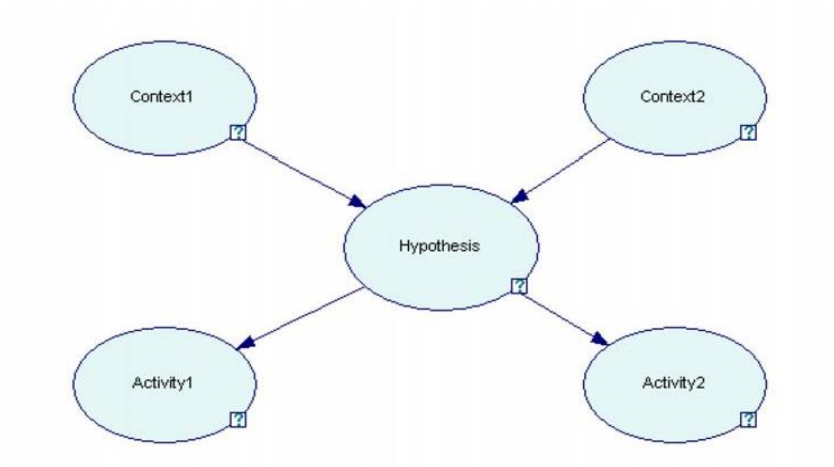
Sannolikhet: Sannolikheten för att en variabel X ska anta värdet γ betecknas $P(X= \gamma)$. Sannolikhet anges alltid som ett tal i intervallet 0 till 1 där $P(X= \gamma) = 0$ ska tolkas som att X aldrig antar värdet γ medan $P(X= \gamma) = 1$ ska tolkas som att X antar värdet = γ vid alla tillfällen då X observeras. Då man använder Bayesianska nätverk för underrättelseanalys räcker det oftast tänka på sannolikhet som en grad av ”trolighet” att en variabel har ett visst värde.

Exempel: *Antag att X är en binär variabel som kan anta värdena ”true” och ”false”. X=true betyder att en viss händelse har inträffat, X=false betyder att händelsen inte har inträffat. P(X=true)=0 betyder i detta sammanhang att det är bekräftat att händelsen inte har inträffat, P(X=true)=1 betyder att det är bekräftat att händelsen har inträffat och P(X=true)=0,5 betyder att inget av de två alternativen är mer sannolikt än det andra.*

Betingad sannolikhet: Om sannolikheten för att exempelvis variabeln X= true beror av värdet på en eller flera andra variabler så kan man definiera den *betingade sannolikheten* för X=true. Den betingade sannolikheten att X=true givet att variabeln Y=false skrivs som P(X=true|Y=false) och tolkas som ”sannolikheten att X= true om det är känt att Y=false”.

Sannolikhetsfunktion: Sannolikhetsfunktionen för den diskreta variabeln X betecknas P(X) och tilldelar en viss sannolikhet till varje tänkbart tillstånd X kan anta. I ett enkelt exempel kan vi tänka oss att *a*, *b*, *c* och *d* representerar alla möjliga värden på X. Då består sannolikhetsfunktionen P(X) av sannolikheterna P(X=*a*), P(X=*b*), P(X=*c*) och P(X=*d*). Sannolikhetsfunktionen för en variabel kan vara betingad och skrivs då som P(X|Y) om X är den aktuella variabeln och Y är den variabel som X beror av.

Med hjälp av dessa grundläggande begrepp kan vi nu beskriva metoden.

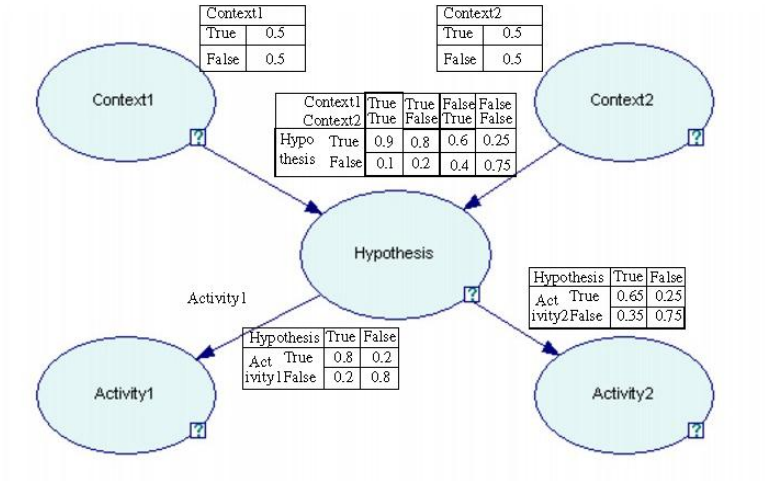


Figur 5. Ett Bayesianskt nätverk med fem noder (visualiserat med verktyget GeNIe). Noderna *Context1* och *Context2* har båda en direkt påverkan på noden *Hypothesis*, vilket visas av pilarna. Noden *Hypothesis* har i sin tur en direkt påverkan på noderna *Activity1* och *Activity2*. En effekt av detta är att noderna *Context1* och *Context2* genom hypotesnoden har en indirekt påverkan på *Activity1* och *Activity2*.

I ett Bayesianskt nätverk associeras varje nod med en variabel vars värde talar om vad tillståndet är i noden. Varje variabel har en tillhörande sannolikhetsfunktion. Om man inte känner till tillståndet hos en viss nod använder det Bayesianska nätverket nodens sannolikhetsfunktion för att beräkna sannolikheten för de olika tillstånd som noden kan ha. Om noden är kopplad till andra noder, vars tillstånd inte heller är kända, måste nodens sannolikhetsfunktion anropa sannolikhetsfunktionerna för dessa andra noder för att kunna beräkna de sökta sannolikheterna för den första noden. På så vis förs osäkerheter i systemet vidare genom nätverket.

I Figur 5 ges ett exempel på ett Bayesianskt nätverk innehållandes fem noder med tillhörande stokastiska variabler: *Context1* (med variabel C1), *Context2* (med variabel C2), *Hypothesis* (med variabel H), *Activity1* (med variabel A1) och *Activity2* (med variabel A2).

Vi antar att varje nod i detta nätverk har minst två möjliga ömsesidigt uteslutande tillstånd. Exempelvis kanske noden Activity1 är associerad med fientlig radiokommunikation och då skulle två ömsesidigt uteslutande tillstånd kunna vara *förekomst av radiokommunikation* (A1=true) och *avsaknad av radiokommunikation* (A1=false). Varje pil i nätverket visar en påverkan av en nod på en annan. Hur stark denna påverkan är måste anges av användaren i en



Figur 6. Ett Bayesianskt nätverk med fem binära variabler (variablerna kan bara ha ett av två tillstånd, *true* eller *false*). För varje nod finns en sannolikhetstabell (CPT) definierad.

tabell, en så kallad *conditional probability table*[10] (CPT). Som namnet antyder innehåller en CPT den betingade sannolikhetsfunktionen för en viss variabel i nätverket. Exempelvis finns en CPT som beskriver hur sannolikheten för hypotesvariabeln H beror av variablerna C1 och C2, alltså P(H|C1,C2). I Figur 6 visas exempel på CPT:er för alla variabler i nätverket.

I det aktuella nätverket är noderna Context1 och Context2 oberoende av andra noder. De har istället givna a priori-sannolikheter för sina möjliga tillstånd (se Figur 6). Har man inte gjort några observationer av tillstånden i nätverkets noder baseras alla beräknade sannolikheter i nätverket på a priori-sannolikheterna i noderna Context1 och Context2. Skulle man däremot känna till att t.ex. C1=true och C2=false så baseras sannolikheterna i nätverket istället på dessa värden. Sannolikhetsfunktionen för variabeln H skulle då enligt CPT för hypotesnoden ges av P(H=true)=0,8 och P(H=false)=0,2 (givet att inget är känt om tillstånden i noderna Activity1 och Activity2). Med hjälp av de betingade sannolikhets-funktionerna i CPT:erna kan man beräkna sannolikheten för valfri variabel, givet tillstånden på de noder i nätverket som kunnat observeras. Förfarandet kallas *inferens* och hur det går till i det generella fallet beskrivs i [37].

Bayesianska nätverk är, som tidigare nämnts, särskilt lämpliga att använda när man är intresserad av att skatta sannolikheten för händelser eller tillstånd som inte kan observeras, men som man vet har samband med observerbara händelser och tillstånd (indikatorer). Exempel på två sådana situationer ges i nästa avsnitt.

[10] Engelskans *conditional probability* betyder *betingad sannolikhet*.

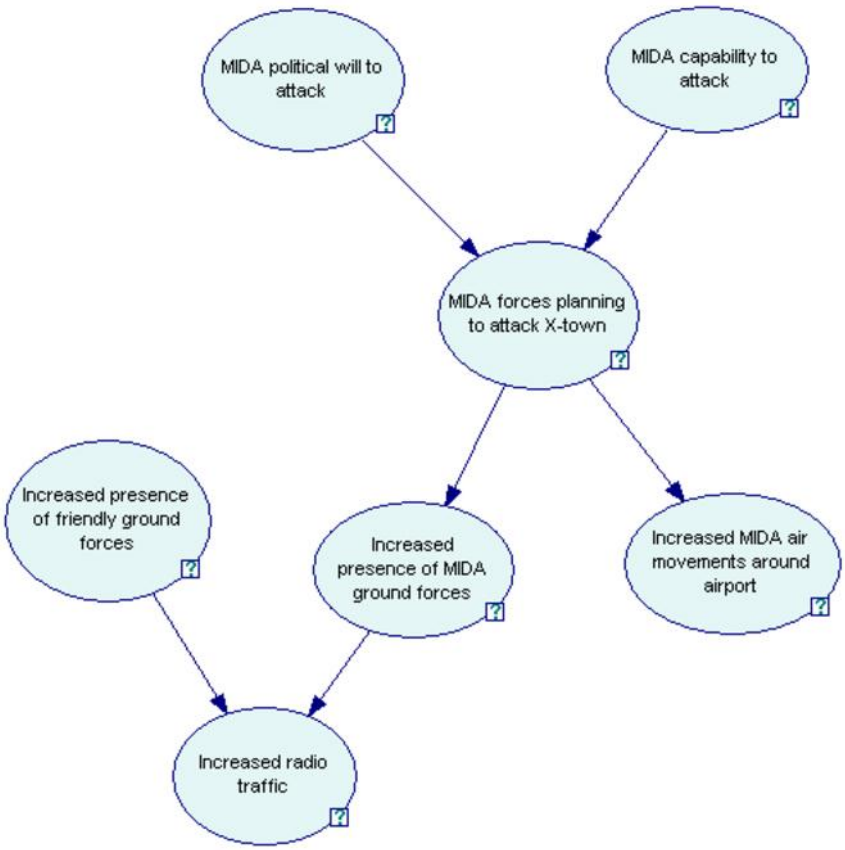
Fördelar	Nackdelar
1. Lättförståelig grafisk representation 2. Korrekt matematisk hantering av (betingade) sannolikheter 3. Kräver inte att alla observerbara variabler observeras för att sannolikheterna ska kunna uppdateras 4. Nya observationer kan läggas till utan besvärliga omräkningar	1. Svårt att skatta sannolikheterna som ska anges i CPT:erna då statistiskt underlag att basera skattningarna på saknas (mer om detta i kapitel 3.2 *Från kvalitativt till kvantitativt – Att utvinna sannolikheter ur domänkunskap*). 2. Problematiskt att hantera variabler med kontinuerliga värden 3. Svårt att hantera osäkra observationer av tillståndsnoder (med hjälp av olika trick kan man komma runt detta problem, hur det går till beskrivs dock inte i denna rapport) 4. Vanligt förekommande är att man misslyckas med att beskriva betingade sannolikheter på rätt sätt. Inom rättsväsendet finns kända fall där man nyttjat sannolikhetsargument på ett felaktigt sätt vilket har lett till felaktiga domar [38].

