Försvarsmaktens gemensamma riskhanteringsmodell

THÉRÈSE PALM

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
Försvarsanalys
164 90 Stockholm

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

www.foi.se

FOI-R--2591--SE
ISSN 1650-1942

Metodrapport
Oktober 2008

Försvarsanalys

Thérèse Palm

Försvarsmaktens gemensamma riskhanteringsmodell

En beskrivning av modellen samt jämförelse med

riskhanteringsmodeller hos civila myndigheter

Titel	Försvarsmaktens gemensamma riskhanteringsmodell. En beskrivning av modellen samt jämförelse med riskhanteringsmodeller hos civila myndigheter
Title	Risk Management in the Swedish Armed Forces. A description of the model and a comparison with risk management models in civilian authorities
Rapportnr/Report no	FOI-R--2591--SE
Rapporttyp Report Type	Metodrapport Methodology report
Månad/Month	Oktober / October
Utgivningsår/Year	2008
Antal sidor/Pages	64 p
ISSN	ISSN 1650-1942
Kund/Customer	Försvarsmakten / Swedish Armed Forces
Forskningsområde Programme area	2. Operationsanalys, modellering och simulering 2. Operational Research, Modelling and Simulation
Delområde Subcategory	22 Metod och utredningsstöd 22 Operational Analysis and Support
Projektnr/Project no	E11101
Godkänd av/Approved by	Göran Kindvall

FOI, Totalförsvarets Forskningsinstitut
Avdelningen för Försvarsanalys

164 90 Stockholm

FOI, Swedish Defence Research Agency
Division of Defence Analysis

SE-164 90 Stockholm

Sammanfattning

I november 2005 dödades två svenska soldater i Afghanistan av en vägbomb som exploderade under deras fordon. Försvarsmaktens interna utredning av händelsen visade att skilda hot- och riskbedömningar hade gjorts av olika funktioner och nivåer i organisationen. Överbefälhavaren beslutade att en gemensam metod för riskhantering behövdes. I samband med att en modell för detta togs fram efterfrågade även Försvarsmaktens generaldirektör en jämförelse av Försvarsmaktens nya modell och modeller i andra myndigheter.

Syftet med denna rapport är att informera om och beskriva den modell för riskhantering som Försvarsmakten utvecklat (i samarbete med operationsanalytiker från FOI), samt beskriva några erfarenheter från utvecklandet av modellen. Dessutom är syftet att ge en översiktlig jämförelse av olika modeller som används av svenska myndigheter, samt att föra en allmän diskussion om den stora begreppsfloran inom riskhanteringsområdet och problematiken kring detta. Det finns en mängd begrepp inom området riskhantering, och tyvärr används de inte entydigt. Många problem eller svårigheter i riskhanteringsarbete beror på att olika människor använder samma ord för olika saker eller olika ord för samma sak.

Försvarsmaktens modell är främst inriktad på operativ verksamhet och internationella insatser i synnerhet. I modellen ska först grundvärden för riskhanteringen identifieras, därefter görs en bedömning av hot respektive sårbarheter. Utifrån dessa genomförs sedan en riskbedömning, och slutligen tas beslut om att acceptera eller åtgärda riskerna. I jämförelsen mellan Försvarsmaktens modell och övriga studerade modeller kan man konstatera att alla myndigheter har en modell som är avpassad främst för sin egen verksamhet. Trots detta är de allra flesta modellerna i grunden strukturellt lika. Största skillnaden mellan modellerna är hur detaljstyrda de är. Försvarsmaktens och Länsstyrelsens modeller är väldigt konkreta och detaljstyrda, medan övriga myndigheter mer har riktlinjer för hur riskanalys och riskhantering kan

genomföras. En annan större skillnad mellan modellerna är huruvida en sårbarhetsbedömning genomförs och när i processen det sker. I Försvarsmaktens modell ligger sårbarhetsbedömningen till grund för riskbedömningen, medan den i till exempel Krisberedskapsmyndighetens modell genomförs efter det att själva riskanalysen är slutförd (det vill säga att riskanalysen istället ligger till grund för sårbarhetsanalysen).

Nyckelord:

risk, riskhantering, riskanalys, riskbedömning, riskvärdering, RSA, hot, hotbedömning, sårbarhet, sårbarhetsbedömning, Försvarsmakten, civila myndigheter

Summary

In November 2005, two Swedish soldiers were killed in Afghanistan by an improvised explosive device that exploded under their vehicle. The Swedish Armed Forces' internal investigation of the incident showed that different threat and risk assessments had been made by various functions and levels in the organisation. The Supreme Commander decided that a common risk management approach was needed. In connection with the development of a risk management model the Defence Director General requested a comparison between the new model and the models produced by other authorities.

The purpose of this report is to provide information on the risk management model the Swedish Armed Forces (in cooperation with operational analysts from the Swedish Defence Research Agency) has developed, and also to describe some experiences from the development work. In addition, the aim is to provide a brief comparison of different models used by Swedish authorities, and to hold a general discussion of the great number of concepts in the area of risk management and the problems surrounding it. There are a variety of concepts in the field of risk management, and unfortunately they are used ambiguously. Many problems or difficulties in the risk management approach are due to different people using the same words for different things, or different words for the same thing.

The Swedish Armed Forces' model is primarily focused on operations in theatre. In the model, basic values for risk management are first identified, and then assessments of threats and vulnerabilities are made. Based on these, a risk assessment is produced, and finally a decision to accept the risks or to mitigate the risks is taken. In the comparison between the Swedish Armed Forces' model and the other studied models, it can be seen that all authorities have a model that is suitable mainly for their own activities. Despite this, a majority of the models are structurally similar. The largest difference between the models is how detail-driven they are. The Swedish Armed Forces' model and the County

Administrative Board’s models are very specific and detail-driven, while other authorities merely provide guidance on how risk analysis and risk management can be implemented. Another major difference between the models is whether a vulnerability assessment is carried out and where in the process that is done. In the Swedish Armed Forces’ model the vulnerability assessments form the basis of the risk assessments, while in the Swedish Emergency Management Agency’s model, for example, the vulnerability assessment is carried out after the risk analysis is completed (that is, the risk analysis form the basis of the vulnerability assessment).

Keywords:

risk, risk management, risk analysis, risk evaluation, risk assessment, threat, threat assessment, vulnerability, vulnerability assessment, Swedish Armed Forces, Defence Forces, civilian authorities

Innehållsförteckning

1 Inledning

I november 2005 dog två svenska soldater i Afghanistan, efter att en vägbomb exploderat under deras fordon. Försvarsmaktens interna utredning av händelsen visade att skilda hot- och riskbedömningar hade gjorts av olika funktioner och nivåer i organisationen. Överbefälhavaren beslutade att en gemensam riskhanteringsmetod behövdes. I samband med att en modell för detta togs fram efterfrågade även Försvarsmaktens generaldirektör en jämförelse av Försvarsmaktens nya modell och modeller i andra myndigheter. Modellen utvecklades under 2006 av en arbetsgrupp bestående av representanter från de olika nivåerna inom Försvarsmakten, från taktisk till strategisk nivå.

1.1 Syfte

Denna rapport är den första av två rapporter om Försvarsmaktens riskhanteringsmodell. Syftet med rapporten är att informera om och beskriva Försvarsmaktens nya gemensamma riskhanteringsmodell samt några erfarenheter från utvecklandet av modellen. Dessutom är syftet att ge en översiktlig bild av olika modeller som används av andra svenska myndigheter, samt att föra en allmän diskussion om den stora begreppsfloran inom riskhanteringsområdet och problematiken kring detta.

Den andra rapporten kommer att behandla erfarenheter från användandet av modellen i Försvarsmakten, tillsammans med slutsatser från detta samt förslag på vidareutveckling av modellen.

1.2 Målgrupp

Rapporten är riktad dels till personal inom Försvarsmakten som varit med att utveckla, eller arbetar med, Försvarsmaktens gemensamma riskhanteringsmodell, dels till FOI-personal som arbetar med risk- och sårbarhetsanalyser, riskhantering eller jobbar inom försvarssektorn. Kapitlet om Försvarsmaktens modell är framför allt riktad till dessa. Övriga delar av rapporten är skrivna för att passa en bredare publik, och kan med fördel läsas av alla som jobbar med, eller är intresserade av, riskanalyser och riskhanteringsmodeller.

1.3 Metod och avgränsningar

Rapporten bygger till största delen på personlig medverkan (som operationsanalytiker på Insatsstaben) i utvecklandet av Försvarsmaktens riskhanteringsmodell under hösten 2006, medverkan i framtagandet av utbildning på modellen under våren 2007, samt i arbeten där modellen använts, även det under våren 2007.

Rapporten fokuserar på Försvarsmaktens riskhanteringsmodell, men i rapporten presenteras även ett urval av modeller från andra svenska myndigheter. Avsikten är inte att ge en heltäckande presentation av alla modeller som har utvecklats och används inom myndighetsvärlden, utan att ge några exempel på hur olika modeller kan se ut, vad som skiljer dem åt samt vilka styrkor respektive svagheter de har. De valda modellerna kommer från myndigheter som i viss utsträckning har liknande verksamhet som Försvarsmakten eller jobbar med liknande hotbilder, eller av andra skäl kan vara intressanta för jämförelsen. Dessa modeller har ofta fokus på riskhantering gentemot personals liv och hälsa. Jämförelsen bygger framför allt på informationsmaterial och handböcker från de utvalda myndigheterna.

1.4 Disposition

I kapitel två görs en översiktlig utredning av begrepp och termer inom riskanalys och riskhantering som introduktion till området. Här förs också en diskussion om problematiken kring jämförelser av modeller inom detta område samt svårigheterna med riskbedömning i förhållande till värdet på ett människoliv. Kapitel tre beskriver Försvarsmaktens riskhanteringsmodell och några erfarenheter från arbetet med denna. Kapitel fyra behandlar ett urval av civila myndigheters modeller, vilka jämförs inbördes och med Försvarsmaktens modell i kapitel fem.

I Bilaga 1 återfinns en översiktsbild på Försvarsmaktens riskhanteringsmodell och de olika bedömningsskalor som används i denna, samt ett fiktivt exempel på riskhanteringsverktyget. Bilaga 2 visar en jämförande figur över de olika beskrivna modellerna och i Bilaga 3 återfinns en lista över använda akronymer samt ordlista på använda begrepp.

2 Risk och riskhantering

”Vi är ständigt omgivna av olika typer av risker i vårt dagliga liv. […] Varje aktivitet involverar risker, men en del risker och risknivåer kan vi inte tänka oss att acceptera. Vi vill alla leva ett liv fritt från risker, men detta är omöjligt.” [1]

I det här kapitlet diskuteras vad som avses med begreppen risk och riskhantering, samt andra begrepp kopplade till riskhanteringsprocessen. Syftet med kapitlet är att introducera den oinvigde i de begrepp och definitioner som används i riskhantering i allmänhet, och denna rapport i synnerhet. Syftet är också att föra en allmän diskussion om den stora begreppsfloran inom området, problematiken vid jämförelser av olika riskhanteringsmodeller samt en kort diskussion om vad som är en godtagbar risk kopplat till värdet av människoliv.

2.1 Begrepp och definitioner

Det finns en mängd begrepp inom riskhanteringsområdet, och tyvärr används de inte entydigt. Många problem eller svårigheter i riskhanteringsarbete beror på att olika människor använder samma ord för olika saker eller olika ord för samma sak.[2]

2.1.1 Hot och risker

Risk är ett mångtydigt begrepp, där inte ens ursprunget är säkert. Grimvall menar att ordet förmodligen kommer från den klassiska grekiskan där ordet kopplades samman med olyckor till sjöss.[3] Aven, däremot, hävdar att ordet härstammar ur den tidiga italienskans *risicare* som betyder ”att våga”.[4] Det finns således också flera olika definitioner på vad risk är.[5] Risk kan innebära en oönskad händelse som kan inträffa, men inte behöver inträffa. Risk kan också betyda orsaken till eller sannolikheten för den oönskade händelsen. Slutligen kan man med risk mena det statistiska väntevärdet för en oväntad händelse eller faktumet att ett beslut fattas mot bakgrund av kända sannolikheter. Det senare brukar ofta sägas vara ett ”beslut under risk”.

[1] Näsman (2005)
[2] Wennersten (2004)
[3] Grimvall (2003)
[4] Aven (2003)
[5] Hansson (2000), Hansson (2002)

Försvarsmakten har i sin modell valt att använda definitionen från internationella standardiseringsorganets ISO/IEC Guide 73, det vill säga att risk är:

> *” kombinationen av sannolikheten för en viss händelse och dess konsekvenser”.*

I dagligt tal, och ibland även inom riskhantering, används emellanåt begreppen hot och risk nästan synonymt, men i något olika sammanhang. Det låter till exempel mer naturligt att tala om risken att klämmas fast i en maskin än hotet att göra detsamma, precis som det i många fall i till exempel militära internationella insatser faller sig naturligare att tala om olika typer av (terror)hot mot verksamheten i stället för risker.

I verksamheter där händelser inträffar som beror på medvetna mänskliga fientliga handlingar förefaller det således naturligare att tala om hot än om risker, både i dagligt tal och i riskhanteringssammanhang. Dessa hot brukar ibland även benämnas *aktörsdrivna*, eller *antagonistiska*, hot för att ytterligare poängtera dessas natur. För andra händelser (till exempel olyckor, naturkatastrofer och arbetsskador) är det mer naturligt att använda ordet risk.
Krisberedskapsmyndigheten (KBM) beskriver skillnaden mellan hot och risk som att

> *”[hot är] en aktörs kapacitet och avsikt att genomföra skadliga handlingar [eller så] kan ett hot bestå av en händelse eller en företeelse som i sig framkallar fara mot något eller någon utan att det i sammanhanget förekommer aktörer med kapacitet och avsikt att orsaka skada. […] I förhållande till hot ska risk ses som en mer konkret effekt av olika företeelser.”* [6]

2.1.2 Riskanalys och riskhantering

Enligt *Federation of European Risk Management Associations* (FERMA) är riskhantering den process som organisationer använder sig av för att uppnå en systematisk hantering av sina risker, och ska:

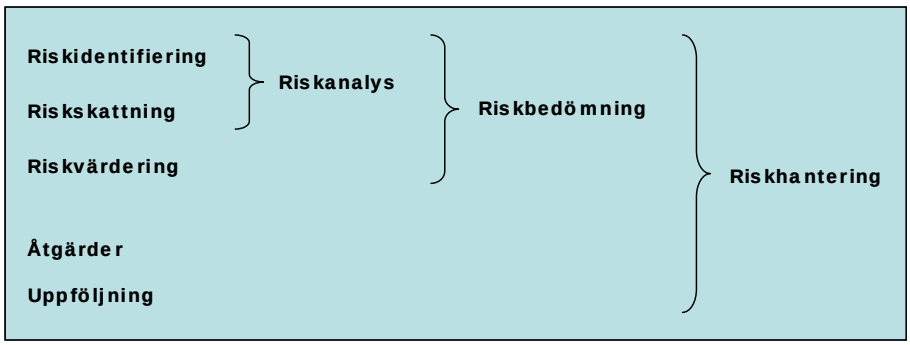
- vara en kontinuerlig och framåtriktad process, och
- metodiskt beakta alla risker i förfluten tid, nutid och framtid.[7]

[6] KBM (2006b)
[7] FERMA (2003)

European Network and Information Security Agency (ENISA) definierar riskhantering något mer detaljerat:

> *”Risk Management is the process of weighting policy alternatives by selecting appropriate prevention and control options.”* [8]

Formerna och verktygen för riskhantering skiljer sig åt mellan olika organisationer och verksamheter. Det är därför svårt att ge en heltäckande och detaljerad beskrivning av riskhanteringsprocessen. I grova drag består dock riskhanteringsprocessen av fyra olika steg: riskidentifiering, riskskattning, riskvärdering samt åtgärder och uppföljning (se även Figur 1).



Figur 1. Beståndsdelarna i en riskhantering.[9]

I det första steget, riskidentifieringen, ska uppgiften avgränsas och hoten mot, eller riskerna i, verksamheten identifieras, tydliggöras och kategoriseras. Detta kan exempelvis göras genom att ställa frågor som ”vad kan hända?” och ”vad kan gå fel som kan leda till ett utfall med farlig exponering?”. Riskidentifieringen är icke-numerisk och därför kan med fördel olika brainstorming-metoder användas för att generera listan med hot/risker. De identifierade riskerna bör beskrivas på ett kortfattat, begripligt och strukturerat sätt.[10]

Ett problem med riskidentifieringen är att risker kan förbises på grund av att de ännu inte resulterat i någon olycka. Att misslyckas med att identifiera någon riskkälla kommer att leda till en undervärdering av den totala risken. Identifieringen är således viktig för riskanalysens validitet och kvalitet.[11]

[8] Marinos (2005)
[9] Wennersten (2004)
[10] I FERMA (2003) finns ett exempel på hur en sådan riskbeskrivning kan presenteras.
[11] KBM (2006a)

I nästa steg görs en uppskattning av risken och ”rimligheten” av olika utfall. I den mån det finns statistiska data att bygga skattningarna på kan dessa användas. I övriga fall måste en subjektiv bedömning göras. Riskidentifieringen och riskskattningen bildar tillsammans riskanalysen som kortfattat kan sägas svara på följande frågor:

- Vad kan hända?
- Hur troligt är det att det händer?
- Vilka är konsekvenserna av händelsen? [12]

I riskanalysen försöker man alltså att identifiera vilken typ av risker som hotar verksamheten och att värdera magnituden på dessa risker. Kombinationen av den skattade sannolikheten och konsekvensen av ett fullföljt hot ger ett riskvärde som sedan värderas gentemot på förhand givna riskkriterier i det tredje steget. Tillsammans med riskanalysen ger detta det som brukar kallas riskbedömning. I vissa fall finns ett ytterligare steg mellan riskskattningen och riskvärderingen – riskperception. Riskperceptionen är kopplad till de psykologiska aspekterna av risk.[13]

Slutligen ska beslut tas om vilka risker som ska accepteras respektive åtgärdas. Syftet med detta steg är att styra eller begränsa risken. Tre grupper av intressenter är involverade i beslutstagandet i riskhanteringsprocessen: beslutsfattarna, kostnads- och nyttobärarna samt riskbärarna.[14] Ibland flyter dessa tre grupper mer eller mindre samman (se Figur 2).

Figur 2. Tre grupper är inblandade i beslutstagandet i riskhanteringsprocessen.

[12] Abrahamsson & Magnusson (2003)
[13] Näsman (2005)
[14] Holmgren (2006); Holmgren & Thedéen (2003); Näsman (2005)

I till exempel militära sammanhang så glider cirklarna isär mer ju högre upp i organisationen man befinner sig.[15] Allra sist i riskhanteringen görs en uppföljning på de åtgärder som har vidtagits för att säkerställa att önskad riskhämmande effekt har uppnåtts.

Området som ska riskhanteras måste vara tydligt definierat och avgränsat. Det är viktigt att alla som är inblandade i en riskhantering har en gemensam förståelse för metoden som används och området som ska riskhanteras.

De ovan använda begreppen är allmänt vedertagna, även om som tidigare nämnts, inte alla individer lägger samma betydelse i dem. I verksamheter där riskhanteringen görs utifrån aktörsdrivna hot kan tyvärr begreppen bli något missvisande. Det är ju till exempel inte riskerna, utan hoten, som identifieras i riskidentifieringssteget. Vidare kan det också poängteras att till exempel att ”bedöma risken” inte nödvändigtvis är samma sak som ”riskbedömning”. Bedömning, skattning, beräkning, med mera, används i många fall som synonymer, både i vardagliga sammanhang och ur rent språkliga perspektiv i till exempel en rapport.

En del i begreppsförvirringen har förmodligen uppkommit när termer har blivit översatta från engelska. Exempelvis kan ”risk assessment” översättas till antingen riskbedömning eller riskvärdering, två begrepp vilka i sin tur kan ställas emot engelskans ”risk estimation”. FERMA har i sin översättning av *A risk management standard*[16] valt att översätta ”assessment” med värdering och ”estimation” med bedömning precis som Näsman, medan exempelvis de svenska författarna Gunnarsson, Thedéen och Wennersten i sina respektive förklaringar av riskbedömning snarare verkar beskriva det som i standarden benämns ”risk assessment”.[17]

2.1.3 Sårbarhet och sårbarhetsanalys

I en riskhanteringsprocess ingår oftast även en sårbarhetsanalys. Sårbarhetsanalysen syftar till att reda ut vilka svagheter som finns i systemet som riskhanteras genom att titta på var och hur systemet kan skadas. Krisberedskapsmyndigheten definierar sårbarhet som ”hur mycket och hur

[15] På lägre nivåer, t.ex. en beslutsfattare i ett insatsområde, är de tre rollerna nästan helt sammanfogade, medan på en hög nivå i organisationen så sitter ofta beslutsfattaren i en stab, kostnadsbäraren i en annan, medan risktagaren befinner sig direkt i insatsområdet.
[16] AIRMIC, ALARM, IRM (2002); FERMA (2003)
[17] Näsman (2005); Gunnarsson (1995); Thedéen (1995); Wennersten (2003)

allvarligt ett system påverkas av en händelse”[18], där graden av sårbarhet bestäms av förmågan att förutse, hantera, motstå och återhämta sig från händelsen. Sårbarhetsanalysen har generellt sett ett mer kvalitativt angreppssätt än riskanalysen (som är mer kvantitativ)[19] och kan beskrivas som ett systematiskt sätt att utvärdera och fastställa sårbarhet. Sårbarhetsanalysen kallas ibland även förmågeanalys. Förmågan kan exempelvis handla om att kunna lindra konsekvenserna av ett verkställt hot såsom sjukvårdens förmåga att omhänderta skadade eller telekommunikationssektorns förmåga att hantera störningar i telenäten.

I vissa sammanhang talar man oftare om begreppet RSA, risk- och sårbarhetsanalyser, istället för riskhantering. RSA syftar till att minska risker och sårbarheter samt förbättra krishanteringsförmågan.[20] Arbetet syftar även till att öka medvetenhet och kunskap hos beslutsfattare och verksamhetsansvariga om vilka hot och risker som finns inom det egna verksamhetsområdet (precis som för hela riskhanteringsprocessen).

2.2 Problematik vid jämförelser

På grund av denna stora mängd av begrepp och definitioner som florerar inom riskhantering är det svårt att jämföra olika riskhanteringsmodeller på ett överblickbart och konstruktivt sätt. Varje modell har sin egen indelning och benämning av de olika stegen i riskhanteringsprocessen. Detta gör det svårt att beskriva modellerna på ett enhetligt och lättöverskådligt sätt. En möjlighet, för att underlätta för läsaren, vore att i beskrivningen av respektive modell försöka ”översätta” modellens uttryck till en på förhand bestämd begreppsflora. Detta skulle underlätta jämförelsen av modellerna, men samtidigt försvåra för den som vill fördjupa sig i någon modell eller jobba med den. Därför kommer de olika modellerna i kapitel tre och fyra beskrivas med deras respektive benämningar, men med tydliga förklaringar.

[18] KBM (2006a)
[19] Mossberg, *et al*. (2007)
[20] KBM (2006b)

2.3 Acceptabla risker och värdet av människoliv

En intressant aspekt när man pratar om hot och risker mot individer är konsekvenserna av ett verkställt hot, eller utlöst risk, och i synnerhet hur människoliv värderas. Vad är en godtagbar risk? Hur många skadade eller döda är acceptabelt i förhållande till en viss risk? Det gäller att avgöra hur stora risker som kan accepteras i olika sammanhang. Ofta är denna risk kopplad till en viss ekonomisk kostnad, och indirekt sätts alltså en pris på varje individs liv. Ska detta pris skilja för till exempel en soldat i Afghanistan jämfört med en soldat på en övning i Sverige?

Möller framhåller att ”[d]et gäller att avgöra hur stora risker för att människor skall förolyckas som kan accepteras i olika sammanhang. Man måste med andra ord ta ställning till vilka insatser i form av investeringar, regleringar och annat som bör göras för att förhindra att mänskligt liv går till spillo.”[21] Detta kan till exempel göras genom att använda sig av kostnads-nyttoanalyser och beräkningar med ”statistiska” liv.

2.3.1 Statistiskt liv

Ett grundläggande begrepp som kan användas vid värdering av säkerhet är värdet av ett statistiskt liv (VSL). VSL värderar befolkningens vilja att betala för en i något avseende ökad säkerhet. Det vill säga, medborgarna uppger sin betalningsvilja för att minska risken så mycket att det statistiskt sett kommer att dö en person mindre.

Som en enkel illustration av VSL kan man tänka sig ett samhälle med 10 000 individer, där det i genomsnitt årligen dör en person. Om varje individ i genomsnitt kan tänka sig att betala 1 000 kr för att eliminera denna risk, så är samhällets totala betalningsvilja för att rädda ett liv tio miljoner kronor.

2.3.2 Kostnads-nyttoanalys[22]

Kostnads-nyttoanalys eller *cost-benefit* analyser (CBA) syftar till att hitta en effektiv balans mellan risker, åtgärder och kostnader. Nyttan av en (riskhämmande) åtgärd ska vägas mot dess kostnad, där nyttan mäts som ökningar i individers välfärd och kostnaden mäts som minskningar av

[21] Möller (1986)
[22] Utförligare beskrivning av kostnads-nyttoanalys återfinns exempelvis i Mattson (2006).

densamma. I en kostnads-nyttoanalys jämförs ett projekts totala nytta med projektets samtliga kostnader. För att detta ska vara möjligt måste begreppen mätas i samma enhet. I CBA har man valt att uttrycka värderingarna i pengar.[23]

CBA (och VSL) förutsätter att två kriterier är uppfyllda. Dels kan åtgärderna inte gälla specifika identifierade individer, dels får åtgärderna endast innebära små förändringar i risker för ohälsa eller för tidig död.[24] Modellen kan således inte användas när en sjukvårdare prioriterar vem som ska få hjälp vid en inträffad olycka, men däremot vid infrastrukturåtgärder som ökar trafiksäkerheten.