2.5.3.1 Exempel

Exempel 1

Vi betraktar återigen nätverket i Figur 6. Antag att nätverket är en modell av hotbilden mot en viss ambassad i ett insatsland. Värdet på hypotesvariabeln H är särskilt intressant eftersom hypotesnoden representerar en underrättelsefråga, nämligen huruvida ett terrordåd planeras mot ambassaden. I nätverket ingår förutom hypotesnoden de observerbara noderna (indikatorerna) ”Känd hotbild finns” (Context1) och ”Kartläggning av ambassaden har skett” (Activity2). Dessa noder är knutna till variablerna C1 respektive A2. Båda variablerna är binära och kan anta värdena *true* och *false*.

Man har inte fått in någon information som kan kopplas direkt till hypotesen, men via underrättelseuppgifter får man reda på att C1=”false” och A2=”true”. Så snart dessa uppgifter registreras uppdateras sannolikhetsfunktionen för hypotesvariabeln H genom att den betingade sannolikheten



Figur 7. Nedbrytning av underrättelsefrågan ”Pågår förberedelser i Mida för en väpnad attack mot den Kasuriska staden X?”.

P(H|C1=”false”,A2=”true”) beräknas. Notera särskilt att trots att tillståndet i hypotesnoden inte påverkas av tillståndet i noden Activity1så påverkas *a posteriori*-sannolikheten för hypotesnodens möjliga tillstånd av det faktum att man fått bekräftat att A2=true.

Exempel 2

En underrättelseanalytiker, stationerad i det fiktiva Bogaland, undrar om trupper från provinsen Mida planerar att attackera staden X i grannprovinsen Kasurien. Analytikern bryter ned frågan i ett antal indikatorer och relaterar dessa till den ursprungliga frågan (se Figur 7). Den grafiska modellen av den nerbrutna frågan har samma struktur som ett Bayesianskt nätverk (d.v.s. riktad graf). Modellen kan utvidgas till ett Bayesianskt nätverk genom att en matematisk representation

med beroende variabler som representerar tillstånden i noderna läggs till. Analytikern måste också specificera hur de olika variablerna är beroende av varandra genom att ställa upp en sannolikhetstabell (CPT) för varje nod i grafen. Exempel på hur man strukturerat bygger sina Bayesianska nätverk från grunden finns i Kragt [39].

Innan man gjort några observationer av indikatorernas tillstånd ger det Bayesianska nätverket en initial sannolikhet för hypotesen att en attack planeras. Sannolikheterna som angivits i nätverket får finjusteras så att den initiala sannolikheten för hypotesen blir rimlig. När sedan observationer för de olika variablerna anländer kan analytikern mata in dessa i det Bayesianska nätverket och med hjälp av detta snabbt uppskatta om sannolikheten för en förestående attack verkar minska eller öka.

2.5.4 Tillämpningar och erfarenheter

2.5.4.1 Allmänt

Litteraturen om teoretiska och praktiska tillämpningar av Bayesianska nätverk är omfattande, se t.ex. [37]. Inom området underrättelseanalys är det mer tunnsått, men exempel finns (se avsnittet nedan om tillämpningar och erfarenheter på FOI). Ett exempel är Sticha m.fl. [40]. De beskriver utvecklingen av verktyget APOLLO som är avsett att stödja underrättelseanalytikern både i processen att ta fram ett Bayesianskt nätverk och under själva användandet.

Relevant litteratur är också sådan som använder Bayesianska nätverk för att stödja diagnostik (som i fallet med felsökning av skrivare som nämns ovan).

2.5.4.2 På FOI

Bayesianska nätverk har tillämpats i olika sammanhang på FOI. Suzic [41] presenterar ett sätt att använda Bayesianska nätverk för att beskriva fientliga avsikter med hjälp av doktriner och noder som beskriver observationer av fientliga förbands beteenden. Modellen användes i ett antal följande arbeten. För beräkningar med Bayesianska nätverk användes matlabpaketet BNT[11].

Blixt m.fl. [42] har specifikt studerat Bayesianska nätverk från underrättelse-analytikerns perspektiv och har identifierat flera lämpliga tillämpningsområden. I rapporten dras slutsatsen att Bayesianska nätverk är särskilt lämpligt att använda för datafusion, bedömning av trovärdigheten hos underrättelser, samt framtagning av bedömningsunderlag. Rapporten blickar även längre tillbaka i tiden till FOI-tillämpningar av Bayesianska nätverk som vi inte tar upp här.

Ferrara m.fl. [43] har utvecklat en underrättelsemodell i form av ett Bayesianskt nätverk, vars syfte är att upptäcka misstänkta banktransaktioner.

[11] http://code.google.com/p/bnt/, besökt 2011-11-16

Johansson och Mårtensons [44] arbete är relaterat till underrättelsemodellen beskriven i exemplet ovan. Genom att analysera det Bayesianska nätverket avgörs vilken ytterligare information som måste samlas in för att förbättra situationsuppfattningen. Arbetet utnyttjar verktyget GeNIe[12] för att konstruera och arbeta med Bayesianska nätverk och utökar även GeNIe för att kunna hantera osäkra observationer.

2.5.5 Teknikstöd

Det finns idag gott om verktyg för att skapa och arbeta med Bayesianska nätverk. En del är kommersiella som Hugin[13] och Netica[14] medan andra kan användas fritt, som GeNIe. En del mjukvara förkommer i öppen form som mer eller mindre utvecklade forskningsprototyper som JavaBayes[15] (Carnegie Mellon), SamIAm[16] (UCLA) och matlabpaketet BNT (British Columbia).

Det av FOI utvecklade underrättelsestödet Impactorium [35] har också möjlighet att stödja modellering med Bayesianska nätverk.

2.6 Analys av konkurrerande hypoteser

Modellegenskaper: Modelldriven (till viss del datadriven), kvalitativ (kan göras kvantitativ), hypotestestande

2.6.1 Användningsområden

Analys av konkurrerande hypoteser (ACH)[17] är en metod som används då man har ett antal alternativa hypoteser och man på ett systematiskt sätt vill gå igenom de evidens som finns för att avgöra vilken eller vilka av dessa hypoteser som bör betraktas som mest (eller minst) trolig. Analysen görs i tabellform och huvudsyftet med metoden är att säkra att bedömningar görs på sakliga grunder.

Eftersom metoden hjälper till att synliggöra antaganden och subjektiva tolkningar av fakta är den lämplig att använda som underlag för diskussioner mellan två eller flera parter som gör olika bedömningar av det tillgängliga materialet. Den kan också användas som stöd för en analys av vilka evidens som är mest relevanta att försöka inhämta framöver.

[12] http://genie.sis.pitt.edu/ (besökt 2011-11-16)
[13] www.hugin.com/ (besökt 2011-11-16)
[14] www.norsys.com/ (besökt 2011-11-16)
[15] www.cs.cmu.edu/~javabayes/Home/ (besökt 2011-11-16)
[16] http://reasoning.cs.ucla.edu/samiam/ (besökt 2011-11-16)
[17] På engelska heter metoden ”Analysis of Competing Hypotheses”. Förkortningen ACH är vedertagen och används ofta även i svenskt tal.

Problem där Analys av konkurrerande hypoteser kan användas

- **Analys av möjliga framtida händelseutvecklingar**

  Exempel: Efter en lång period av folkliga protester faller regimen i Land X. Det finns flera grupper, både demokratiska och mindre demokratiska, som har intresse av att ta över makten i landet. En grupp av säkerhetspolitiska analytiker på FOI identifierar fem huvudhypoteser om den fortsatta händelseutvecklingen i regionen. Man använder Analys av konkurrerande hypoteser för att strukturera argument och observationer som talar för eller emot respektive hypotes.

- **Analys av möjliga förklaringar till något som inträffat**

  Vid brottsutredningar kan Analys av konkurrerande hypoteser användas för att analysera hypoteser om tillvägagångssätt, tänkbara gärningsmän, etc.

2.6.2 Nödvändiga förutsättningar

1. **Man bör inte ha mer än ca 5-7 alternativa hypoteser**

   Det finns ingen formell begränsning för hur många hypoteser som kan analyseras samtidigt med metoden, men eftersom varje hypotes analyseras manuellt i en relativt tidskrävande process kan man inte ha med mer än ett begränsat antal hypoteser, helst inte fler än 5-7 stycken.

2. **Hypoteserna måste vara ömsesidigt uteslutande**

   Två eller flera hypoteser kan inte vara sanna samtidigt.

2.6.3 Beskrivning av metoden

I korthet går Analys av konkurrerande hypoteser ut på att man identifierar alla evidens, d.v.s. alla fakta och antaganden som kan vara relevanta i sammanhanget. Sedan bedömer man i tur och ordning hur förekomsten eller avsaknaden av dessa evidens påverkar sannolikheten för var och en av de aktuella hypoteserna. Fokus ligger på att utesluta hypoteser snarare än att verifiera dem, och när analysen är klar återstår i regel ett antal möjliga hypoteser samt en analys av vilka evidens som stödjer, alternativt talar emot, respektive hypotes.

Proceduren kan beskrivas med följande steg:

1. Skriv en lista med alla aktuella hypoteser. Beskriv varje hypotes i den detalj som krävs för att man ska kunna koppla den till de evidens som finns. Notera att hypoteserna måste vara ömsesidigt uteslutande. Överväg alltid möjligheten att man utsatts för en vilseledningskampanj och om det är relevant så lägg även till detta som en separat hypotes.
2. Skriv en lista med alla evidens, inklusive antaganden och logiska argument. Glöm inte att evidens både kan utgöras av observationer och av avsaknaden av observationer som man skulle ha förväntat sig att se.
3. Sätt upp en tabell med hypoteser vs. evidens.
4. För varje kombination *Hypotes – Evidens*, skriv in en klassificering i tabellen som beskriver hur väl den aktuella evidensen stämmer med hypotesen. Använd t.ex. notationen ”- -” (talar starkt mot hypotesen), ”-” (talar mot hypotesen), ”/” (talar varken för eller emot hypotesen), ”+” (talar för hypotesen), ”+ +” (talar starkt för hypotesen), ”EA” (ej applicerbar). För att få ett rättvisande resultat måste man i det här steget väga in både evidensens trovärdighet och dess relevans för hypotesen. Om klassificeringen i något fall är beroende av yttre omständigheter så skriver man upp vilka omständigheter det rör sig om.
5. Revidera tabellen.
    a. Kan man slå ihop två eller flera hypoteser, d.v.s. formulera en (troligen mer generell) hypotes som även innefattar de tidigare?
    b. Kan man lägga till hypoteser?
6. Låt eventuellt ett datorprogram beräkna jämförelsetal för hypoteserna (läs mer om detta under rubriken *Teknikstöd* nedan).
7. Analysera resultatet.
    a. Robusthet: Testa antagandet att något eller några evidens är felaktiga, missvisande, feltolkade eller fabricerade. Håller slutsatserna ändå?
    b. Hur säkra är de eventuella antaganden som slutsatserna vilar på?
8. Sammanfatta slutsatser, gärna skriftligt. Sammanfattningen ska innehålla en diskussion om hypotesernas relativa trovärdighet.