Ofta används ett effektivitetskriterium för att avgöra om en åtgärd bör vidtas eller inte. Ett sådant kriterium är Paretokriteriet, vilket innebär att en åtgärd är önskvärd om en individ får det bättre utan att någon annan individ får det sämre.[25] Dock är det många åtgärder som kan innebära att några får det sämre mot att fler får det bättre. Med Hicks/Kaldor-kriteriet väljer man istället den åtgärd där nyttan överstiger kostnaden. Kriteriet är en vidareutveckling av Paretokriteriet och går ut på att de vinnande individerna kan kompensera förlorarna om samhällets totala välfärd maximeras.[26] VSL används i dessa sammanhang om åtgärden som diskuteras räddar liv. Om kostnaden för en åtgärd som räddar ett liv är lägre än värdet på det statistiska livet så bör åtgärden genomföras, annars inte. Generellt ska således totala kostnaden för åtgärden vara lägre än VSL × antalet liv som åtgärden räddar.

Det är dock inte alltid vi agerar efter dessa principer. Guido Calabresi[27] har pekat på skillnaden mellan vad samhället ibland spenderar på att rädda livet på en identifierad person i fara och vad det spenderar för att minska antalet framtida dödsolyckor. Han ger ett exempel med en instängd gruvarbetare och jämför de ansträngningar och kostnader som spenderas för att undsätta honom med avsaknaden på avskaffandet av farliga plankorsningar, vilket skulle rädda fler liv för samma pengar. Två aspekter spelar in här, dels att vid en olycka finns en *identifierad* person som är i fara, dels de knappa *tidsförhållandena*. De ”statistiska” liven räddas vanligtvis i framtiden, så när olyckan väl är framme väljer människor att prioritera den individ som behöver hjälpen just då.

[23] Svensson (2007)
[24] Hultkrantz & Svensson (2008)
[25] Lindahl (2001)
[26] Denna kompensation är dock endast hypotetisk, och innebär inte att den nödvändigtvis måste ske.
[27] Ur Glover (1990)

Resultatet från en CBA behöver inte heller följas slaviskt, utan är ett systematiskt sätt att identifiera och värdera åtgärder och leder således till bättre underbyggda beslut.[28]

2.3.3 Invändningar

De finns tre vanliga invändningar till att försöka värdera mänskligt liv:[29]

- Mänskligt liv är av oändligt värde
- Det är farligt att försöka sätta ett värde på mänskligt liv
- Det är missvisande att försöka beräkna ett genomsnittsvärde då ingen människa är den andra lik och det är opassande att beräkna individuella värden

Av dessa tre är den första den absolut vanligaste invändningen. Antar vi att ett liv är oändligt mycket värt får vi dock orimliga resultat vid åtgärdsprioriteringar eftersom detta skulle innebära att alla projekt som minskar risken för död är lönsamma (oavsett kostnad). Vid ett sådant tillvägagångssätt skulle vi i princip inte ha uppnått någon användbar prioritering alls, vilket medför att inga resurser ska läggas på åtgärder som inte minskar risker. Dessutom handlar enskilda individer långt ifrån alltid i kongruens med ett oändligt livsvärde (t.ex. när vi inte använder cykelhjälm eller flytväst).

Den andra invändningen handlar om att när ett pris är satt på någonting genomgår det någon form av kvalitetsförändring (känslan av att titta på en oändligt vacker tavla avtar när man hör att tavlan sålts för endast 2 000 kr). Det finns också en känsla av att om ett pris är satt på någonting så kan detta någonting bli köpt. Om en individs liv är värt till exempel en miljon kronor för samhället, skulle enligt detta argument, hon kunna bli köpt och ”tillintetgjord” ostraffat av en individ som har en miljon att betala in till samhället.

Oavsett vilket av argumenten vi talar om gäller dock att vi inte försöker beräkna vad ett mänskligt liv *borde* vara värt, utan vilket värde människor *de facto* sätter på ett liv. [30]

[28] Kågebro & Vredin Johansson (2008)
[29] Hayzelden (1968)
[30] Hayzelden (1968)

3 Försvarsmaktens riskhanteringsmodell

Detta kapitel beskriver den riskhanteringsmodell som tagits fram inom Försvarsmakten (FM) och bygger framför allt på arbetshandlingar som använts vid utvecklandet av riskhanteringsmodellen samt författarens egna erfarenheter som operationsanalytiker på Insatsstaben från detta arbete. Beskrivningen har sedan kompletterats med information ur Metodanvisning för FM Gemensamma Riskhanteringsmodell[31] om inte annat anges.

En översiktsbild över modellen och de bedömningsskalor som används återfinns i Bilaga 1. Förklaring av akronymer finns i Bilaga 3.

3.1 Bakgrund

Som tidigare nämnts, dödades i november 2005 två svenska soldater i Afghanistan, vilket var de första (och hittills enda) dödsfallen Sverige råkat ut för sedan vårt engagemang i Afghanistan påbörjades. Soldaterna som dog färdades på en väg när en så kallad IED, *improvised explosive device*, exploderade under deras fordon. Händelsen ledde till att ett antal utredningar och arbetsgrupper tillsattes för att om möjligt förhindra nya liknande incidenter. Försvarsmaktens interna utredning visade att olika hot- och riskbedömningar hade gjorts av olika funktioner och nivåer i organisationen, vilket i sin tur kan ha lett till att felaktiga beslut hade tagits någonstans i beslutskedjan. Överbefälhavaren (ÖB) uttalade en önskan om gemensam ”risk management” i Försvarsmakten och ”arbetsgrupp riskhantering” startades upp. Gruppen bestod av representanter från de olika nivåerna i organisationen (från taktisk till militärstrategisk nivå) samt representanter från ett antal specifika funktioner. Militära underrättelse- och säkerhetstjänsten (MUST) tillsammans med Insatsstaben var sammanhållande för gruppen. Uppdraget var att ta fram en sammanvägd metod för riskbedömning och riskhantering för de insatser som Försvarsmakten genomför.

Ett antal krav/riktlinjer ställdes upp för metoden:

- Metoden ska kunna användas för bedömning och hantering av alla typer av risker, oavsett ”riskutlösande faktor”[32]
- Metoden ska kunna användas vid såväl insatser inom som utom riket

[31] FM (2007) (remissutgåva)
[32] Riskutlösande faktor förklaras ytterligare i avsnitt 3.2.1

- Metoden ska kunna vara användbar på alla militära nivåer
- Metoden ska vara transparent och spårbar så att chefen kan granska och ifrågasätta resultatet av analysen
- Metoden ska kunna användas i situationer där Försvarsmakten och civila myndigheter samverkar inom ett område där gemensam riskhantering krävs
- Metoden ska vara anpassad efter Försvarsmaktens behov, men så långt som möjligt harmoniera med Nato:s riskhanteringsprocesser

Under 2006 pågick arbetet med att ta fram en sammanvägd metod för riskbedömning och riskhantering för de insatser som Försvarsmakten genomför. Modellen, ”FM gemensamma riskhanteringsmodell”, är främst framtagen som ett stöd vid analys och hantering av de risker Försvarsmakten utsätts för vid internationell verksamhet, i syfte att:

- ge chefer ett adekvat underlag för beslutsfattande,
- underlätta samarbete mellan funktioner och nivåer, samt
- säkerställa spårbarhet och transparens,

men ska, i enlighet med föregående punktlista, även kunna användas för andra typer av riskhantering inom Försvarsmakten.

3.2 Modellen

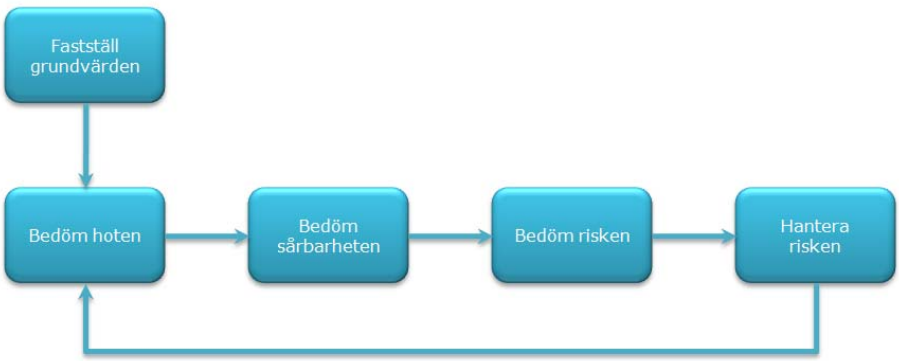
Riskhanteringsmodellen blev klar i början av 2007 och har sedan dess genomgått ett antal smärre korrigeringar och förbättringar. Det har också utarbetats en omfattande metodanvisning för modellen. Metodanvisningen kommer i sin slutliga version bli en del i Försvarsmaktens serie av handböcker.[33]

I Försvarsmaktens modell (som i första hand är avpassad för riskhantering av aktörsdrivna hot) används följande definitioner för begreppen hot och risk:

Hot	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten
Risk	Produkten av sannolikheten för att ett givet hot realiseras och därmed uppkommande skadekostnad

Modellen består av fem steg (se Figur 3), där olika funktioner och nivåer i Försvarsmaktens organisation är ansvariga för olika steg.

[33] Handboken kommer att publiceras under slutet av 2008 eller början av 2009.



Figur 3. De fem stegen i Försvarsmaktens riskhanteringsmodell.

3.2.1 Steg 1 – Fastställ grundvärden

I det första steget ska grundvärdena för riskhanteringen fastställas. Detta görs av den ansvarige chefen.

Riskhanteringen inleds med att definiera uppgiften som ska riskhanteras. I detta ingår att bestämma vilken tidsperiod och vilket område riskhanteringen ska omfatta, samt utifrån vilka uppgifter och förutsättningar analysen ska göras.[34] Därefter läggs grunden i riskhanteringsarbetet genom att identifiera vad som är skyddsvärt.

En skyddsvärd tillgång är någonting som Försvarsmakten av olika anledningar anser värt att skydda.[35] Skyddsvärda tillgångar kan till exempel uppstå inom något av områdena information, personal, materiel eller förtroende. När det gäller de internationella insatserna utgår riskhanteringen ofta från personalens liv och hälsa.

Ibland kan det dock vara svårt att avgöra om en verksamhet är skyddsvärd. För att avgöra om något är skyddsvärt kan man titta på vilken skada som uppkommer om det studerade blir kompromitterat. Detta kan också vara användbart i senare steg i riskhanteringen, när konsekvenserna av ett visst hot ska bedömas. Det är också viktigt att tänka på att påverkan på en skyddsvärd tillgång indirekt även kan påverka andra skyddsvärda tillgångar (och i vissa fall även leda till allvarligare konsekvenser än för den ursprungliga skyddsvärda tillgången). Om till exempel en minnessticka med sekretessbelagd information glöms kvar på en

[34] Uppgiften skulle till exempel kunna vara att genomföra riskhantering på insatsen i Afghanistan för perioden år 2008 utgående ifrån svenska operationsplanen för insatsen.
[35] H Säk Hot (2006)

konferensanläggning är den skyddsvärda tillgången ”sekretessbelagd information” och den direkta konsekvensen skulle kunna bli att dokument med Nato-hemligklassad information röjs. Detta påverkar dock i sin tur den skyddsvärda tillgången ”anseende”, och får indirekta konsekvenser i form av exempelvis begränsningar i tillgång till Nato-information och minskat samarbete med Nato i framtiden. Detta skulle ske på grund av att länderna i Nato anser att Sverige inte klarar av att hantera sekretessbelagd information på ett tillfredsställande sätt och att de därmed inte längre kan lita på Sverige.

Innan nästa steg i riskhanteringen påbörjas måste den ansvarige chefen även fastställa vilka utlösande faktorer som är aktuella för uppgiften samt vilken konsekvensskala som ska användas. Utlösande faktorer är de tänkbara hot som kan förekomma i området och som är riktade mot den skyddsvärda tillgången. Hoten ska vara rimliga, relevanta och i ett hanterbart antal.[36] Ju mer precist de utlösande faktorerna beskrivs, desto lättare blir det att genomföra påföljande steg i riskhanteringsprocessen. Exempel på hot vid riskhantering av utlandsinsats skulle kunna vara ”IED mot fordon och transporter” eller ”våldsamt upplopp riktat mot camp”.

I detta första steg av riskhanteringen ska chefen även besluta om en konsekvensskala. Skalan är tiogradig, från ”försumbar” (1) till ”synnerligen allvarlig” (10). Vad de olika stegen innebär definieras av chefen innan själva riskanalysen påbörjas, och utformas utifrån den miljö för vilken riskanalysen ska göras. Med fördel bestäms lägsta och högsta nivå först och därefter mellanliggande steg. Se Tabell 1 nedan för två exempel med olika gradering där personalens liv och hälsa har prioriterats. Det är även möjligt att vikta konsekvensskalan genom att gruppera flera steg (se Tabell 2).

Alla beslut under steg 1 ska fattas av ansvarig chef (till exempel chefen för en taktisk stab eller ÖB) och dokumenteras skriftligt.

[36] H Säk Hot (2006)

Tabell 1. Konsekvensskalor.
Tabellen visar skalans gradering och två exempel där personalens liv och hälsa prioriterats. Förutom att olika lägsta respektive högsta nivå är satt i exemplen, är exempel 2 även mer utförligt beskrivet vilket minskar risken för tolkningssvårigheter.