Fördelar	Nackdelar
1. Ger en spårbarhet i analysprocessen 2. Tydliggör antaganden och subjektiva tolkningar av fakta	1. Vissa problem är svåra att modellera så att ACH kan tillämpas. Det gäller särskilt problem där det finns komplicerade beroenden mellan olika evidens och/eller mellan evidens och hypotes [45]. 2. Det är opraktiskt och svårt att behöva vikta ihop bedömningen av evidensens trovärdighet med deras respektive relevans för huvudhypotesen. 3. Det saknas tillräckliga vetenskapliga studier som visar när metoden är lämplig att använda [45,46].

9. Identifiera viktiga observationer som kan göras framöver.
    a. Evidens som stärker den nuvarande analysen - Fokusera i första hand på att hitta evidens som utesluter mindre troliga hypoteser snarare än evidens som stödjer redan sannolika hypoteser.
    b. Evidens som kullkastar eller ifrågasätter den nuvarande analysen.

Ibland stämmer inte resultaten av analysen med intuitionen. Det kan då vara en god idé att gå igenom följande punkter.

- Kan orsaken vara att du gör egna antaganden eller använder information som inte finns representerad som evidens i ACH-tabellen? Fundera i så fall på om den informationen ska inkluderas i tabellen eller om intuitionen kan vara felaktig eller baserad på förutfattade meningar?
- Får en osannolik hypotes en alldeles för hög sannolikhet relativt de andra hypoteserna? Även om en hypotes kan anses vara mindre intressant måste det finnas sakliga evidens som talar mot den innan den kan uteslutas. Kan man hitta och lägga till sådana evidens till analysen?
- Tänk på att analysen inte fångar alla olika grader av relevans som olika evidens kan ha. I verkligheten kan man t.ex. tänka sig att man får in en rapport som med all säkerhet utesluter alla hypoteser utom en. Detta specialfall kan inte hanteras av metoden.

- Har vissa evidens minskat i betydelse p.g.a. att de är gamla? I så fall kanske inte andra evidens får det genomslag i analysen som man skulle förvänta sig.

I likhet med många andra analytiska metoder ger ACH i regel bäst resultat när den tillämpas av en grupp analytiker som arbetar tillsammans. Personer med olika erfarenheter kan då bidra med olika infallsvinklar till ett problem och komplettera varandra när evidens ska viktas. Det är en klar fördel om någon med tidigare erfarenhet av ACH deltar i analysen eftersom man då kan lägga mindre tid på att hantera metodiken och mer tid på att analysera själva problemet [45].

2.6.3.1 Exempel

För att illustrera hur metoden kan användas modifierar vi ett exempel hämtat från FOI-rapporten *Datorstöd för hypoteshantering inom underrättelseanalys* [47]. I exemplet som används har en liten flicka försvunnit från en campingplats och man använder ACH för att analysera möjliga förklaringar till försvinnandet.

Hypoteser

I utredningen identifieras snabbt tre huvudhypoteser som kan förklara försvinnandet.

1. Flickan har frivilligt och på egen hand gett sig av från campingplatsen och gått vilse, alternativt hållit sig undan.
2. Flickan har varit med om en olycka på eller i närheten av campingen och är skadad eller i värsta fall avliden, t.ex. kan hon ha ramlat i vattnet, hon kan ha trampat genom golvet i ett övergivet hus eller så kan hon ha fått någonting tungt fallande över sig.
3. Flickan har utsatts för ett brott och har blivit bortförd mot sin vilja.

Evidens

Några av de uppgifter som framkommer under utredningen och som bedöms kunna ha ett samband med försvinnandet är dessa.

1. Två obesvarade mobilsamtal har ringts från flickans telefon till mammans telefon efter att hon sist sågs på campingen.
2. Ett hårspänne som tillhör flickan har hittats i ett skogsparti bredvid campingen.
3. En äldre dam uppger att hon har sett en ensam flicka på tågstationen några timmar efter försvinnandet.
4. Flickans familj har tidigare förekommit i utredningar hos socialtjänsten.

	Brott	Olycka	Frivilligt försvinnande
Mobilsamtal	-	/	+
Upphittat hårspänne	/	/	?
Vittnesuppgifter	-	- -	+ +
Uppgifter från socialtjänsten	+	/	+

Tabell 6. Tabell som visar hur evidensen värderas i förhållande till de tre hypoteserna i fallet med den försvunna flickan.

Värdering av evidens

Utifrån de identifierade hypoteserna och evidensen skapar man en tabell (se Tabell 6). Vid en genomgången av funna evidens bedöms både hur starkt evidensen stöder eller talar emot respektive hypotes och hur stor tilltro man har till evidensen. De sammantagna värderingarna förs in i tabellen. I det aktuella fallet görs följande bedömningar.

- Om flickan hade utsatts för brott hade hon sannolikt inte fått möjlighet att använda sin telefon. Eftersom flickan inte bara vid ett utan vid två tillfällen har försökt ringa till sin mamma bedöms det vara mindre troligt att hon utsatts för brott.
- Det upphittade hårspännet kan visa sig vara viktigt i en senare del av utredningen då man jobbar med mer detaljerade hypoteser, men det talar varken för eller emot någon av de aktuella hypoteserna.
- Skulle det visa sig att flickan befunnit sig ensam på tågstationen strax efter försvinnandet är det troligaste att hon tagit sig dit själv och att hon inte har utsatts för brott. Vittnet som eventuellt sett flickan har i det här fallet bedömts vara pålitligt och man har därför stor tilltro till hennes uppgifter. Vittnet har dessutom kunnat lämna ett detaljerat signalement som stämmer väl in på den försvunna flickan. Sammantaget gör detta att vittnesuppgifterna ges stor tyngd i Tabell 6.
- Flickan bor tillsammans med sin mamma och dennas sambo. Enligt socialtjänstens uppgifter pågår det en vårdnadstvist mellan flickans mamma och hennes biologiska pappa. Under omständigheterna måste man beakta möjligheten att flickans försvinnande har med vårdnadstvisten att göra. Flickans oroliga hemförhållanden kan också i sig vara en orsak till att hon bestämt sig för att ”rymma hemifrån”.

2.6.4 Tillämpningar och erfarenheter

2.6.4.1 Allmänt

ACH är en etablerad metod inom underrättelseanalys. Metoden utvecklades under 80-talet av Richards J. Heuer som då arbetade för CIA. För mer läsning om ACH och dess användning i underrättelseanalys hänvisas läsaren till [48].

2.6.4.2 På FOI

På FOI har ACH inte använts i större utsträckning för analys, däremot genomfördes under 2010-2011 en jämförande utvärdering av de två analytiska strategierna Kritiskt tänkande och ACH. Ett antal försöksgrupper fick i uppdrag att resonera kring samma problem med hjälp av en av de två utvärderade metoderna. I studien ingick också referensgrupper som jobbade med samma problem men utan att använda en given metod. Då gruppernas resultat och upplevelser av arbetsprocessen jämfördes visade det sig något oväntat att grupperna som använde ACH generellt klarade uppgiften sämre än de andra. En bidragande faktor ansågs vara att grupperna som använde ACH var ovana vid metoden och hade svårt att använda den effektivt, men man konstaterade också att problemet som behandlats möjligen inte var lämpligt att analysera med hjälp av ACH eftersom det var tämligen komplext. Särskilt problematiskt var det faktum att evidensen inte var oberoende av varandra. Försöken och de resultat man kom fram till i utvärderingen beskrivs i rapporten *Analytic Strategies for Collaborative Intelligence Analysis* [45].

Ett exempel på hur ACH skulle kunna användas i underrättelseanalys presenteras i artikeln *Analysis of competing hypothesis for investigating lone wolf terrorists* [49]. I artikeln beskrivs ett koncept för hur ACH skulle kunna användas för att identifiera ensamagerande hotaktörer, s.k. ”Lone wolves”, på Internet.

2.6.5 Tekniksтöd

ACH kräver inget tekniskt stöd, men det finns flera fördelar med att använda datorprogram som designats för att stödja ACH-analys.

- Hanteringen av flera alternativa hypoteser underlättas väsentligt genom att man får hjälp att hålla ordning på evidens och annan information. Det blir också lättare att jämföra olika hypoteser med varandra.
- Man kan visualisera resultaten och enkelt visa t.ex. var olika analytikers bedömningar skiljer sig åt eller är lika.
- Man får hjälp med att bevara spårbarhet då modellen ändras.
- Det underlättar analysen att lätt kunna sortera tabellen efter olika kriterier.

Richards J. Heuer som utvecklade metoden har själv varit med och utvecklat programvara för ACH-analys på Palo Alto Research Center. Programmet har vidareutvecklats för att kunna stödja kollaborativt arbete med hypoteser och 2011 jobbade bl.a. Heuer med Pherson Associates för att göra mjukvaran möjlig att samköra med mjukvara för andra analytiska tekniker [50].

I FOI-rapporten *Datorstöd för hypoteshantering inom underrättelseanalys* [47] beskrivs hur bl.a. stöd för ACH skulle kunna integreras i som en del i ett mer generellt verktyg för ”intelligent” hypoteshantering.

2.7 Orsak-verkandiagram

Modellegenskaper: Modelldriven, kvalitativ (kan göras kvantitativ)

2.7.1 Användningsområden

Orsak-verkandiagram används för att skapa förståelse för beroenden mellan olika faktorer i ett system, t.ex. mellan aktörer i ett konfliktområde eller mellan stegen i processen att rekrytera och träna självmordsbombare. Modellen tas med fördel fram i grupp med bred kompetensbas och fungerar då som ett sätt att gemensamt avgöra vilka faktorer som är av vikt för de faktorer som man är särskilt intresserad av och eventuellt vill påverka. Själva modelleringen kan också ge en bra grund för att bedöma var det är nödvändigt att inhämta mer information om systemet.

Problem där Orsak-verkandiagram kan användas

1. I en konfliktsituation kan det vara av vikt att förstå dynamiken mellan och drivkrafterna för olika aktörer. Ett Orsak-verkandiagram kan öka förståelsen för dessa och ligga till grund för framtagning av prognoser för systemet.
2. Ett Orsak-verkandiagram kan också fungera som ett beslutsstöd om man vill påverka systemet i någon bestämd riktning. Om vårt mål är att faktor A ska öka, vilka andra faktorer ska vi försöka öka respektive minska för att nå dit?

2.7.2 Nödvändiga förutsättningar

- **God kännedom om domänen**

  För att ett Orsak-verkandiagram ska kunna användas för beslutsstöd måste de viktigaste faktorerna och relationerna finnas med och beroendena mellan dem vara korrekt modellerade. Om någon

betydelsefull faktor missats kan slutsatser dragna utifrån modellen bli helt missvisande.

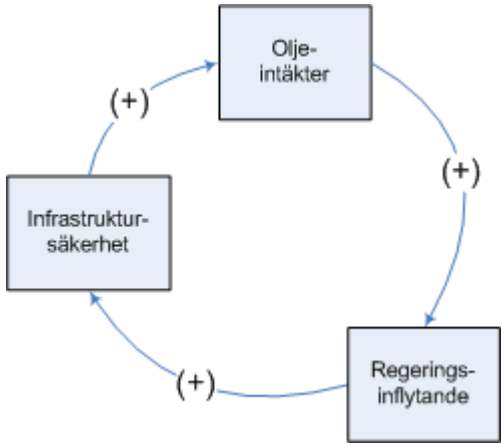
2.7.3 Beskrivning av metoden

Orsak-verkandiagram[18] (eng. Causal Loop Diagram) är en modell som används inom systemanalys för att åskådliggöra hur olika systemkomponenter (variabler) påverkar varandra. Själva metoden för att ta fram modellen är mindre central och kan se ut på flera sätt. En variant beskrivs i exempelavsnittet nedan.

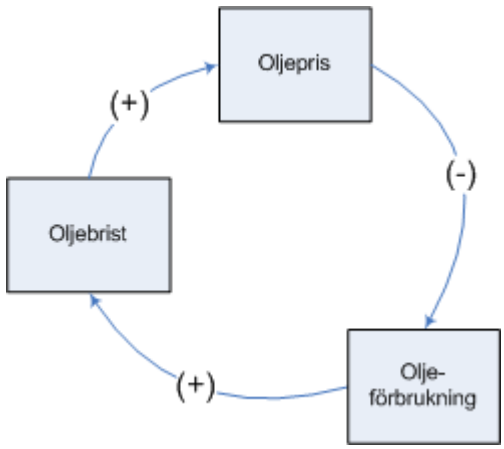
I sitt grundutförande innehåller modellen variabelnoder samt riktade länkar som antingen kan vara positiva eller negativa. En positiv länk från nod A till B innebär att om värdet för nod A ökar så påverkas även värdet för nod B i positiv riktning. Minskar istället värdet för A så påverkas värdet för B i negativ riktning. En negativ länk betyder att B påverkas negativt om värdet för A ökar och vice versa. I Orsak-verkandiagram är det tillåtet att skapa loopar. Dessa loopar får olika karaktär beroende på om loopen har en total positiv påverkan på sig själv eller en total negativ. För att avgöra om en loop är positiv eller negativ kan man följa loopen och ”byta tecken” för varje negativ länk som passeras. En positiv loop kallas förstärkande (se Figur 8) och beskriver ett exponentiellt växande fenomen, medan en negativ loop kallas balanserande (se Figur 9) och beskriver ett stabiliserande fenomen. Det går även att markera tidsfördröjningar för att fånga att en påverkan sker först efter en viss tid.

Fördelar	Nackdelar
1. Lättfattlig grafisk representation vid mindre modeller 2. Tillåter modellering av loop-beroenden, till skillnad från t.ex. Bayesianska nätverk	1. Svåröverskådligt vid större modeller 2. Komplext att hantera om man vill införa kvantitativa aspekter 3. Svårt att göra långsiktiga prognoser, eftersom styrkan och tecknet på länkarna i verkligheten ofta beror på variabelvärdena. När dessa ändras över tiden ändras alltså även modellen.

[18] Orsak-verkandiagram benämns ofta ”influensdiagram” i systemanalyssammanhang. Detta begrepp har dock en helt annan och mer etablerad betydelse inom grafiska probabilistiska modeller som också behandlas i denna rapport varför vi undviker att använda det här.



Figur 8. Exempel på en förstärkande loop. Ökade oljeintäkter ökar regeringens inflytande. Detta medger ökade möjligheter till investeringar i infrastrukturen och dess säkerhet vilket gynnar oljeindustrin.



Figur 9. Exempel på en balanserande loop. Ett höjt oljepris leder till minskad oljeförbrukning som i sin tur gör att tillgången till olja ökar (oljebristen minskar). Detta leder till att behovet av ett ökat oljepris minskar.

2.7.3.1 Exempel

För att illustrera metoden stegar vi igenom skapandet av en exempelmodell. Syftet med modellen är att skapa förståelse för vilka faktorer som är av vikt för maktbalansen i provinsen East Mida i det fiktiva Bogaland[19].

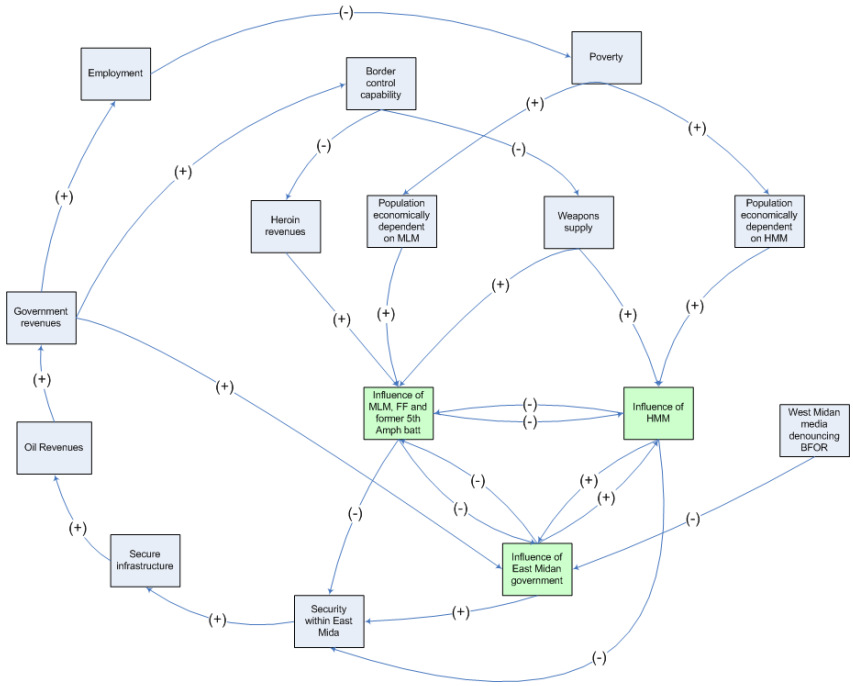
1. Börja med en brainstorm-övning. Lista egenskaper som har med fenomenet/problemet att göra, exempelvis säkerhetsläget, befolkningens och utlandets inställning till respektive aktör, aktörernas finansieringsvägar etc.
2. Samla ihop liknande faktorer till en gemensam formulering på en lämplig abstraktionsnivå. ”Förmåga till gränskontroll” kan vara mer lämpligt än att ha enskilda noder för ”Smuggelkontroll i Norrköping”, ”Förmåga att upptäcka och förhindra människohandel” och ”Gränsbevakning mot Kasurien”. Se till att formuleringen av faktorerna tillåter att de kan öka respektive minska i värde.
3. Koppla samman de noder som uppenbart påverkar varandra och markera om det är en positiv eller negativ påverkan.
4. Gå igenom diagrammet och kontrollera att inga återkopplande loopar har missats och att de har rätt ”tecken”. Komplettera genom att föra in eventuella egenskaper från brainstorm-listan som ännu inte förts in.
5. Kontrollera att de frågeställningar som du är intresserad av går att besvara utifrån modellen. Annars kan en ny iteration med en kompletterad lista krävas.

2.7.4 Tillämpningar och erfarenheter

2.7.4.1 På FOI

Orsak-verkandiagram har inte systematiskt använts på FOI, men vissa erfarenheter finns beskrivna i FOI-rapporterna *Technology to Support Assessment of Operations* [27] och *System Analysis for Knowledge Support* [28]. Den sistnämnda rapporten beskriver bl.a. hur systemanalys användes i experimentverksamhet inom FM under övningen Viking-08.

[19] Bogalandscenariot är ett scenario som använts och utvecklats under många år för större stabsövningar såsom CJSE och Vikingövningarna. Det beskriver ett typiskt operativt scenario med en sönderfallande stat drabbad av inbördesstrider och intervenerande grannstater, krigsherrar, flyktingströmmar etc. Svenska kartan och ortnamn används, men fiktiva personer, organisationer och statsnamn.



Figur 10. Exempel på ett Orsak-verkandiagram. Huvudaktörerna vars maktbalans man vill analysera markeras med grönt.

2.7.5 Teknikstöd

Grundläggande Orsak-verkandiagram går enkelt att skapa i de flesta ritprogram. Vid mer komplicerade diagram kan man vara betjänt av ett layout-stöd för att automatiskt skapa överskådlighet. Sådant stöd finner man i lite mer avancerade ritprogram (t.ex. Microsoft Visio eller gratisverktyget yEd[20]). För mer avancerade analyser av Orsak-verkandiagram där man även önskar stöd för kvantitativa analyser finns ett kommersiellt system, Consideo Modeler[21], som erbjuder simuleringsstöd för detta.

[20] www.yworks.com/en/products_yed_about.html
[21] www.consideo.com

2.8 Bow-Tie-diagram

Modellegenskaper: Modelldriven, kvalitativ (kan göras kvantitativ)

2.8.1 Användningsområden

Bow-Tie-diagram är en grafisk modell som används vid riskanalys för att ge en överblick över hur olika åtgärder samspelar för att förhindra och/eller mildra effekterna av en oönskad kritisk händelse. Ett Bow-Tie-diagram utgörs av ett nätverk där den centrala noden representerar den kritiska händelsen. Genom sin enkla uppbyggnad där hot och förebyggande insatser placeras till vänster om den kritiska noden och konsekvenser och konsekvensmildrande åtgärder placeras till höger om den kritiska noden blir diagrammet intuitivt och lätt att tolka. Bow-Tie-diagram kan användas för att analysera såväl terrordåd och hotande miljökatastrofer som dataintrång och affärsrisker.

Problem där Bow-Tie-diagram kan användas

1. Bow-Tie-diagram är särskilt användbara då man försöker skaffa sig en överblick över vilka säkerhetshot man har bemött med adekvata säkerhetsåtgärder och identifiera eventuella luckor i säkerhetssystemet.
2. Bow-Tie-diagram kan användas i många sammanhang som underlag för att kunna visa att en seriös genomgång av säkerhetsrisker och åtgärder har genomförts.