Konsekvensskala		Exempel 1	Exempel 2
9-10	Synnerligen allvarlig	Flera döda och/eller svårt skadade.	Ett stort antal döda (>10) och många allvarligt skadade.
7-8	Allvarlig	Skada som kräver avancerad läkarvård. Dödsfall kan förekomma.	Flera döda (<10) och flera allvarligt skadade.
5-6	Kännbar	Skada som kräver läkarvård.	Skada som kräver kvalificerad sjukvård (Role 3)[37]. Permanenta fysiska men, och dödsfall, kan förekomma.
3-4	Lindrig	Skada som kräver enklare vård.	Skada som kräver läkarvård (Role 1-2). Eventuellt kortare konvalescens, men inga permanenta fysiska men.
1-2	Försumbar	Skada som ej kräver vård.	Skada som kräver enklare vård (egenvård, sjuksköterska).

Tabell 2. Viktade konsekvensskalor.

Konsekvens		Skala 1	Skala 2
Synnerligen allvarlig	Förbandet kan inte lösa huvuduppgiften	10	5-10
Allvarlig	Förbandet kan endast lösa huvuduppgiften, dessutom med begränsningar	9	4
Kännbar	Förbandet kan endast lösa huvuduppgiften	8	3
Lindrig	Förbandet kan lösa huvuduppgiften, men med begränsningar i sidouppgifter	6-7	2
Försumbar	Förbandet kan lösa huvuduppgiften och sidouppgifter	1-5	1

[37] För utförligare beskrivning av Role-begreppen, se Ordförklaringen i Bilaga 3.

3.2.2 Steg 2 – Bedöm hotet

När de utlösande faktorerna, eller hoten, är fastställda ska dessa bedömas utifrån intention, kapacitet och tillfälle.[38] Intentionen är en aktörs vilja, motiv och mål. Kapaciteten är en aktörs resurser och förmågor (i form av exempelvis utrustning och personal). Tillfälle syftar till när och var en aktör kan angripa en skyddsvärd tillgång. Dessa tre faktorer vägs samman och resulterar i en hotnivå. Hotnivån ges på en femgradig skala, enligt Tabell 3 på nästa sida.

Det går dock inte att ”beräkna” en hotnivå utifrån de tre variablerna. Ta exempelvis en situation där man gjort bedömningen att aktören både har mycket hög kapacitet (5) och mycket stora möjligheter (5), men ingen synbar intention (1). Om vi beräknar medelvärdet får vi hotnivå 4, det vill säga ”Högt hot”, men är detta rimligt? Ta exemplet att den skyddsvärda tillgången är liv och hälsa för personal vid en av FOI:s avdelningar, och att aktören är en annan avdelning vid FOI. Denna andra avdelning har både kapacitet och tillfälle att (negativt) påverka den första avdelningen genom sina expertkunskaper om till exempel farliga ämnen. Däremot torde intentionen att utnyttja dessa kunskaper i någon form av ”angrepp” vara näst intill obefintligt. Det vore orimligt att klassa denna situation som ett högt hot.

Hotbedömningen görs av aktuell underrättelsefunktion (till exempel MUST, J2 eller G2), och det krävs kvalificerade resurser för att kunna göra en tillförlitlig hotbedömning. Ibland är det inte ens möjligt att avgöra hur allvarligt ett hot är. För mer utförlig information om hotbedömningar hänvisas till Metodanvisning FM Gemensamma riskhanteringsmodell och Försvarsmaktens handbok för hotbedömning.[39]

3.2.3 Steg 3 – Bedöm sårbarheten

Sårbarhetsbedömningen är en värdering av den egna organisationen i förhållande till de aktuella hoten. Bedömningen görs med avseende på säkerhetsmedvetande, resurser och exponering.[40] Säkerhetsmedvetandet är den egna viljan att skydda sig mot de aktuella hoten, genom exempelvis utbildning eller uppträdande. Resurser är organisationens tillgängliga resurser (utrustning) för skydd mot aktuellt hot, och exponering är var och när man utsätter sig för hot. Även sårbarhetsbedömningen kräver mycket resurser och kunskap för att ge ett gott resultat.

[38] H Säk Hot (2006)
[39] FM (2007); H Säk Hot (2006)
[40] H Säk Skydd (2007)

Tabell 3. Hotnivåer.

Hotnivå			Beskrivning
5	Mycket högt hot	Röd	Incidenter inträffar mer eller mindre dagligen. Aktören bedöms försöka genomföra verksamheten till varje pris utan hänsyn till konsekvenser för den egna säkerheten. Ogynnsamma miljö- och/eller sociala faktorer finns och har mycket stor och uppdragshotande inverkan.
4	Högt hot	Orange	Information som tyder på hög kapacitet, intention och tillfälle hos potentiell aktör. Incidenter har inträffat vid ett flertal tillfällen i närtid. Ogynnsamma miljö- och/eller sociala faktorer finns och har stor och möjligen uppdragshotande inverkan.
3	Förhöjt hot	Gul	Information som tyder på reell kapacitet, intention och tillfälle hos potentiell aktör. Enstaka incidenter har inträffat. Ogynnsamma miljö- och/eller sociala faktorer finns och har stor, men inte uppdragshotande, inverkan.
2	Lågt hot	Grön	Information som tyder på begränsad kapacitet, intention och tillfälle hos potentiell aktör. Inga incidenter har förekommit i närtid. Ogynnsamma miljö- och/eller sociala faktorer finns men har låg inverkan.
1	Inget identifierat hot	Vit	Ingen information som tyder på kapacitet, intention och tillfälle hos en potentiell aktör. Inga incidenter har förekommit i närtid. Ogynnsamma miljö- och/eller sociala faktorer saknas.

Sårbarheten bedöms på en femgradig skala (motsvarande den för hotbedömningen, se Bilaga 1) för varje enskild faktor. Vilka faktorer som bedöms beror återigen på vad uppgiften som ska riskhanteras består av. För internationella insatser har man valt att dela in sårbarheterna i fyra kategorier: förebyggande skydd (t.ex. utbildning, förbandssammansättning), aktivt skydd (t.ex. vapen- och varningssystem), passivt skydd (t.ex. skyddsrum, splitterskydd) samt återhämtning/återställning (t.ex. sjukvårdsresurser, reparationsresurser).[41] Kategorierna är desamma som används för *Force Protection* inom Nato.

När riskanalysen görs på ett nytt område, till exempel i planeringsfasen av en ny insats, är det extra viktigt att fundera över omständigheterna kring de skyddsvärda tillgångarna som omfattas av riskanalysen, eftersom denna ligger till grund för vilka resurser förbandet får.

Sårbarhetsbedömningen görs av aktuell planeringsfunktion (till exempel J3 eller M3).

3.2.4 Steg 4 – Bedöm risken

Resultatet av hotbedömningen (steg 2) och sårbarhetsbedömningen (steg 3) ger underlag för riskbedömningen som görs av underrättelse- och genomförande-funktionerna gemensamt.

I riskbedömningen ska bedömas dels sannolikheten för att ett hot inträffar, dels vilken konsekvens hotet skulle få. I Försvarsmaktens modell betecknar risk, som tidigare nämnts, kombinationen av sannolikhet och konsekvens.

Sannolikheten kan antingen skattas utifrån bedömarnas egna erfarenheter (kvalitativ bedömning) eller beräknas med någon metod utifrån statistiskt material (kvantitativ bedömning). Vid riskhantering av internationella insatser är det vanligast att en kvalitativ bedömning görs, eftersom förhållandena sällan är likvärdiga från insats till insats. För att en bedömning ska få tillräcklig kvalitet måste skattningarna göras av personer med god kännedom om aktuella förhållanden, och det är detta steg 2 och 3 i modellen säkerställer.

Både sannolikheten och konsekvensen bedöms på en tiogradig skala. Konsekvensskalan fastslogs av ansvarig chef under steg 1 och sannolikhetsskalan är en statisk skala, enligt Tabell 4. Om personerna som genomför bedömandet inte skulle komma överens har underrättelsefunktionen rätt att ta beslut när det

[41] Krisberedskapsmyndigheten använder som jämförelse de fyra faserna: förebyggande, förberedande, hanterande och återuppbyggande (KBM, 2006a).

gäller sannolikhetsbedömningen, medan genomförandefunktionen beslutar nivån för konsekvensbedömningen.

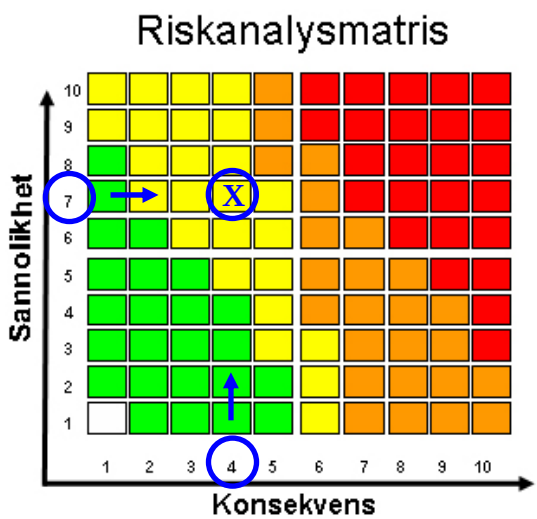
Tabell 4. Sannollikhetsskalan

Sannolikhetsskala		
Sannolik	> 50 %	9-10
Trolig	< 50 %	7-8
Möjlig	< 25 %	5-6
Mindre trolig	< 5 %	3-4
Osannolik	< 1 %	1-2

Sannolikhetsvärdet och konsekvensvärdet förs sedan in i en riskanalysmatris (se Figur 4), varur ett risknivåvärde kan utläsas. Risknivåskalan är motsvarande hot- och sårbarhetsskalorna (se Tabell 5). Riskanalysmatrisen är konstruerad så att konsekvensen väger tyngre än sannolikheten eftersom en allvarlig konsekvens har bedömts ha större betydelse än en hög sannolikhet. Om sannolikhet och konsekvens hade vägt lika tungt hade matrisen varit symmetrisk. Nu kan man tydligt se att till exempel den övre vänstra kvadranten i riskanalysmatrisen har lägre risknivåer än den nedre högra kvadranten.

Tabell 5. Risknivåskalan.

Risknivåskala	
5	Mycket hög risk
4	Hög risk
3	Förhöjd risk
2	Låg risk
1	Ingen synbar risk



Figur 4. Riskanalysmatrisen.
Om konsekvensen bedöms till 4 och sannolikheten till 7, så blir risknivån gul = förhöjd risk.

I tre situationer sätts risknivån automatiskt till ”ingen synbar risk”. Dessa tre fall är:

- Om ett visst hot har bedömts utgöra ”inget synbart hot”
- Om sannolikheten för ett visst hot bedöms vara ”noll”
- Om konsekvensen av ett inträffat hot bedöms vara obefintlig (det vill säga om det inträffade hotet omöjligen kan penetrera befintliga skyddsåtgärder).[42]

Eftersom riskbedömningen ofta består av två subjektiva bedömningar, som sedan kombineras, blir resultatet än mer osäkert än de ursprungliga faktorerna. Det är således viktigt att hot- och sårbarhetsbedömningar, som ligger till grund för riskbedömningen, genomförs så noggrant som möjligt.

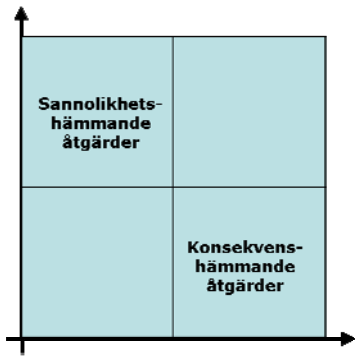
3.2.5 Steg 5 – Hantera risken

Detta steg kan jämföras med riskvärderingssteget i den allmänna beskrivningen av riskhantering i kapitel två, och syftar till att avgöra om en identifierad risk kan accepteras eller ska åtgärdas. När analysen är klar ska den ansvarige chefen (samma som i steg 1) ta ställning till om risken (det vill säga risknivån för ett specifikt hot) är acceptabel eller inte. Om risken inte kan accepteras ska beslut om skyddsåtgärder tas för att minska risken. I det omfattande arbetet med hot- och sårbarhetsbedömningarna kan förslag på möjliga skyddsåtgärder redan ha framkommit, vilket i så fall underlättar själva riskhanteringsarbetet.

De förslag på åtgärder som tas fram måste dock ”testas” i riskhanteringsmodellen för att säkerställa att åtgärderna inte leder till nya högre risker. Detta kan göras genom att på nytt titta på hot- och sårbarhetsbedömningarna och, med den eller de föreslagna åtgärderna i åtanke, göra en ny bedömning för de faktorer där det är relevant och på så sätt generera en ny riskbedömning som (förhoppningsvis) resulterar i en ny lägre risknivå. I allmänhet hanterar man risker inom den övre vänstra kvadraten i riskanalysmatrisen främst genom sannolikhetshämmande åtgärder, medan risker inom den nedre högra kvadranten hanteras främst genom konsekvenshämmande åtgärder (se Figur 5).

[42] Bakgrunden till denna lösning beskrivs i avsnitt 3.5.

Om de egna resurserna inte räcker till för de skyddsåtgärder som anses nödvändiga ska hemställan göras till högre chef om ytterligare resurser för att skapa en situation med en acceptabel risknivå. Om den ansvarige chefen således inser att denna riskökning är så stor att han eller hon inte har tillräckliga medel för att vidta skyddsåtgärder och att den högre risknivån inte är acceptabel, hemställs om ytterligare resurser från högre chef (i nästa nivå i organisationen). Denna chef måste sedan i sin tur avgöra om, och i så fall vilka, åtgärder som ska vidtas eller om risken ska accepteras. Om han eller hon beslutar att acceptera den högre risken, har också ansvaret flyttats till denne chef, annars hemställs återigen till högre chef om ytterligare resurser, osv.



Figur 5. Sannolikhets- och konsekvenshämmande åtgärder.

Alla beslut i detta steg skall precis som i första steget dokumenteras skriftligt.

3.3 Verktyg

Tillsammans med riskhanteringsmodellen som just beskrivits har Försvarsmakten även tagit fram ett ”verktyg” som ska användas vid hot-, sårbarhets- och riskbedömningarna. I verktyget, som mer är ett hjälpmedel i form av en stor excel-matris, fylls de utlösande faktorerna i på ena axeln mot skyddsvärd tillgång, bedömd hotnivå, sårbarhetsnivå, sannolikhet, konsekvens och slutligen risknivå på den andra axeln. Genom att fylla i hela matrisen fås en god översikt på hela riskbedömningen. I Figur 6 återfinns ett komprimerat exempel på delarna i verktyget, och i Bilaga 1 återfinns ett mer utförligt fiktivt exempel på hur verktyget kan se ut och användas.

HOT		SKYDDS-VÄRDA TILLGÅNGAR	IDENTIFIERA SKYDD BEDÖM SÅRBARHETER										
			Förebyggande skydd			Aktivt skydd		Passivt skydd		Återhämtning/ Återställaning			
Konkret oönskad händelse/ företeelse/ vapensystem/ metod/modus	Hotnivå		Utbildning	PSYOPS	CIMIC	Varningssystem	Elektroniska motmedel	Pers utr., kroppsskydd	Splitterskyddade fordon	Kamrathjälp	MEDEVAC	Sjukvård ROLE 1-3	STRATEVAC
IED mot fordon	3	Liv och hälsa	3	2	2	5	5	2	4	2	3	2	1
Konkret hot B													
Konkret hot C													

Figur 6. Verktyg för bedömning av hot, sårbarheter och risknivåer.

3.4 När och hur ofta ska analyserna ske?

En riskanalys ska göras:

- regelbundet för mål och uppföljning,
- vid förändringar,
- vid ny kunskap, samt
- vid icke-rutin-operationer.[43]

En grov riskanalys bör göras redan i samband med diskussionerna mellan den politiska nivån och Försvarsmakten om en presumtiv insats. När beslut om insats är fattat tas det första riskhanteringsbeslutet. När planeringen väl sätter igång kan analysen förfinas och nya beslut tas. Det räcker dock inte med att göra denna första analys och riskhantering, utan processen måste upprepas kontinuerligt. Hur ofta riskanalysen bör uppdateras beror på vilken nivå i organisationen man befinner sig på. Vid en internationell insats är nivåerna hemma i Sverige ansvariga för att bevaka utvecklingen i insatsområdet på längre sikt, medan förbandet på plats dagligen måste fatta riskhanteringsbeslut.[44] De olika tidsperspektiven är kopplade till tiden det tar att implementera skyddsåtgärder på respektive nivå. I insatsområdet kan det kanske vara aktuellt att genomföra

[43] Wennersten (2004)
[44] Riskhanteringsmodellen används dock inte direkt i dagliga beslut.

analysen åtminstone en gång per månad, medan det för den gemensamma riskanalysen kanske räcker med två gånger per år.[45] Se även Tabell 6.

Tidpunkt	Riskanalys	Riskhanteringsbeslut
Under diskussioner mellan politisk nivå och FM	Grov riskanalys på militärstrategisk nivå	Beslut om insats
Planering av insats (efter beslut)	Gemensam riskanalys i samband med detaljplanering	Ev. samordnade riskhanteringsbeslut innan deployering
Ca 3 månader in i insats	Omfattande gemensam riskanalys	Samordnat riskhanteringsbeslut
Löpande under pågående insats	Varje nivå överser riskanalysen vid förändringar	Respektive nivå fattar risk-hanteringsbeslut efter givna förutsättningar
Ca var 6:e månad	Gemensam översyn av tidigare gjord riskanalys	Samordnat riskhanteringsbeslut om behov av justeringar finns
På förekommen anledning	Gemensam översyn av tidigare gjord riskanalys	Samordnat riskhanteringsbeslut om behov av justeringar finns

Tabell 6. Tidpunkter för riskhantering

De högre nivåerna i organisationen bör dock ta del av de lägre nivåernas analyser vartefter de produceras. Om det vid en uppdatering av riskanalysen upptäcks att ett visst hot leder till en ökad risknivå ska nödvändiga åtgärder vidtas (alternativt beslut om ökad risktagning tas enligt ovan).

[45] Detta är endast ett exempel. Beroende på hotbild i insatsområdet kan chefen bli tvungen att fatta beslut om och genomdriva skyddsåtgärder snabbare än planerat.

3.5 Erfarenheter från utvecklandet av modellen

Här följer en diskussion kring erfarenheter från författarens personliga medverkan som operationsanalytiker på Insatsstaben i utvecklandet av Försvarsmaktens nya riskhanteringsmodell. Ytterligare erfarenheter och slutsatser från användandet av modellen kommer att publiceras i en separat rapport under början av 2009.

Riskmatrisen som används i modellens fjärde steg har under utvecklingsarbetet varit föremål för omfattande diskussioner, bland annat diskuterades detaljnivån i matrisen länge. Vissa deltagare i arbetsgruppen ansåg att en matris med fem steg på varje axel var tillräckligt, medan andra ville ha en mer detaljerad matris. Att resultatet slutligen blev den mer detaljerade varianten berodde sannolikt på att det i denna variant enklare går att ”kryssa in” de bedömda risknivåerna i matrisen (se Figur 4 i avsnitt 3.2.4) och på så sätt få en överblick över de olika riskerna. MUST har även tagit fram en mindre detaljerad variant som används i Försvarsmaktens handbok för säkerhetsskyddstjänst.[46]

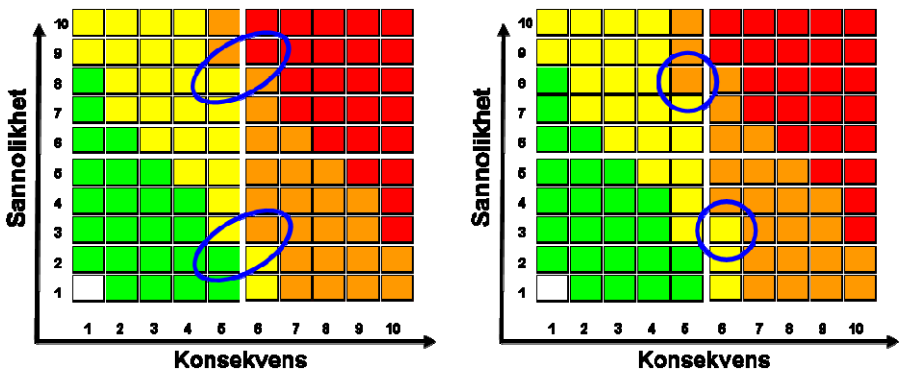
Det diskuterades också om det skulle finnas med en vit ruta (”ingen synbar risk”) i matrisen överhuvudtaget eller om det vita området till och med skulle sträcka sig över hela första raden och/eller hela första kolumnen. Denna diskussion, som främst fördes mellan operationsanalytikerna på Insatsstaben och den ansvarige analytikern på MUST, härrörde ur frågan huruvida ett hot som bedömts som ”inget synbart hot” verkligen är ett hot som ska riskhanteras. I samma anda diskuterades även avsaknaden av alternativen ”ingen konsekvens” och ”sannolikhet noll”. Slutresultatet av diskussionerna blev att matrisen inte skulle förändras och att dessa tre (special)fall hanteras i särskild ordning (om något av dessa tre kriterier är uppfyllt sätts risken till ”ingen synbar risk” direkt). Motivet till att behålla hot som bedömts till ”inget synbart hot” i riskhanteringen var dels att få bättre spårbarhet mellan jämförelserna, dels att inte riskera att ”tappa bort” ett visst hot i framtida bedömningar på grund av att det tagits bort ur hotkatalogen i en tidigare jämförelse. Hotnivån kan ju trots allt ändras över tiden.

Motivet till att även ha med ”ingen konsekvens” och ”sannolikhet noll”, var att det trots allt kändes naturligt att kunna skilja på en situation där konsekvensen/sannolikheten är näst intill obefintlig (eller fullständigt okänd) från en situation där man känner till konsekvensen/sannolikheten, fast den har ett

[46] Se H Säk Skydd (2007)

mycket lågt värde. Det var då mer praktiskt att lägga till dessa specialfall i modellen, än att förändra alla skalor och matrisen för att korrigera detta.[47]

En tredje synpunkt som framfördes av Insatsstabens operationsanalytiker var att på två ställen i matrisen ökade risknivån med två nivåer om man endast förflyttade sig ett steg på sannolikhets- respektive konsekvensskalan. Detta verkade lite olyckligt, speciellt då dessa förflyttningar på konsekvensaxeln skedde inom de skalsteg som ofta grupperas. Detta fick en enkel lösning genom att två av rutorna i matrisen bytte färg med varandra. På detta sätt försvann ”två-nivåhoppet” samtidigt som fördelningen mellan de olika risknivåerna i matrisen inte förändrades.



Figur 7. Ursprunglig matris till vänster och ny åtgärdad matris till höger. Vid förflyttning från 5 till 6 på konsekvensskalan samtidigt som förflyttning från 2 till 3 eller från 8 till 9 på sannolikhetsskalan i den vänstra figuren, förändras risknivån två nivåer. Detta åtgärdades genom att ändra risknivån på två rutor i matrisen, från orange till gul i den nedre rutan respektive från gul till orange i den övre rutan (resultatet, med de två rutorna inringade, i den högra matrisen).

Det sista steget i riskhanteringsmodellen, riskvärderingen eller att ”hantera risken” som Försvarsmakten valt att kallat det, är det minst utvecklade i modellen. Det finns egentligen ingen metod utvecklad för detta steg överhuvudtaget, utan i dagsläget antas att eventuella åtgärder och prioriteringar hanteras utanför modellen. I den ursprungliga modellen fanns inte heller någon återkoppling från detta steg tillbaka in i modellen (till steg 2). Detta infördes dock efter en diskussion i arbetsgruppen.

[47] Ursprungliga argumenten mot detta var att sannolikheten aldrig kan vara noll och att någon konsekvens alltid finns.

3.6 Vägen framåt

Under våren 2007 genomfördes en första utbildningsomgång om modellen, verktyget och metoderna som används i arbetet. I samband med denna genomfördes även en första riskanalys för de insatser Försvarsmakten är engagerade i (t.ex. ISAF och KFOR) samt för vissa områden och insatser där ett framtida svenskt bidrag kunde bli aktuellt. Även *Nordic Battle Group* (NBG) har under 2007 och 2008 använt modellen i sitt planeringsarbete. Analyserna har uppdaterats, och det har även gjorts bedömanden (med uppdaterande analys) för den nya insatsen i Tchad.

De synpunkter som framkom vid utbildningen och efterföljande arbete har tagits tillvara och mindre förändringar gjorts i själva modellen och metoderna.[48] En andra, förbättrad och mer utförlig, remissutgåva av metodanvisningen har också producerats.[49] Innan metodanvisningen slutgiltigt fastställs kommer ett antal intervjuer genomföras med beslutsfattare och användare av modellen. Resultatet från dessa kommer att inarbetas i metodanvisningen innan den slutgiltigt fastställs och trycks som en del i Försvarsmaktens serie av handböcker. Erfarenheterna som framkommer från intervjuerna kommer också, tillsammans med tidigare genomförda mer informella intervjuer och andra erfarenheter från användandet av modellen, att publiceras i en andra FOI-rapport om Försvarsmaktens riskhanteringsmodell i början av 2009.

[48] Modell, verktyg och metoder är i denna rapport beskrivna förändringarna medtagna
[49] FM (2007)

4 Riskhanteringsmodeller hos andra myndigheter

I samband med utvecklingen av Försvarsmaktens gemensamma riskhanteringsmodell efterfrågade Försvarsmaktens generaldirektör en snabb jämförelse av den nyutvecklade metoden och modeller hos andra (civila) myndigheter. Jämförelsen har fokuserats på de myndigheter (eller del av myndigheter) som själva publicerar rekommendationer om riskanalys och riskhantering till andra statliga myndigheter och kommuner eller av annat skäl är intressanta för jämförelsen. De undersökta myndigheterna är:

- Krisberedskapsmyndigheten (KBM)
- Räddningsverket (SRV)
- Kammarkollegiet
- Länsstyrelsen i Stockholms län[50]
- Säkerhetspolisen[51] (Säpo)
- Vägverket[52]

De flesta av dessa myndigheter (eller delar av myndigheter) publicerar handböcker, vägledningar eller annan dylik information om hur riskanalys och/eller riskhantering ska genomföras. I och med myndigheternas olika arbetsområden har också riskhanteringsprocesserna olika fokus, men ofta ligger viss tyngd på riskhantering gentemot personals liv och hälsa.[53] Nedan beskrivs varje organisations riskanalys- eller riskhanteringsprocess översiktligt.