Koppling till Försvarsmaktens gemensamma riskhanteringsmodell

Inom Försvarsmaktens verksamhet finns många slags risker som alla behöver hanteras på ett genomtänkt sätt. Rutiner kring riskhantering har på senare år fått särskild uppmärksamhet, bl.a. p.g.a. den händelse i Afghanistan 2005 där två svenska soldater omkom och den tragiska olyckan 2008 i vilken en värnpliktig omkom efter att hans båt av misstag råkade åka in i ett område där en övning med skarp ammunition pågick. Ett steg i riktning mot ett mer strukturerat riskhanteringsarbete togs 2009 när Försvarsmakten introducerade *Försvarsmaktens gemensamma riskhanteringsmodell* [29]. *Steg 3* i denna modell går ut på att ”identifiera och värdera” befintligt skydd samt ”att bedöma sårbarheter mot aktuella konkreta hot”. I [29] nämns särskilt att det i *Steg 3* i riskhanteringsmodellen finns ett behov av metodutveckling. Bow-Tie-analys är ett verktyg som skulle kunna bidra till att fylla detta behov. En fördel i sammanhanget är att riskanalysen i Bow-Tie-diagram kan kopplas till klassiska risk-matriser liknande dem som används för riskvärdering i FM:s riskhanteringsmodell. Stöd för att koppla diagrammen till risk-matriser finns bl.a. i programvaran BowTie Pro™ (se kapitel 2.8.5 *Teknikstöd*).

2.8.2 Nödvändiga förutsättningar

- **God domänkunskap**

  Bow-Tie-diagram är i största allmänhet väldigt flexibla och kräver egentligen inte mer av själva problemställningen än att det finns en väldefinierad riskhändelse att utgå från. För att kunna genomföra en pålitlig riskanalys krävs emellertid god domänkännedom så att man inte missar orsaker, konsekvenser och samband som bör inkluderas i diagrammet.

2.8.3 Beskrivning av metoden

Ett Bow-Tie-diagram är uppbyggt kring en central händelse som identifierats som oönskad eftersom den medför negativa konsekvenser. Det kan typiskt röra sig om någon form av olycka, men metoden med Bow-Tie-diagram är flexibel och kan appliceras på många olika slags riskhändelser (och med viss modifikation även på riskscenarier som löper under en längre tidsperiod).

Ett Bow-Tie-diagram karaktäriseras av att det innehåller fem olika sorters noder. Förutom en risknod som representerar den oönskade händelsen finns noder som representerar:

- Möjliga orsaker till riskhändelsen
- Konsekvenser om riskhändelsen inträffar
- Åtgärder som kan minska sannolikheten för att riskhändelsen inträffar
- Åtgärder för att mildra konsekvenserna

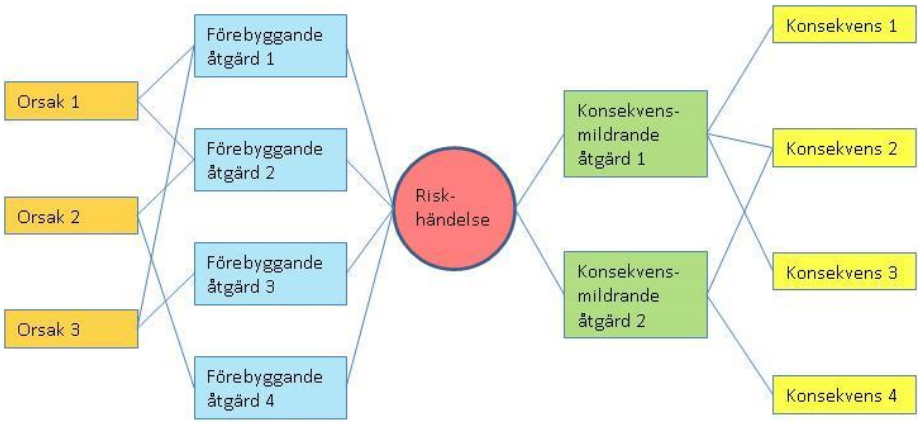
Vidare är ett Bow-Tie-diagram organiserat så att det i princip går att läsa det från vänster till höger i kronologisk ordning. Noderna följer då ordningen:

Orsaker – Förebyggande åtgärder – Riskhändelse – Konsekvensmildrande åtgärder – Konsekvenser

Organisationen av noderna gör att diagrammet får formen av en skjortfluga (Bow-Tie) vilket kan ses i Figur 11.

Proceduren för att skapa ett Bow-Tie-diagram kan beskrivas i följande sex punkter. Punkt 1-5 genomförs med fördel som gruppaktiviteter.

1. Börja med att identifiera riskhändelsen. Beskriv den gärna skriftligt.



Figur 11. Generell struktur i ett Bow-Tie-diagram.

2. Identifiera alla omständigheter och händelser som skulle kunna bidra till att ”trigga” riskhändelsen eller som på annat sätt påverkar sannolikheten för att riskhändelsen ska inträffa. Här kan det vara relevant att inkludera t.ex. observationer som tyder på att riskhändelsen håller på att inträffa.
3. Identifiera de konsekvenser som riskhändelsen kan ge upphov till.
4. Identifiera alla vidtagna åtgärder och befintliga säkerhetssystem som syftar till att förebygga eller minska effekterna av riskhändelsen. Observera att säkerhetssystem kan vara av både teknisk och organisatorisk karaktär.
    a. Tekniska: Hårdvara, mjukvara, verktyg, utrustning, sensorer, larmsystem, m.m.
    b. Organisatoriska: Ledning, organisation, policy, rutiner, utbildning, uppföljning, m.m.
5. För varje säkerhetssystem/åtgärd besvara följande frågor:
    a. Syftar åtgärden till att förebygga riskhändelsen eller till att mildra effekterna?
    b. Om åtgärden är förebyggande, vilken eller vilka orsaker till riskhändelsen kan den motverka? Alternativt om åtgärden är konsekvensmildrande, vilken eller vilka konsekvenser mildrar den?
    c. Är effekten av åtgärden beroende av någon annan åtgärd, t.ex. genom att två åtgärder *tillsammans* kan hindra riskhändelsen från att inträffa?

6. Utgående från resultaten från punkt 1-5, rita upp ett Bow-Tie-diagram med riskhändelse, hot, konsekvenser och åtgärder enligt Figur 11. Alla förebyggande respektive konsekvensmildrande åtgärder ska vara kopplade till risknoden. Kopplingarna mellan orsaker och förebyggande åtgärder samt mellan konsekvensmildrande åtgärder och konsekvenser är de som identifierades i 5b.

I de flesta fall kan man behöva vara lite flexibel i själva modelleringen. T.ex. kan det vara rimligt att slå ihop en grupp av snarlika konsekvenser och låta dem representeras av en ”konsekvenstyp”. En fördel med Bow-Tie-diagram är att de kombinerar analysen av hot och förebyggande åtgärder med konsekvensanalysen. Därigenom bidrar de till ett helhetstänkande för hela riskhanteringsprocessen. Nyttan med Bow-Tie-diagram är framförallt att de gör det lätt att hitta eventuella brister i befintliga säkerhetssystem. I diagrammet är det lätt att identifiera orsaksnoder som saknar koppling till förebyggande motåtgärder. På motsvarande sätt kan man identifiera konsekvenser som man med existerande lösningar inte motverkar.

Bow-Tie-diagram används normalt för icke-kvantitativ analys, men det går att modifiera metoden så att åtminstone semi-kvantitativ analys blir möjlig [9,30]. För att göra det behöver man för det första se till att användaren kan göra bedömningar enligt någon numerisk skala (exempelvis en skala från 1 till 5) av t.ex. graden av skada som en konsekvens åstadkommer och storleken på den motverkande effekten en förebyggande åtgärd har på en viss orsak. För det andra måste man definiera matematiska formler som väger ihop siffrorna i modellen på ett meningsfullt sätt så att det t.ex. går att rangordna olika konsekvenser efter, säg, *Påverkan på omgivningen* eller *Sannolikhet att inträffa*. Stöd för semi-kvantitativ analys finns i vissa analysprogram (se kapitel 2.8.5 *Teknikstöd*).

2.8.3.1 Exempel

Vi illustrerar Bow-Tie-metodiken med ett exempel på riskhantering inom det civila samhället. I exemplet görs en riskanalys för den oönskade händelsen ”Eldsvåda i hemmet”. Vi tänker oss här att analysen görs av en barnfamilj som

Fördelar	Nackdelar
1. Intuitiv grafisk modell gör Bow-Tie-diagram lätta att tolka 2. Uppmuntrar till en ”helhetssyn” på riskhantering, där både förebyggande och konsekvensmildrande åtgärder beaktas på samma gång	1. Bow-Tie-diagram blir visuellt svåra att överblicka om det finns många kopplingar mellan noderna i systemet.

bor i en fristående villa. Familjen vill göra en genomgång av befintligt brandskydd för att kunna hitta eventuella säkerhetsbrister och identifiera enkla åtgärder som skulle kunna minska konsekvenserna vid eventuell brand. Exemplet är förenklat.

Orsaker

I det aktuella fallet identifierar man tre möjliga brandorsaker:

- Levande ljus som välter eller som brinner ner och sätter eld på eventuella ljusdekorationer.
- Grytor som kokar torrt efter att någon glömt att stänga av spisen.
- Fel i elsystemet. Elsystemet är gammalt och man har återkommande problem med att vissa proppar ofta behöver bytas. Problemen kan möjligen tyda på att de vitvaror som är kopplade till de aktuella propparna inte är korrekt installerade.

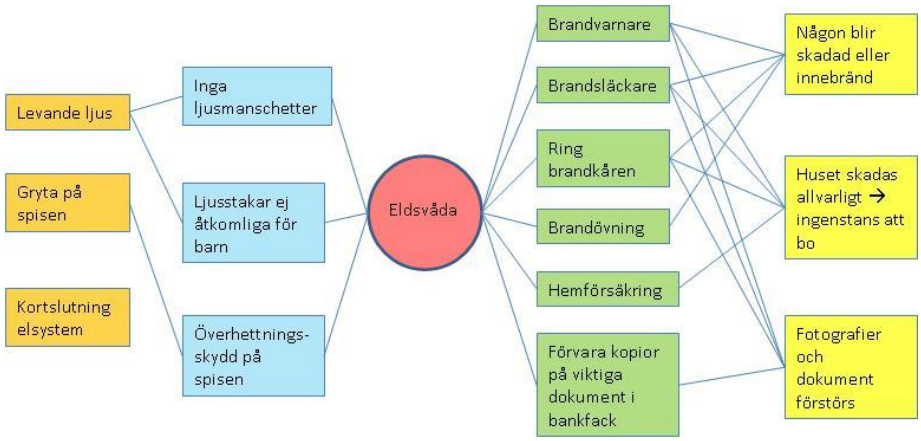
Konsekvenser

En eldsvåda kan få många oönskade konsekvenser, men i det här fallet väljer man att endast betrakta de tre mest allvarliga.

- En eller flera människor kan bli innebrända eller svårt skadade av brand eller rök.
- Familjen kan bli stående utan bostad p.g.a. att huset brunnit ner till grunden eller skadats så allvarligt att det inte går att flytta tillbaka utan omfattande renoveringar.
- Viktiga dokument som t.ex. juridiska avtal och familjefotografier kan förstöras.