[50] Länsstyrelsen i Stockholms län är en del av myndigheten Länsstyrelserna
[51] Säkerhetspolisen är en del av myndigheten Rikspolisstyrelsen
[52] Vägverket ingick inte den ursprungliga jämförelsen som presenterades för Försvarsmaktens generaldirektör
[53] I Kammarkollegiets modell ligger exempelvis större fokus på kostnadskalkylering av riskerna, medan Vägverket använder en intressant metod för värdera människoliv.

4.1 Krisberedskapsmyndigheten

I Krisberedskapsmyndighetens vägledning för statliga myndigheter[54] presenteras en femstegsmodell, enligt följande:

1. **Myndigheters roll och ansvarsområde**
   Identifiera vilken typ av riskhantering och inom vilka områden myndigheten är ålagd att riskhantera.
2. **Identifiering**
   Identifiera vilka hot och risker som föreligger.
3. **Värdering**
   Bedöm sannolikheten för att hoten och riskerna ska inträffa och de konsekvenser de kan leda till.
4. **Förmågebedömning**
   Bedöm förmågan att hantera ett eventuellt effektuerat hot (eller risk).
5. **Resultat och redovisning**
   Redovisa resultatet av riskanalysen tillsammans med åtgärder som måste vidtas och plan för finansieringen av dessa.

I vägledningen presenteras inga konkreta metoder för hur respektive steg skall genomföras. Istället ligger fokus på att ge en ökad förståelse för vad de olika stegen i riskhanteringen ska omfatta och vad som är viktigt att tänka på i varje steg. Vägledningen innehåller även en lista med definitioner på termer och begrepp inom riskhanteringsområdet samt förslag på vidare läsning för varje steg i modellen. I värderingskapitlet ges exempel på sannolikhets- respektive konsekvensskala (i form av femgradiga skalor) samt riskmatris (även den i fem nivåer).

Förmågebedömningen bör, enligt KBM, delas in i tre olika typer av förmågor: krisledningsförmåga, operativ förmåga samt förmåga i samhällsviktig verksamhet att motstå störningar. Det poängteras också att det inom vissa myndigheter kan vara nödvändigt att bryta ner dessa tre i mer specificerade kategorier. Förmågeskalan som KBM använder består av fyra steg från ”god förmåga” till ”ingen eller bristfällig förmåga”.

Vägledningen avslutas med en guide till hur resultatet ska presenteras, fokuserat på den årliga redovisning som Regeringskansliet (och KBM) ska få från andra myndigheter.

[54] KBM (2006b)

4.2 Räddningsverket

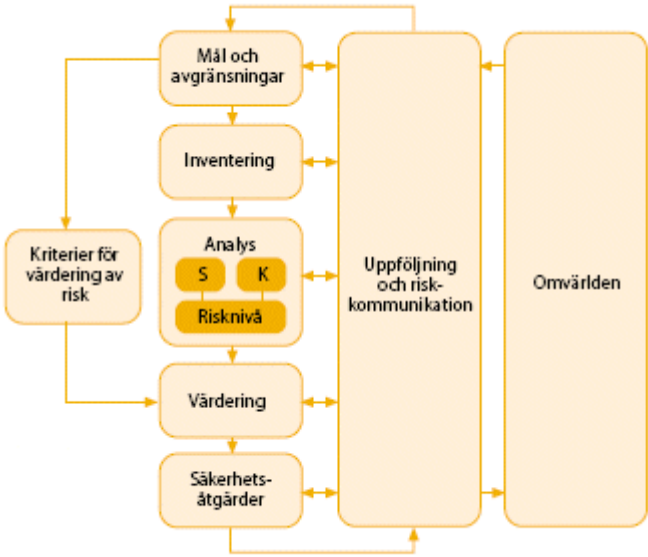
Räddningsverket (SRV) har en omfattande handbok för riskanalys.[55] Handboken täcker framförallt själva riskanalysen, men behandlar även översiktligt hela riskhanteringsprocessen. Handboken består dels av en introduktion till riskanalysområdet, dels av mer detaljerade beskrivningar av genomförandet av en riskanalys. SRV har valt att beskriva processen för olika områden var och en för sig, eftersom man anser att det praktiska genomförandet och lämpliga metoder för detta skiljer sig åt inom olika områden där SRV har ansvar.[56] Samma modell ligger dock till grund för samtliga områden. Även denna modell består av fem steg (se även Figur 8 nedan):

1. **Mål och avgränsningar**
   Utarbeta mål och avgränsningar för riskhanteringen, inklusive kriterier för riskvärdering.
2. **Inventering**
   Inventera och identifiera alla risker inom området.
3. **Analys**
   Bedöm sannolikhet och konsekvens för identifierade risker, och fastställ utifrån dessa en risknivå.
4. **Värdering**
   Avgör med hjälp av riskvärderingskriterierna hur allvarlig risken är.
5. **Säkerhetsåtgärder**
   Arbeta fram åtgärder för de risker som bör åtgärdas.

Den största skillnaden mellan Räddningsverkets handbok och övrigt studerat material är att Räddningsverket har valt att presentera och beskriva en mängd olika analysmetoder som kan användas i arbetet, vilket uppmanar till ett mer systematiskt angreppssätt vid riskanalysarbetet. I och med uppdelningen i olika områden kan också specifika exempel och rekommendationer ges för varje område, inklusive rekommendationer för vilken eller vilka analysmetoder, respektive redovisningstyper, som är bäst avpassade för just det området. Denna uppdelning är fördelaktig för de personer som ska riskhantera inom något av SRV:s områden, men kan vara lite mer tungrott för den som ska genomföra riskhanteringen på ett annat område. Den som vill göra en noggrann riskanalys

[55] SRV (2003)
[56] Uppdelningen är gjord i områdena Processtekniska anläggningar, Farligt gods på järnväg, Brand, Ras och skred samt Översvämning.

bör läsa igenom beskrivningarna för alla områden för att komma fram till vilken metod som är lämplig att användas.



Figur 8. SRV:s riskhanteringsmodell[57]

4.3 Kammarkollegiet

Kammarkollegiets kortfattade handledning för riskhantering behandlar endast ”risker vars negativa följder är ekonomiskt mätbara”[58], men är så generell att den även kan användas för andra typer av risker. Metoden består av fem steg:

1. **Riskidentifiering**
   Identifiera vilka risker som föreligger.
2. **Riskvärdering**
   Gradera de identifierade riskerna i fråga om sannolikhet och konsekvens.
3. **Riskbehandling**
   Besluta om risken ska åtgärdas, begränsas eller accepteras.

[57] Ur SRV (2003)
[58] Kammarkollegiet (2008)

4. **Genomförande av beslut**
   Genomför de åtgärder som beslutats om.

5. **Uppföljning**
   Följ upp effekten av genomförda beslut (framför allt tillämpbart när det gäller riskkostnader).

Kammarkollegiet använder även en något modifierad version där steg 4 och steg 5 ovan är ersatt av:

4. **Riskfinansiering**
   Fastställ hur eventuell skada (om en risk inträffar) ska finansieras.

Inget av stegen är beskrivna i detalj i det material som studerats, men ett antal formulär för riskhanteringen finns med tillhörande ”minimanual”. För exempel på formulär, se Kammarkollegiets hemsida.[59]

4.4 Länsstyrelsen i Stockholms län

Länsstyrelsen i Stockholms län har tillsammans med FOI och LUCRAM vid Lunds Universitet, och med stöd av KBM, utvecklat en scenariobaserad metod för arbete med risk- och sårbarhetsanalyser på lokal och regional nivå. Metoden bygger på att Länsstyrelsen och kommunerna genomför risk- och sårbarhetsanalys (RSA) i varsitt parallellt spår. Analysen består av fyra delar: förberedelse, genomförande, rapportering och riskbehandling. Till hjälp i arbetet har ett datorbaserat verktyg, IBERO, utvecklats.[60]

I kommunernas process väljs i det första steget personer ut att ingå i analysgruppen som ska genomföra risk- och sårbarhetsanalysen. Gruppen sammanställer sedan skyddsvärda tillgångar, risker och resurser i kommunen. Därefter görs en ”grovanalys” (sannolikhet och konsekvens skattas) på de händelser som Länsstyrelsen sammanställt. Utifrån denna väljs sedan de tre mest ”extraordinära” händelserna ut utifrån lokala förhållanden, samt eventuella ytterligare händelser som inte finns representerade i listan. Faktorer som kan påverka händelserna sammanställs, och därefter görs en analys med hjälp av verktyget IBERO. Sista steget i genomförandefasen är att sammanställa risker, sårbarheter och åtgärder. Därefter ska resultatet redovisas och rapporteras vidare, och slutligen sker riskbehandlingen i form av beslut i kommunstyrelsen på åtgärder som måste vidtas, upprättande av handlingsprogram, genomförande av

[59] Kammarkollegiet (2008)
[60] Finns att ladda ner, med mallar och manual på Länsstyrelsens hemsida, se Länsstyrelsen Sthlm (2008)

förebyggande åtgärder samt återkoppling. Parallellt med ovanstående process gör även Länsstyrelsen en risk- och sårbarhetsanalys.[61] De har också en analysgrupp, vilken granskar både myndigheternas och kommunernas RSA. Länsstyrelsen sammanställer sedan alla risk- och sårbarhetsanalyser och upprättar en rapport för hela länet. Därefter fattas, precis som på kommunnivån, beslut om vilka åtgärder som måste vidtas, genomföras, etc.

4.5 Säkerhetspolisen

Säkerhetspolisen (Säpo) har tagit fram en vägledning för säkerhetsanalys[62], som är ganska lik analysdelen av Försvarsmaktens modell. Säkerhetsanalysen består av tre steg:

1. Inventera skyddsvärda resurser
2. Identifiera hot mot det skyddsvärda[63]
3. Analysera risker och sårbarheter (utifrån sannolikhet och konsekvens)

Både sannolikhet och konsekvens bedöms på en fyrgradig skala, och risknivån blir sedan produkten av sannolikhet och konsekvens. Vägledningen poängterar också vikten av att dokumentation över vidtagna skyddsåtgärder måste finnas, samt att denna skall revideras efter genomförd riskanalys. När säkerhetsanalysen är genomförd skall ytterligare en punkt genomföras:

4. Upprätta handlings- och åtgärdsplan

I detta steg ska de risker som har framkommit bedömas, prioriteras och åtgärdas.

4.6 Vägverket

När Vägverket planerar och räknar på förbättringar av olika vägsträckor ska detta styras av att den samhällsekonomiska intäkten och nyttan överstiger den samhällsekonomiska kostnaden. De positiva och negativa effekterna värderas i monetära termer och den totala effekten eller nyttan jämförs sedan med kostnaden. Kalkylen kan därmed ligga till grund för en sammanfattande samhällsekonomisk bedömning av hur åtgärden påverkar samhället.[64]

[61] En översikt på processen finns på http://www.ab.lst.se/upload/dokument/raddning_och_sakerhet/RSA_processen.ppt
[62] Säpo (2005)
[63] Hoten bedöms utifrån *avsikt* (= intention i FM:s modell) och *förmåga* (= kapacitet + tillfälle i FM:s modell)
[64] VV (2008b)

I Vägverkets verksamhet är det ofta kostnaden för att förbättra eller bygga om en vägsträcka som ställs mot antalet liv som förbättringen eller ombyggnaden kan rädda per år. För att underlätta den typen av beslut genomför man olycksvärderingar. Värderingen består av två delar, en riskvärdering och en värdering av materiella kostnader. I riskvärderingen använder man sig av värdet på statistiskt liv (VSL), vilket är framräknat utifrån undersökningar om individers betalningsvilja för att minska risken att dö eller skadas i en trafikolycka.[65] De materiella kostnaderna beräknas utifrån kostnadsdata baserade på marknadspriser, och innefattar till exempel sjukvårdskostnader och kostnader för skadad egendom.[66] Om kostnaden för vägbygget dividerat med antalet liv man bedömer kunna rädda är lägre än det fastställda värdet från olycksvärderingen bör således vägbygget genomföras, annars inte. I Tabell 7 återfinns Vägverkets fastställda värde på statistiskt liv för de senaste 20 åren. De sista värdena i tabellen fastställdes i mitten av 2008 (2006 års prisnivå). Det totala olycksvärdet (riskvärdering + materiella kostnader) för ett dödsfall under 2008 är 22,3 miljoner kronor.

Tabell 7. Vägverkets värdering av statistiskt liv i prisnivå 1985-2006 (i miljoner kronor). Värdena (från 1999 och framåt) följer i huvudsak de rekommendationer som tagits fram inom det verksgemensamma samarbetet Arbetsgruppen för samhällsekonomiska kalkyl- och analysmetoder (ASEK).

	1985	**1990**	**1993**	**1997**	**1999**	**2001**	**2005**	**2006**
Dödsfall	3,7	6,5	11,0	13,0	13,0	16,3	17,1	21,0
Svårt skadad	0,40	0,70	1,8	2,0	2,0	2,5	2,6	3,5
Lindrig skada	0,015	0,030	0,045	0,090	0,090	0,11	0,12	0,13

Samhällsekonomiska analyser och kalkyler utgör en viktig del av det beslutsunderlag Vägverket tar fram inför planering och prioritering av åtgärder i vägtransportsystemet. Syftet med att tillämpa ett samhällsekonomiskt synsätt är att uppnå en effektiv medelsanvändning och möjliggöra en prioritering mellan olika åtgärder.