Åtgärder och analys

I Figur 12 visas ett Bow-Tie-diagram för händelsen ”Eldsvåda i hemmet”. Förutom orsaker och konsekvenser innehåller diagrammet både förebyggande och konsekvensmildrande åtgärder. Vid analys av diagrammet kan man konstatera att två av de tre möjliga brandorsakerna hanteras med förebyggande åtgärder som minskar brandrisken väsentligt. Familjen har goda rutiner kring hanteringen av levande ljus och den moderna spisen har inbyggt överhettnings-skydd. Desto mer oroande är problemen med elsystemet. I diagrammet syns tydligt att preventiva åtgärder som kan förhindra eldsvåda p.g.a. elfel helt saknas. Här får man alltså förlita sig helt på åtgärder som kan mildra konsekvenserna av en eventuell brand. Eftersom familjen haft problem med proppar som går kommer man fram till att en lämplig förebyggande åtgärd är att låta en elektriker mäta spänningen i systemet och kolla att köksmaskinerna är korrekt inkopplade.



Figur 12. Bow-Tie-diagram för den oönskade händelsen ”Eldsvåda i hemmet”.

Av ekonomiska skäl vill man inte dra om hela elsystemet om det inte finns skäl att tro att felen är allvarliga, men för att ytterligare minska risken för att någon ska skadas i samband med en eventuell brand så bestämmer man sig för att genomföra en brandövning med hela familjen. Sammanfattningsvis kommer man alltså att kunna lägga till två noder i diagrammet; dels en förebyggande åtgärd (elektriker kontrollerar elsystemet) som kopplas till orsaken ”Kortslutning elsystem”, dels en konsekvensmildrande åtgärd (brandövning) som kopplas till konsekvensen ”Någon blir skadad eller innebränd”.

2.8.4 Tillämpningar och erfarenheter

2.8.4.1 Allmänt

Bow-Tie-diagrammet utvecklades under 70-talet, för att sedan bli något av ett standardverktyg för riskbedömning under slutet av 90-talet. Det första större företag som integrerade riskanalys med hjälp av Bow-Tie-diagram i sina processer var oljebolaget Shell, detta som en direkt följd av ökad riskmedvetenhet efter att oljeplattformen Piper Alpha totalförstördes i en brand 1988. 167 personer omkom i katastrofen och enorma finansiella världen förstördes. I efterhand konstaterades att det funnits allvarliga brister i säkerhetsrutinerna på plattformen och att säkerhetssystem saknades eller inte fungerade som de skulle.

Idag regleras oljeindustrin till stor del av lagar och regler och aktörer på marknaden förväntas löpande redovisa sitt förebyggande arbete för riskhantering, bl.a. genom att tillhandahålla schematiska diagram av Bow-Tie-modell. Användningen av Bow-Tie-diagram har med tiden spritt sig från oljeindustrin till

annan tung industri, t.ex. gruvindustrin, men även till myndigheter, finans- och försvarsrelaterade verksamheter.

2.8.4.2 På FOI

På FOI har Bow-Tie-diagram använts på försök i EU-projektet SUPPORT[22] för att analysera kritiska händelser (såväl olyckor som sabotage) inom hamndomänen. Syftet har varit att identifiera brister i dagens hamnsäkerhetssystem vilka i framtiden skulle kunna åtgärdas med nya tekniska hjälpmedel.

2.8.5 Teknikstöd

Det finns flera kommersiella verktyg som kan användas för att skapa Bow-Tie-diagram:

- BowTie Pro™ [23] lanserades 2004 och är ett program som är särskilt anpassat för att skapa och hantera Bow-Tie-diagram. En av fördelarna med mjukvaran är att den gör det lätt att koppla ett Bow-Tie-diagram till olika sorters underlag, t.ex. dokument som innehåller företagets policy, rutiner eller åtgärdslistor. Programvaran gör det också möjligt för användaren att lägga in vissa bedömningar i modellen så att det därigenom blir möjligt att göra en semi-kvantitativ analys.
- Företaget UReason tillhandahåller mjukvarulösningar för industrin (kemi, gas och olja, elkraft och infrastruktur) inom områdena process-simulering, larmhantering och beslutstöd. Deras mjukvara stödjer bl.a. Bow-Tie-analys [24].

[22] www.support-project.eu/
[23] www.bowtiepro.com
[24] www.ureason.com

3 Diskussion

I kapitel 2 *Verktygsbeskrivningar* ges översiktliga beskrivningar av ett antal analysmodeller. Dessa modeller utgör bara en handfull av alla analysmodeller som finns att tillgå. Exempel på andra analytiska verktyg som kan vara intressanta för underrättelseanalys är *Ishikawa diagram*[25] (fiskbensdiagram), *Root cause analys*[26] och *Why–because analys*[27]. Ytterligare exempel finns beskrivna i [50].

Metod	Datadriven/ Modelldriven	Kvalitativ/ Kvantitativ	Hypotesskapande/ Hypotestestande
Morfologisk analys	Modelldriven	Kvalitativ	Hypotesskapande
Grundad teori	Datadriven	Kvalitativ	Hypotesskapande
Attackträd	Modelldriven	Kvalitativ	Hypotesskapande/ Hypotestestande
Wigmoreanska träd	Modelldriven	Delvis kvantitativ	Hypotestestande
Bayesianska nätverk	Modelldriven (finns även som datadriven variant där modellen lärs in från data)	Kvantitativ	Hypotestestande
Analys av konkurrerande hypoteser	Modelldriven (till viss del datadriven)	Kvalitativ	Hypotestestande
Orsak-verkandiagram	Modelldriven	Kvalitativ	-
Bow-Tie-diagram	Modelldriven	Kvalitativ	-

Tabell 7. Klassificering av de analysmetoder som beskrivs i denna rapport.

[25] http://en.wikipedia.org/wiki/Ishikawa_diagram
[26] http://en.wikipedia.org/wiki/Root_cause_analysis
[27] http://en.wikipedia.org/wiki/Why-Because_analysis

Några övergripande egenskaper hos de verktyg som beskrivits i rapporten finns sammanfattade i Tabell 7. Som en parantes kan tilläggas att majoriteten av de verktyg som klassificerats som kvalitativa i någon mening kan göras kvantitativa genom att man knyter siffror till värderingar (t.ex. ”bra”=3, ”mycket bra”=5). Man får dock vara försiktig då man tolkar resultaten från sådana kvantifierade modeller.

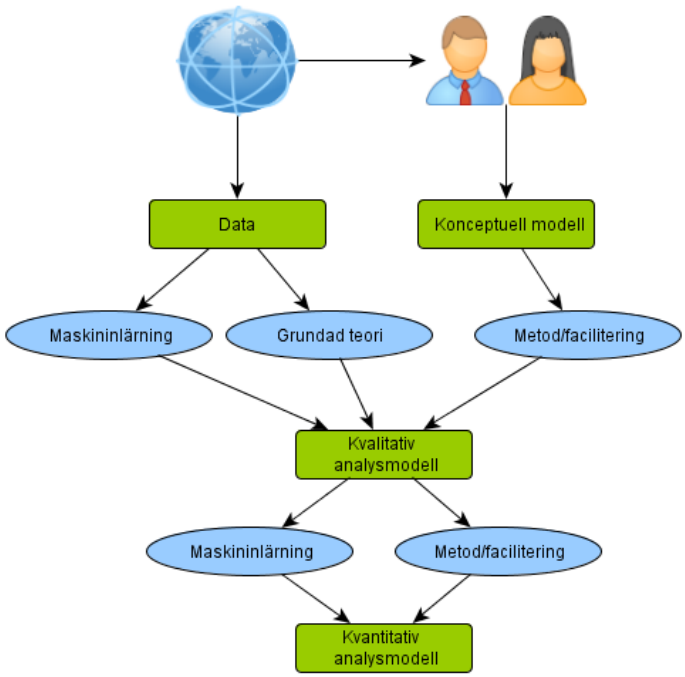
Egenskaperna i tabellen fyller olika behov i den analytiska processen, vilket illustreras i Figur 13 och Figur 14. Utgående från detta betraktelsesätt kommer vi i det här kapitlet att flytta fokus från enskilda verktyg till en mer övergripande betraktelse av analysprocessen. I avsnitt 3.1 *Att tänka på när man väljer verktyg* diskuteras generella faktorer som man bör beakta vid val av verktyg. Därefter följer i avsnitt 3.2 en översikt över faciliteringsmetoder som kan stödja övergången från en kvalitativ analysmodell till en kvantitativ. Avslutningsvis ges i avsnitt 3.3 *Koppling till beslutsfattande* en kort diskussion om hur analytiska verktyg kan kopplas till antingen manuellt eller automatiserat beslutsfattande.

3.1 Att tänka på när man väljer verktyg

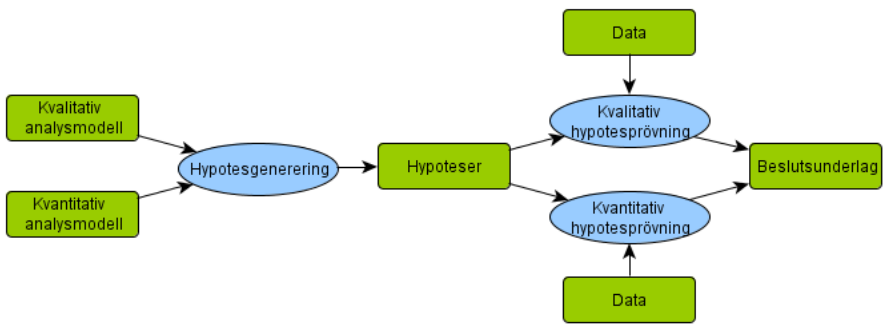
I metodbeskrivningarna i föregående kapitel gavs en del tumregler för när respektive metod passar att använda. Nedan listas ytterligare ett antal övergripande faktorer som kan vara avgörande för modellvalet.

Underrättelsebehovet: Enligt Underrättelsereglementet [1] är det främst typen av underrättelsefråga som påverkar huruvida en datadriven eller modelldriven (baserat på en konceptuell modell) ansats för analysmodellen ska göras. Om frågan kan besvaras utifrån en känd analysmodell som baseras på t.ex. statistik blir valet naturligt datadrivet och fokus förskjuts till inhämtning av rätt underlag. Exempel på en sådan fråga kan vara en bedömning av styrka och status hos en militär förmåga. Om frågan istället rör mer implicita företeelser såsom aktörsrelationer och intentioner blir det svårare att göra rent kvantitativa bedömningar och en modelldriven ansats är naturlig. Underrättelsefrågan utgör också måttstock för hur detaljerad en analysmodell behöver vara. Går det som efterfrågas att svara på utan att vi fördjupar oss i en kvantitativ jämförelse? Är de kausala beroendena viktiga för att vi ska kunna dra rätt slutsatser eller klarar vi oss med att enbart lista kombinationer av variabler som i Morfologisk analys?

Analys, tid kontra komplexitet: Ett komplext problem kräver mycket resurser att modellera. Även om underrättelsefrågan lämpar sig för en detaljerad kvantitativ modell är ofta risken att kvaliteten inte blir tillräckligt hög givet den tid och de resurser som är tilldelade. Är frågeställningen återkommande eller av extra betydelse bör man dock överväga om en extra resursinvestering lönar sig. Tidsförhållanden på taktisk, operativ och strategisk nivå gör att dessa kräver olika överväganden vid modellval. De relativt sett stora resurserna på strategisk



Figur 13. Översikt över hur metoder med olika attribut kan användas inom olika delar av bearbetningsprocessen.