[65] VV (2006); Li & Lindberg (1999)
[66] VV (2008a)

5 Modelljämförelse

Försvarsmaktens modell som beskrivs i kapitel tre jämförs här med de civila myndigheters modeller som finns beskrivna i kapitel fyra. Jämförelsen, som ursprungligen gjordes på uppdrag av Försvarsmaktens generaldirektör, har huvudsakligen genomförts genom att identifiera de likheter och olikheter som finns i modellerna. Materialet som ligger till grund för jämförelsen är hämtat ur handböcker och vägledningar som de undersökta myndigheterna har publicerat samt deras hemsidor. De sju studerade myndigheterna är Försvarsmakten, Krisberedskapsmyndigheten, Räddningsverket, Kammarkollegiet, Länsstyrelsen i Stockholms län, Säkerhetspolisen och Vägverket. I Bilaga 2 återfinns en översiktlig grafisk jämförelse av några av de studerade myndigheternas modeller.

Alla studerade myndigheter har en modell som är avpassad främst för sin egen verksamhet eller verksamhetsområde. Trots detta är de allra flesta modellerna i grunden strukturellt sett lika (undantaget Vägverkets modell). Det som skiljer modellerna åt är framför allt hur detaljstyrande de är. I vissa fall har man valt att presentera flera olika användbara metoder och i andra fall finns bara en metod som är inarbetad i modellen; i vissa fall finns endast riktlinjer, medan det i andra fall finns en noggrann mall som skall följas. Försvarsmaktens modell är en väldigt konkret modell, liksom Länsstyrelsens, medan övriga mer är riktlinjer för hur riskanalys och/eller riskhantering kan genomföras. (Kammarkollegiet har dock ett antal formulär som kan användas i riskbedömningsarbetet.) Detta medför även att dessa två myndigheters modeller är mer detaljstyrande än övriga. Ingen av de två modellerna tar dock hänsyn till kostnaden för eventuella åtgärder och innefattar inte heller metoder för att väga kostnader mot till exempel risker. För detta kan Räddningsverkets handbok, Vägverkets metod, eller annat material inom beslutsteori, komma väl till pass för att utveckla modellerna ytterligare.

Fördelen med de mer styrande modellerna är att de kan vara lättare att förstå och använda. Vägledningar och handböcker lämnar mycket arbete åt riskhanteraren i form av metodutveckling innan arbetet kan sättas igång. Detta arbete är redan gjort åt riskhanteraren i de mer styrda modellerna. Vad gäller Länsstyrelsens metod och verktyg kräver den eventuellt något mer arbete att sätta sig in i och förstå än Försvarsmaktens, men å andra sidan låter man ett datorverktyg göra en del av jobbet. Ett datorverktyg kan dock även minska riskhanterarnas förståelse och förtroende för modellen, då det inte alltid är självklart hur de inmatade uppgifterna hänger ihop med det resultat verktyget sedan presenterar.

En annan större skillnad mellan modellerna är huruvida en sårbarhetsbedömning genomförs och när i processen den görs. I Försvarsmaktens modell ligger sårbarhetsbedömningen till grund för riskbedömningen, medan den i till exempel

Krisberedskapsmyndighetens modell genomförs efter det att själva riskanalysen är slutförd (det vill säga att riskanalysen istället ligger till grund för sårbarhetsanalysen). I Kammarkollegiets modell görs överhuvudtaget ingen bedömning av sårbarheter.

Ur ett ”försvarsmaktsperspektiv” är flera av modellerna också mindre relevanta då de inte gör skillnad på hot och risk, vilket är nödvändigt inom mycket av Försvarsmaktens verksamhet. Detta märks kanske ännu tydligare i och med att förutom Försvarsmaktens modell, är Säkerhetspolisens modell den enda av de studerade modellerna som också gör denna åtskillnad. Båda dessa två myndigheter har verksamhet som riktar sig framför allt mot aktörsdrivna hot. Krisberedskapsmyndighetens handledning definierar de två begreppen separat, men gör sedan ingen skillnad på dem i modellen.

Vägverkets modell som är beskriven i denna rapport behandlar inte själva riskanalysen utan är ett hjälpmedel för att avgöra vilka risker, eller i Vägverkets fall åtgärder, som bör prioriteras. Vägverkets metod är intressant ur perspektivet att den är ett hjälpmedel för att prioritera åtgärder och för att väga kostnader mot människoliv. Även i till exempel Försvarsmaktens verksamhet (speciellt i internationella insatser) krävs sådana avvägningar, men i dagsläget finns ingen metod för detta i riskhanteringsarbetet. Om Försvarsmakten skulle vilja använda en metod som denna kan man dock vara tvungen att genomföra egna studier för att räkna fram värden på det statistiska livet, då värdena som Vägverket använder är avpassade för trafikolyckor. Inom Räddningsverket pågår exempelvis ett projekt där man bland annat undersöker huruvida värdena för statistiska liv beräknade för trafikolyckor verkligen är tillämpbara på brand eller andra typer av olyckor.[67]

Sammanfattningsvis är styrkan med Försvarsmaktens modell att den är lätt att förstå och väl anpassad för den verksamhet den främst är framtagen för (det vill säga internationella insatser). Genom att metodiskt genomgå de olika stegen i modellen, med rätt kompetens i den grupp som genomför arbetet, säkerställs att riskhanteringen gjorts efter bästa möjliga förutsättningar. Den ger samsyn inom organisationen på vilka risker som föreligger inom olika områden vilket underlättar kommunikationen mellan de olika nivåerna och funktionerna. Alla beslut dokumenteras även skriftligt, vilket tvingar beslutsfattaren till ett i högre grad medvetet beslut och en mer aktiv roll i riskhanteringsprocessen. Modellen lägger dock mycket stort ansvar på beslutsfattaren då metoden endast genererar förslag på riskhämmande åtgärder, men ingen metod för att prioritera dem sinsemellan (till exempel i förhållande till kostnad som i Vägverkets modell).

[67] Jaldell et al. (2006); SRV (2008)

Referenser

Litteratur

Abrahamsson, M. & Magnusson, S-E (2004). *Risk- och sårbarhetsanalyser. Utgångspunkter för fortsatt arbete*. KBM:s forskningsserie nr 2, Krisberedskapsmyndigheten, Stockholm.

AIRMIC, ALARM & IRM (2002). *A Risk Management Standard.*

Aven, T. (2003). *Foundations of risk analysis - A knowledge and decision-oriented perspective*. John Wiley & Sons.

FERMA (2003). *Standard för risk management.*

FM (2007). *Försvarsmaktens gemensamma riskhanteringsmodell*. Metodanvisning, remissutgåva 2. Försvarsmakten, 01 310:71155.

Glover, J. (1990). *Causing death and saving lives*. Penguin.

Grimvall, G. *et al*. (2003). *Risker i tekniska system*. Studentlitteratur, Lund.

Grimvall, G. & Lindgren, O. (1995). *Risker och riskbedömningar*. Studentlitteratur, Lund.

Gunnarsson, S. O. (1995). Vägtrafiken – ett människa-maskin-miljö-system med stora riskvariationer. *Ur* Grimvall & Lindgren (1995).

H Säk Hot (2006). *Handbok för Försvarsmaktens säkerhetstjänst – Hotbedömning*. Försvarsmakten, M7745-734022.

H Säk Skydd (2007). *Handbok för Försvarsmaktens säkerhetstjänst – Säkerhetsskyddstjänst.* Försvarsmakten, M7739-352005.

Hansson, S. O. (2000). Seven Myths of Risk. Tal vid konferensen *"Stockholm thirty years on. Progress achieved and challenges ahead in international environmental co-operation*". Miljödepartementet, 17-18 juni, 2000.

Hansson, S. O. (2002). Philosophical Perspectives on Risk. Inledningstal vid konferensen "*Research in Ethics and Engineering"*, Delft Tekniska Universitet, 25 april, 2002.

Hayzelden, J.E. (1968). The value of a human life. *Public Administration* 46, 1968, 427-441.

Holmgren, Å. (2006). *Quantitative vulnerability analysis of electric power networks*. Doktorsavhandling, Institutionen för transporter och samhällsekonomi, KTH. TRITA-TEC-PHD 06-001

Holmgren, Å. & Thedéen, T. (2003). Riskanalys. *Ur* Grimvall, *et al.* (2003).

Hultkrantz, L. & Svensson, M. (2008). Värdet av liv. *Ekonomisk debatt*, årg 35:2, 5-16.

Jaldell, H. *et al.* (2006). *Att värdera och jämföra risker. Allmänhetens och beslutsfattares preferenser 2006-2008*. Bildspel från Räddningsverkets forskardagar 2006.

KBM (2006a) *Hot- och riskrapport 2006*. KBM:s temaserie 2006:7. Krisberedskapsmyndigheten, Stockholm.

KBM (2006b). *Risk- och sårbarhetsanalyser – Vägledning för statliga myndigheter*. KBM rekommenderar 2006:4, Krisberedskapsmyndigheten, Stockholm.

KBM (2007). *Krishantering för kommuner och landsting*. Utbildningspaket, Krisberedskapsmyndigheten, Stockholm.

Kågebro, E. & Vredin Johansson, M. (2008). *Ekonomiska verktyg som beslutsstöd i klimatanpassningsarbetet*. Avdelningen för Försvarsanalys, FOI. FOI-R--2530--SE

Li, C-Z. & Lindberg, G. (1999). *Värdet på ett statistiskt liv i Vägverkets planering*. Underlag. Rapport 1999:6. Statens institut för kommunikationsanalys (SIKA).

Lindahl, H. (2001). *Samhällsekonomisk kostnadsanalys av vägbyggen*. Avdelningen för Nationalekonomi, Institutionen för Industriell ekonomi och samhällsvetenskap, LTU. LTH-SHU-EX--01/093--SE

Marinos, L. (2005). *Risk Management at ENISA. A road map – from objectives to achieve practical results.* European Network and Information Security Agency.

Mattson, B. (2006). *Kostnads-nyttoanalys för nybörjare*. Räddningsverket, Karlstad.

Mossberg, K. *et al.* (2007). *Anpassning tillklimatförändringar i risk- och sårbarhetsanalyser på kommunal nivå – underlag för fortsatt arbete.* Underlagsrapport. Avdelningen för Försvarsanalys, FOI. FOI-R--2412--SE

Möller, G. (1986). *Risker och människolivets värde.* Almqvist & Wiksell International, Stockholm.

Nato (2007a). *NATO Logistics Handbook.* North Atlantic Treaty Organisation.

Nato (2007b). *NATO Glossary of terms and definitions* (AAP-6). Nato Standardisation Agency, North Atlantic Treaty Organisation.

Näsman, P. (2005). *Risk Analysis – A Tool in Decision-making*. Gruppen för säkerhetsforskning, Institutionen för transporter och samhällsekonomi, KTH. TRITA-INFRA 05-022.

SRV (2003). *Handbok för riskanalys*. Räddningsverket, Karlstad.

Svensson, M. (2007). *What is a Life Worth? Methodological Issues in Estimating the Value of a Statistical Life*. Örebro Studies in Economics 14. Örebro universitet.

Säpo (2005). *En vägledning till säkerhetsanalys*. Råd och anvisningar 2005. Säkerhetspolisen.

Thedéen, T. (1995). Risk och beslut – begrepp, modeller och metoder. *Ur* Grimvall & Lindgren (1995).

VV (2006). *Vägverkets samhällsekonomiska kalkylvärden*. Publikation 2006:127. Vägverket, Borlänge.

VV (2008a). *Målstyrning av trafiksäkerhetsarbetet. Aktörssamverkan mot nya etappmål år 2020*. Publikation 2008:31. Vägverket, Borlänge.

VV (2008b). *Vägverkets samhällsekonomiska kalkylvärden*. Publikation 2008:67. Vägverket, Borlänge.

Wennersten, R. (2003). Industriell riskhantering. *Ur* Grimvall *et al*. (2003).