Figur 14. Översikt av sambandet mellan hypotesgenerering, hypotesprövning och beslutsfattande.

nivå kan tillåta en uttömmande Morfologisk analys och omfattande hypotesprövning. Samtidigt är flera frågeställningar på strategisk nivå mer av kvalitativ natur och sällan upprepande.

Beslut, tid kontra komplexitet: Motsvarande tidsförhållanden som för analys gäller generellt sett även för beslut på taktisk, operativ och strategisk nivå. Framförallt kan det på taktisk nivå (och ännu mer på stridsteknisk) betyda att tid för hypotesprövningen som ligger till grund för beslut är kritisk och en viss grad av automation är önskvärd. Detta betyder att en detaljerad och gärna kvantitativ modell ändå är önskvärd, speciellt om analysarbetet kan göras i ett tidigare och icke tidskritiskt "off-line"-läge.

Kombination av verktyg: Flera av modellerna som presenterats i den här rapporten kan anpassas i uttrycksfullhet efter behov, alternativt användas i kombination (se Figur 13 och Figur 14). Som exempel kan nämnas att Orsak-verkandiagram i sin enklaste form enbart innehåller kvalitativ information men kan utökas så att varje variabel kan anta kvantitativa värden och relationerna beskrivas av matematiska funktioner. Detta kan utnyttjas i simuleringar för systemprediktion. Ett exempel på hur modeller kan kombineras ges i [51], där en modell för miljökonsekvenser vid brandbekämpning kartläggs. Här görs först en kvalitativ Morfologisk analys för att generera samtliga tänkbara scenarion. Dessa scenarier förfinas sedan genom att kausala samband mellan variablerna, samt sannolikheter för hur de påverkar varandra, definieras. Detta steg gör det möjligt att analysera scenarierna med hjälp av Bayesianska nätverk. Samtliga modellparametrar skattas genom facilitering av domänexpertis (se avsnitt 3.2).

3.2 Från kvalitativt till kvantitativt – Att utvinna sannolikheter ur domänkunskap

Hos analysverktyg som förlitar sig på kvantitativa parametrar är en förutsättning för användbarhet att parametrarna sätts till värden som någorlunda väl motsvarar den verklighet som verktyget avser modellera. Somliga parametrar är uppenbara av den givna situation i vilken verktyget tillämpas – det kan exempelvis röra sig om skalningsparametrar som antal objekt av något slag. Betydligt svårare är det dock när parametrarna representerar sannolikheter för att olika tillstånd föreligger eller händelser inträffar, något som inte minst är fallet med Bayesianska nätverk och besläktade probabilistiska modeller. Sannolikheten att en händelse skall inträffa är ett abstrakt begrepp som inte direkt kan observeras i verkligheten annat än i erfarenheten av hur ofta händelsen har inträffat tidigare under givna förutsättningar.

För välstuderade typsituationer där stora mängder empiriska data finns att tillgå kan vanliga statistiska metoder användas för att på ett tillförlitligt sätt skatta de efterfrågade sannolikheterna. Men det är vanligt att de sannolikheter man är

intresserad av inte kan härledas från datamängder eller litteratur, och att den enda källan till kunskap är domänexpertens erfarenhet av fenomenet i fråga [52,53]. Naturligtvis är expertens erfarenhet inte lagrad på numerisk form, utan som en kvalitativ situationskännedom. Det ligger därför nära till hands att helt enkelt låta experten värdera de efterfrågade sannolikheterna. Denna sannolikhetsutvinningsprocess[28] är dock långt mindre trivial och oproblematisk än den vid första anblick kan förefalla.

Till att börja med kan domänexperter sällan förväntas vara tillräckligt väl förtrogna med sannolikhetsbegreppet för att effektivt kunna använda det för att beskriva vag kunskap. Somliga kan t.o.m. känna ett obehag och uttrycka motstånd inför en numerisk värdering av osäkerheten i deras kunskap [53]. Därtill är metoder baserade på direkt sannolikhetsskattning behäftade med en rad problem relaterade till *kognitiva biaser* hos experten (se nedan), varför en rad *indirekta* skattningsmetoder har utvecklats, vilka allmänt går ut på att ställa experten inför hypotetiska beslutssituationer där expertens agerande kan användas för att härleda sannolikheten i fråga.

Oavsett vilken typ av metod som används är det viktigt med en god facilitator som förklarar upplägget för experterna, utbildar dem i grundläggande sannolikhetsbegrepp och hjälper dem igenom metoden.

En vanlig direkt skattningsmetod är att låta experten ange varje sannolikhet genom att sätta en markering på en linje numrerad från 0 till 100 procent. Ofta kompletteras dessa skalor värdeord som ”säkert”, ”sannolikt”, ”förväntat”, ”50-50”, ”osäkert”, ”osannolikt”, ”omöjligt” för att kvalitativt kalibrera expertens bedömning. Fördelen med denna metod är att den medger snabb skattning av många parametrar.

Vid komplexa bedömningar såsom av sannolikheter använder sig människan undermedvetet av tumregler, så kallade *heuristiker*. Dessa underlättar skattningsuppgiften och kan i många vardagliga sammanhang ge goda approximationer, men i många andra fall ger de upphov till felskattningar genom *kognitiva biaser*. Exempel på heuristiker är *tillgänglighets-heuristiken* och *ankring och justering* [54]. Tillgänglighets-heuristiken skattar sannolikheten för en händelse utifrån hur lätt händelsen kan dras till minnes. Exempel på felskattningar till följd av denna heuristik är överskattning av risken för flygplansolyckor jämfört med bilolyckor p.g.a. de förstnämndas prominens i media. Ankring och justering innebär att man utgår ifrån ett initialvärde – vilket typiskt är godtyckligt, exempelvis den första parametern man skattar – och sedan justerar utifrån det. Ofta är justeringarna otillräckliga vilket gör att sannolikheterna otillbörligen färgas av det kanske helt irrelevanta initialvärdet.

[28] I engelskspråkig litteratur används begreppet *probability elicitation*, eller mer allmänt *knowledge elicitation*.

Utöver kognitiva biaser kan snedvridning förekomma till följd av att experten har egenintresse kopplat till den skattning de gör, så kallad *motivationsbias*. Det kan vara att de vill framstå som säkrare i sin bedömning än vad som är fallet, eller att de övervärderar risken för en händelse om vilken de besitter unik kunskap.

Ett sätt att undvika kognitiva biaser vid sannolikhetsskattning är att helt enkelt kringgå själva skattningen med hjälp av indirekta skattningsmetoder. Bland dessa återfinns *spelmetoder*, varav en variant ställer experten inför ett val mellan två lotterier. Om vi vill skatta sannolikheten att X inträffar låter vi lotteri A (eller snarare en tänkt bookmaker) ge en vinst på, säg, 10000 kr om X inträffar och 0 kr annars, medan det rena lotteriet B ger samma vinstsumma med en sannolikhet p som sätts av facilitatorn (vald oberoende av någon antagen sannolikhet för X). Facilitatorn justerar p till dess att brytpunkten hittas där experten skiftar mellan val av A eller B. Givet att experten handlar rationellt och i vinstintresse[29] kan p i brytpunkten anses motsvara expertens sannolikhetsbedömning av X. Fördelen med indirekta metoder som denna är att de genom att inte avkräva experten ett direkt numeriskt värde undviker många av de kognitiva biaser som kommer med direkt skattning. Den största nackdelen med spelmetoder är att de är väldigt tidskrävande.

Ytterligare en skattningsmetod ersätter skattningar av enskilda sannolikheter med parvisa relativa skattningar på formen ”hur mycket mer sannolikt är det att A inträffar än att B inträffar?”. De parvisa bedömningarna ger upphov till ett överbestämt problem, vilket bland annat kan ge en indikation om hur internt konsistenta expertens bedömningar är[30]. Med matematiska metoder kan rimliga approximationer av de eftersökta sannolikheterna sedan räknas fram. Denna metod baserar sig på nyttovärderingsmetoden AHP[31] [53]. Metoden har den fördelen att människor tenderar att vara bättre på relativa skattningar än absoluta. Nackdelen är att de parvisa jämförelserna ger upphov till ett mycket stort antal värderingar – att exempelvis skatta 100 sannolikheter kräver ca 5000 värderingar.

Bayesianska nätverk kräver i regel skattning av ett stort antal sannolikheter, varför snabba direkta skattningar ibland kan vara att föredra, även om de lider av kognitiva biaser. Det finns även sätt att reducera arbetsbördan med skattning. En sådan metod bygger på att genom känslighetsanalys utröna vilka parametrar i modellen som ger störst utslag och att fokusera skattning på dem [52].

[29] Det är ett matematiskt faktum att en rationell och vinstmaximerande spelstrategi är ekvivalent med en konsistent sannolikhetsvärdering [55]

[30] Ett enkelt exempel för att illustrera principen: Om händelse A bedöms sannolikare än händelse B, B bedöms sannolikare än C och C bedöms sannolikare än A har vi en uppenbar motsägelse. Även mer subtila fall, där numeriska bedömningar ej till fullo överensstämmer, hanteras av metoden.

[31] Analytical Hierarchical Process

En god facilitator kan reducera effekten av bias genom att öva experterna på förhand och göra dem medvetna om vanliga fallgropar. Målet med en god facilitering är att så troget som möjligt fånga *expertens uppfattning* oavsett hur väl denna uppfattning stämmer överens med verkligheten [56]. För det krävs kunskap i såväl psykologi som statistik, och givetvis gott faciliteringshantverk.

3.3 Koppling till beslutsfattande

Majoriteten av de metoder som beskrivs i denna rapport syftar till att generera, alternativt pröva, olika hypoteser. På detta sätt ger de stöd i en analysprocess som i slutänden syftar till att möjliggöra bra och välunderbyggda beslut. Beslutsfattande är inte i fokus för denna rapport, men det kan vara värt att notera att det finns existerande metoder för att utifrån en kvantitativ analys rekommendera olika beslut. Dessa bygger vanligtvis på normativ beslutsteori, i vilken man utgår ifrån att syftet är att fatta rationella beslut som i någon mening är optimala. Inom normativ beslutsteori har principen om maximerad förväntad nytta (eller minimerad förväntad kostnad, beroende på typen av beslut) en central roll. Enligt denna teori kan man ställa upp ett beslutsproblem i termer av tillstånd, handlingar och utfall. Det sanna tillståndet av världen man försöker modellera kan då sägas vara det man försöker uppskatta vid analysarbetet. Handlingarna är de olika handlingsalternativ (beslut) man som beslutsfattare kan välja emellan, medan de olika möjliga utfallen är kombinationer av handlingar och tillstånd.

Som ett klassiskt exempel för att visa principen tänker vi oss en beslutssituation där en person på morgonen har att välja mellan två handlingsalternativ: att ta med ett paraply till jobbet respektive att inte ta med ett paraply. I detta förenklade exempel finns det bara två olika tillstånd av intresse: att det kommer att regna under dagen respektive att det inte kommer att regna under dagen. Till varje möjligt utfall (kombination av handling och tillstånd) tilldelas en nytta (eller kostnad). Att ta med paraplyet om det inte regnar kan anses vara förknippat med en viss negativ nytta i form av att släpa runt på ett paraply i onödan, medan det kan anses vara förknippat med en stor nytta utifall att det visar sig att det börjar regna. En positiv nytta kan identifieras för fallet då ett beslut tas om att inte ta med sig paraplyet om det inte börjar regna under dagen, däremot skulle de flesta troligen associera en negativ nytta till utfallet att man lämnar paraplyet hemma om det regnar. Enligt principen om maximerad förväntad nytta ska en rationell beslutsfattare då alltid ta det beslut som maximerar den förväntade nyttan. I paraplyexemplet är detta starkt knutet till den prognos (analys) som gjorts av om det kommer regna under dagen. Om sannolikheten för detta tillstånd bedöms vara mycket låg så blir det rationella beslutet att lämna paraplyet hemma, medan det vid en mycket hög sannolikhet är mer rationellt att ta med paraplyet (de olika gränserna beror på de exakta sannolikheter och nyttor som tilldelas). På samma sätt som prognosen för regn blir relevant i detta exempel så

blir den analys som görs med metoder beskrivna i denna rapport relevanta för de beslut som sedan fattas.

För Bayesianska nätverk finns en direkt utvidgning av modellen som går under namnet *influensdiagram* och som har nära koppling till beslutsfattande. Med hjälp av influensdiagram kan en analytiker utöver att modellera och analysera möjliga tillstånd också modellera möjliga handlingar och nyttan av olika utfall. Detta gör att man som direkt resultat av analysen kan få en rekommendation av ett beslut, något som i sin tur gör att det blir möjligt att automatisera beslutsfattandet. Med detta sagt bör man emellertid ta i beaktande att det inte alltid går att ställa upp ett utfallsrum med tillhörande nyttor. Man bör också hålla i minnet att beslut i praktiken ofta fattas utifrån intuition och erfarenhet snarare än utifrån resultat av beräkningar som har till syfte att maximera ”förväntad nytta”.

4 Referenser

1. Försvarsmaktens underrättelsereglemente, FM UndR, 2010.
2. P.E. Lehner et al., *Confirmation Bias in Complex Analyses*, IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans, Vol. 38, No. 3, May 2008.
3. T. Ritchey, *Fritz Zwicky, Morphologie and Policy Analysis*, presented at the 16th EURO Conference on Operational Analysis, Brussels, 1998.
4. F. Zwicky, *Discovery, Invention, Research - Through the Morphological Approach*, Toronto: The Macmillan Company, 1969.
5. T. Ritchey, *Omvärlden år 2021 – fyra globala scenarier*, Naturvårdsverket rapport 4726, 1997
6. J. Voros, *Morphological prospection: profiling the shapes of things to come*, Foresight, 11(6):4-20, 2009
7. M. Stenström, *Morfologisk analys i grupp – en personlig handledning*, FOI-R--3125--SE, 2011
8. H. Eriksson, T. Ritchey och M. Stenström, *Värdering av räddningstjänstens beredskap för kemolyckor, Handledning för användare av VIK – Värderingsinstrument kem, Andra reviderade och utökade upplagan*, FOI-R--0861--SE, 2003.
9. M. Stenström, *Morfologisk analys av SKI:s beredskap*, SKI Rapport 2004:47
10. I. Johansen, *Scenarioklasser i Forsvarsstudie 2007: En morfologisk analyse av sikkerhetspolitiske utfordringer*, FFI-rapport 2006/02664
11. Öborn et al, *Five scenarios for 2050 – conditions for Agriculture and Land Use*, SLU 2011
12. H. Carlsen och K. H. Dreborg, *Dynamisk generering av socio-ekonomiska scenarier för klimatanpassning: metod, byggstenar och exempel*, FOI-R--2512--SE, 2008
13. P. Hörling, J. Schubert och J, Walter, *Collaborative Synchronization Management Tool, A User's Guide*, FOI-R--2706--SE, 2009.
14. J. Schubert och P. Hörling, *Collaborative Synchronization Management Tool – Final Report*, FOI-R--3298--SE, November 2011.
15. J. Hartman, *Grundad Teori: Teorigenerering på empirisk grund*, Studentlitteratur, Lund, 2001.

16. B. Glaser, *Basics of grounded theory analysis*, Mill Valley, CA: Sociology Press, 1992.

17. C.-H. Chou, F. M. Zahedi och H. Zhao, *Ontology for Developing Web Sites for Natural Disaster Management: Methodology and Implementation*, IEEE Trans. on systems, man and cybernetics A: systems and humans, Vol. 41, No. 1, pp. 50-62, 2011.

18. P. Agrell, *System theory for systems practice*, FOA D 102229, 1992.

19. D. T. MacLeod, *Leveraging Academia to Improve NGO Driven Intelligence. J. Conflict Studies*, Vol. 29, 2009.

20. A. D. Miller, *Homeland Security Intelligence to What End?*, Naval Postgraduate School Master thesis, 2010.

21. G. J. Wineera, *Intelligence preparation of the battlefield in the contemporary operating environment: a grounded theory of the New Zealand experience*, Massey University master thesis, 2011.

22. T. Koenig, *Routinizing Frame Analysis through the Use of CAQDAS*, Proc. Sixth International Conference on Social Science Methodology, 2004.

23. B. Schneier, *Attack trees*, Dr Dobbs Journal, 24(12), 1999.

24. S. Mauw och M. Oostdijk, *Foundations of attack trees*, in International conference on information security and cryptology (icisc 2005), pages 186-198, Springer-Verlag, Berlin, 2005.

25. P. Abdulla, J. Cederberg och L. Kaati, *Analyzing the Security in the GSM Radio Network Using Attack Jungles*, ISoLA (1) 2010: 60-74.

26. J. Brynielsson, A. Horndahl, L. Kaati och P. Svenson, *Development of Computerized Support Tools for Intelligence Work*, 14th ICCRTS: "C2 and Agility", 2010.

27. C. Mårtenson och P. Svenson, *Technology to Support Assessment of Operations*, FOI R--2871--SE, 2009.

28. P. Wikberg, J. Westin, J. Lindoff, M. Lundin, M. Hammervik och L.-Å. Hansson, *System Analysis for Knowledge Support*, FOI Memo 2600.

29. Försvarsmaktens gemensamma riskhanteringsmodell, 2009.

30. C. Jacinto och C. Silva, *A semi-quantitative assessment of occupational risks using bow-tie representation*, Safety Science, Volume 48, Issue 8, Pages 973-979, October 2010.

31. G. Tecuci et al., *Teaching Intelligence Analysis with TIACRITIS*, American Intelligence Journal, Vol. 28, Nr 2, 2010.

32. G. Tecuci et al., *The Disciple-RKF Learning and Reasoning Agent*, Comp. Int., Vol. 21, Nr 4, pp. 462-479, 2005.

33. G. Tecuci et al., *Cognitive Assistants for Analysts*, Journal of Intelligence Community Research and Development, 2007.

34. T. Anderson et al., *Analysis of evidence*, Cambridge University Press, 2005.

35. A. Horndahl, P. Hörling, L. Kaati, C. Mårtenson och P. Svenson, *Transferprojekt Impactorium 2010 – 2011*, Slutrapport, under tryck.

36. D. Heckerman, J. S. Breese och K. Rommelse, *Decision-theoretic troubleshooting*, Communications of the ACM, Vol. 38, pp. 49-57, 1995.

37. J. Pearl, *Probabilistic Reasoning in Intelligent Systems*, Morgan Kaufmann, San Francisco, CA, 1988.

38. N. Fenton och M. Neil, *Avoiding Probabilistic Reasoning Fallacies in Legal Practice using Bayesian Networks*, accepterad för publicering i Australian Journal of Legal Philosophy, 2011. URL:http://www.eecs.qmul.ac.uk/~norman/papers/fenton_neil_prob_fallacies_June2011web.pdf

39. M. E. Kragt, *A beginner's guide to Bayesian network modelling for integrated catchment management*, Technical Report No. 9, July 2009.

40. P. Sticha, D. Buede och R. L. Rees, *APOLLO: An analytical tool for predicting a subject's decision making*, Proceedings of International Conference on Intelligence Analysis, 2005.

41. R. Suzic, *Generic representation of military organisation and military behaviour: UML and Bayesian networks*, In Proceedings of the NATO RTO Symposium on Military Data and Information Fusion, Prague, Czech Republic, October 2003.

42. J. Blixt, B. Jansson och K. Mossberg, *Bayesianska nätverk och dess tillämpningar inom OA-verksamheten*, FOI-R--1411--SE, 2005.

43. L. Ferrara, C. Mårtenson, P. Svenson, P. Svensson, J. Hidalgo, A. Molano och A. L. Madsen, *Integrating data sources and network analysis tools to support the fight against organized crime*, ISI 2008 Workshops, LNCS 5075, pp. 171–182, 2008.

44. R. Johansson och C. Mårtenson, *Information acquisition strategies for Bayesian network-based decision support*, 13th International Conference on Information Fusion, 2010.

45. P. Svenmarck et al, *Analytic Strategies for Collaborative Intelligence Analysis*¸ FOI-R--3177--SE, 2011.

46. N. Thomason, *Alternative competing hypotheses, field evaluation in the intelligence and counterintelligence context: Workshop summary*, National Academies Press, 2010.

47. T. Gustavi, F. Johansson, C. Mårtensson och P. Svenson, *Datorstöd för hypoteshantering inom underrättelseanalys*, FOI-R--3214--SE, 2011.

48. R. Heuer, *The psychology of intelligence analysis*, Washington D.C.: CIA Center for the Study of Intelligence, 1999.

49. L. Kaati och P. Svenson, *Analysis of competing hypothesis for investigating lone wolf terrorists*, Proceedings of the European Intelligence and Security Informatics Conference (EISIC 2011), pp. 295−299, 2011.

50. R. J. Heuer Jr. och R. H. Pherson, *Structured Analytic Techniques for Intelligence Analysis*, CQ Press, 2011.

51. A. de Waal och T. Ritchey, *Combining morphological analysis and Bayesian networks for strategic decision support*, ORiON, Volume 23 (2), pp. 105–121, 2007.

52. M. J. Druzdel och L. C. van der Gaag, *Building Probabilistic Networks: Where Do the Numbers Come From? – A Guide to the Literature*, IEEE Transactions on knowledge and data engineering, Vol. 12:4, 481-486, 2000.

53. S. Renooij, *Probability elicitation for belief networks: issues to consider*, The Knowledge Engineering Review, Vol. 16:3, 255–269, 2001.

54. D. Kahneman, P. Slovic och A. Tversky, *Judgment under Uncertainty: Heuristics and Biases*, Cambridge University Press, 1982.

55. C. M. Caves, *Probabilities as betting odds and the Dutch book*, 2005. http://info.phys.unm.edu/~caves/reports/dutchbook.pdf

56. P. H. Garthwaite, J. B. Kadane och A. O'Hagan, *Statistical Methods for Eliciting Probability Distributions*, Journal of the American Statistical Association, 100(470): 680-701, 2005.