Internetkällor

ENISA (2007). *http://www.enisa.europa.eu/rmra* (2007-08-10)

Kammarkollegiet (2008). *http://www.kammarkollegiet.se/risk/risk.html* (2008-05-25)

Länsstyrelsen Sthlm (2008). *http://www.ab.lst.se* (2008-05-25)
Sökväg: Samhällsskydd – Risk- och sårbarhetsanalyser i Stockholms län

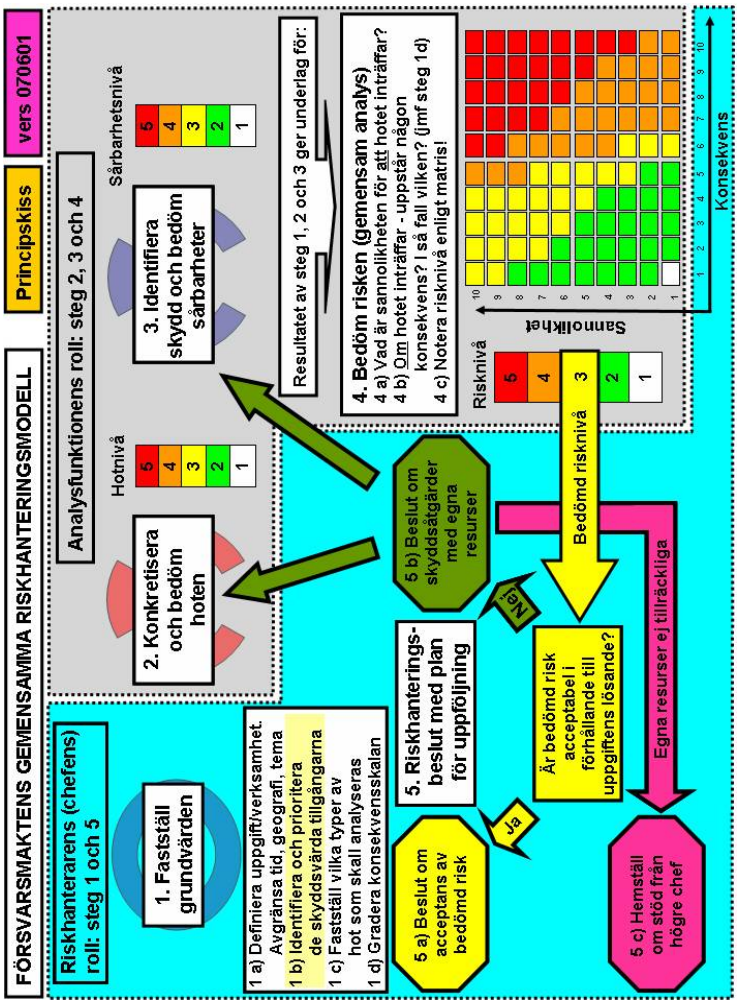
SRV (2008). *http://www.srv.se* (2008-07-16)
Sökväg: Om verket – Forskning – Forskardagar – Forskardagar 2006

Wennersten, R. (2004). *Vad är riskanalys?*. Föreläsningsanteckningar i kurs 3C1383, KTH. (2008-05-05)
http://www.ima.kth.se/im/3C1383/3C4365/PDF/Vad%20är%20riskanalys.pdf

Bilaga 1: Komplement till Försvarsmaktens modell

Modellskiss

Bilden nedan är en principskiss över riskhanteringsprocessen för säkerhetshot. En mer generell skiss finns även för riskhantering i allmänhet (se bilden på framsidan av rapporten). Nedanstående skiss är dock mer detaljerad och åskådliggör tydligare den metod som beskrivits i denna rapport.



Skalor

Hot- och sårbarhetsnivåer

Beskrivningarna för hot- och sårbarhetsnivåerna är endast riktlinjer för bedömning.

Hotnivå		Beskrivning
5	Mycket högt hot	Incidenter inträffar mer eller mindre dagligen. Aktören bedöms försöka genomföra verksamheten till varje pris utan hänsyn till konsekvenser för den egna säkerheten. Ogynnsamma miljö- och/eller sociala faktorer finns och har mycket stor och uppdragshotande inverkan.
4	Högt hot	Information som tyder på hög kapacitet, intention och tillfälle hos potentiell aktör. Incidenter har inträffat vid ett flertal tillfällen i närtid. Ogynnsamma miljö- och/eller sociala faktorer finns och har stor och möjligen uppdragshotande inverkan.
3	Förhöjt hot	Information som tyder på reell kapacitet, intention och tillfälle hos potentiell aktör. Enstaka incidenter har inträffat. Ogynnsamma miljö- och/eller sociala faktorer finns och har stor, men inte uppdragshotande, inverkan.
2	Lågt hot	Information som tyder på begränsad kapacitet, intention och tillfälle hos potentiell aktör. Inga incidenter har förekommit i närtid. Ogynnsamma miljö- och/eller sociala faktorer finns men har låg inverkan.
1	Inget identifierat hot	Ingen information som tyder på kapacitet, intention och tillfälle hos en potentiell aktör. Inga incidenter har förekommit i närtid. Ogynnsamma miljö- och/eller sociala faktorer saknas.

Sårbarhetsnivå		Beskrivning
5	Mycket hög risk	Inga eller endast enstaka skyddsåtgärder är vidtagna. Tillgång till eller påverkan på den skyddsvärda tillgången är mycket lätt att åstadkomma.
4	Hög risk	Skyddsåtgärder existerar, men ett flertal sårbarheter möjliggör tillgång till eller påverkan på den skyddsvärda tillgången.
3	Förhöjd risk	Effektiva skyddsåtgärder är implementerade, men enstaka sårbarheter förekommer vilka kan utnyttjas för tillgång till eller påverkan på den skyddsvärda tillgången.
2	Låg risk	Effektiva och av varandra oberoende skyddsåtgärder är implementerade. Tillgång till eller påverkan på den skyddsvärda tillgången är mycket svår att åstadkomma.
1	Ingen synbar risk	Flera effektiv och av varandra oberoende skyddsåtgärder är implementerade. Inga kända sårbarheter är identifierade.

Sannolikhetsskala och konsekvensskala

Sannolikhetsskalan är statisk, medan konsekvensskalan definieras för varje område som riskhanteras. Nedanstående beskrivning är endast ett exempel på hur en konsekvensskala kan utformas.

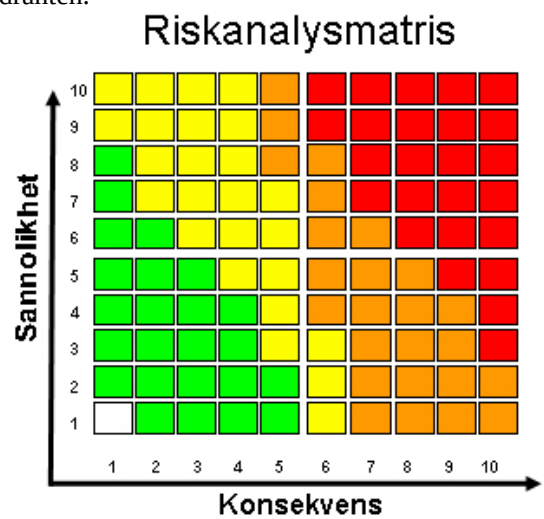
Sannolikhetsskala		
Sannolik	> 50 %	9-10
Trolig	< 50 %	7-8
Möjlig	< 25 %	5-6
Mindre trolig	< 5 %	3-4
Osannolik	< 1 %	1-2

Konsekvensskala		**Beskrivning** (exempel)
9-10	Synnerligen allvarlig	Ett stort antal döda (>10) och många allvarligt skadade.
7-8	Allvarlig	Flera döda (<10) och flera allvarligt skadade.
5-6	Kännbar	Skada som kräver kvalificerad sjukvård (ROLE 3). Permanenta fysiska men, och dödsfall, kan förekomma.
3-4	Lindrig	Skada som kräver läkarvård (ROLE 1-2). Eventuellt kortare konvalescens, men inga permanenta fysiska men.
1-2	Försumbar	Skada som kräver enklare vård (egenvård, sjuksköterska).

Risknivåer och riskmatris

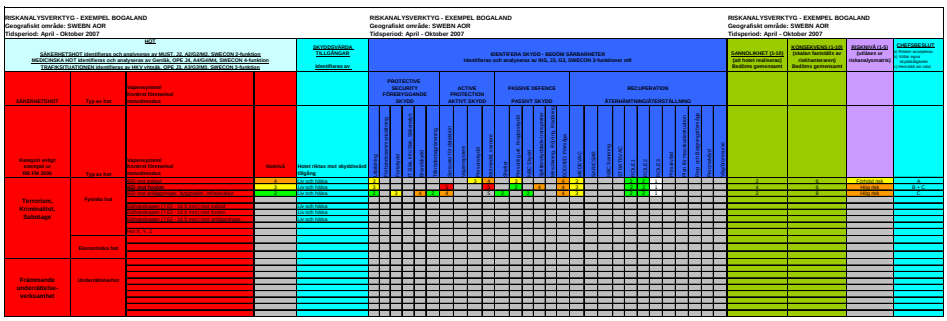
Risknivån beräknas ur sannolikheten för att en viss händelse inträffar och konsekvenserna av den samma. Riskanalysmatrisen är som synes inte symmetrisk, utan konsekvensen väger tyngre än sannolikheten eftersom en allvarlig konsekvens har bedömts ha större betydelse än en hög sannolikhet. Man kan till exempel se att den övre vänstra kvadranten i riskanalysmatrisen har lägre risknivåer än den nedre högra kvadranten.

Risknivåskala	
5	Mycket hög risk
4	Hög risk
3	Förhöjd risk
2	Låg risk
1	Ingen synbar risk



Verktyget

Verktyget används som hjälpmedel i riskhanteringsprocessen. I den röda delen återfinns hotkatalogen, den första cyan-färgade delen anger skyddsvärd tillgång och den blå delen avser skydd. Den gröna delen används för sannolikhets- och konsekvensbedömningarna och i den lila kolumnen anges risknivån. I den sista cyan-färgade kolumnen anges vilken form av chefsbeslut som ska tas. I de grå delarna anges hot-, sårbarhets- och risknivåerna. Detta görs med de färg- och nivånummerbeteckningar som respektive skala använder.



Nedan följer uppförstoringar av de olika delarna av verktyget.

Geografiskt område: SWEBN AOR
Tidsperiod: April - Oktober 2007

HOT SÄKERHETSHOT identifieras och analyseras av MUST, J2, A2/G2/M2, SWECON 2-funktion MEDICINSKA HOT identifieras och analyseras av Genläk, OPE J4, A4/G4/M4, SWECON 4-funktion TRAFIKSITUATIONEN identifieras av HKV vhtsäk, OPE J3, A3/G3/M3, SWECON 3-funktion				SKYDDSVÄRDA TILLGÅNGAR Identifieras av
SÄKERHETSHOT	Typ av hot	Vapensystem/ Konkret företeelse/ metod/modus		
Kategori enligt exempel ur RB FM 2006	Typ av hot	Vapensystem/ Konkret företeelse/ metod/modus	Hotnivå	Hotet riktas mot skyddsvärd tillgång
Terrorism, Kriminalitet, Sabotage	Fysiska hot	IED mot individ	4	Liv och hälsa
		IED mot fordon	3	Liv och hälsa
		IED mot anläggningar, byggnader, infrastruktur	2	Liv och hälsa
		Eldhandvapen (7.62 - 14.5 mm) mot individ		Liv och hälsa
		Eldhandvapen (7.62 - 14.5 mm) mot fordon		Liv och hälsa
		Eldhandvapen (7.62 - 14.5 mm) mot anläggningar…		Liv och hälsa
		Hot X, Y, Z		
	Ekonomiska hot			
Främmande underrättelse-verksamhet	Underrättelsehot			

RISKANALYSVERKTYG - EXEMPEL BOGALAND
Geografiskt område: SWEBN AOR
Tidsperiod: April - Oktober 2007

IDENTIFERA SKYDD - BEDÖM SÅRBARHETER
Identifieras och analyseras av INS, J3, G3, SWECON 3-funktioner mfl

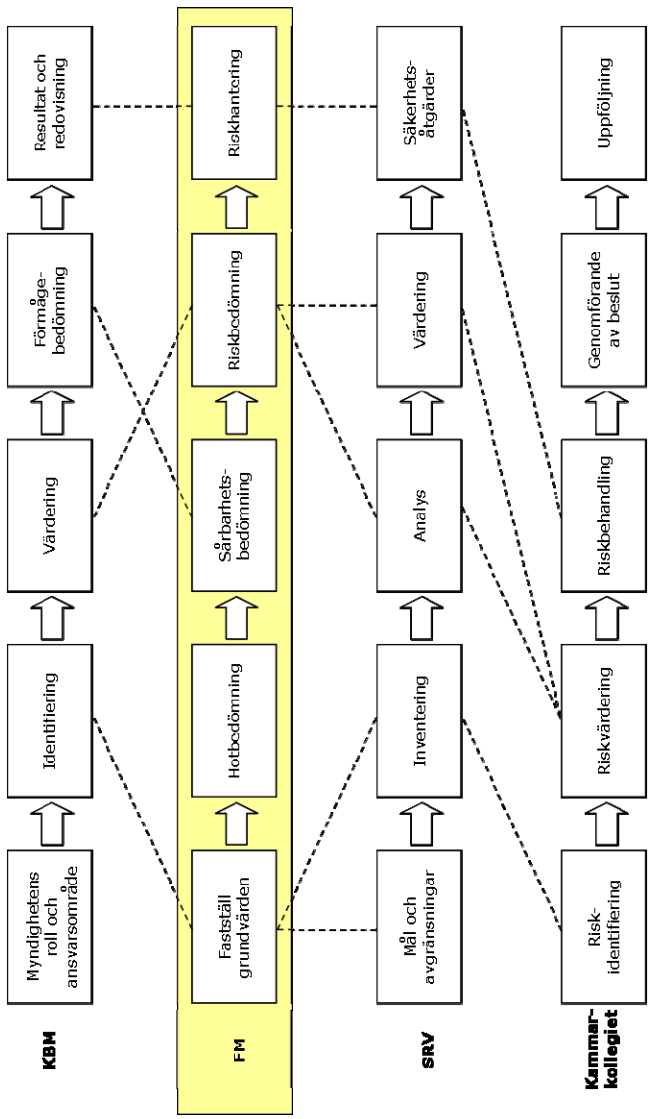
PROTECTIVE SECURITY FÖREBYGGANDE SKYDD						ACTIVE PROTECTION AKTIVT SKYDD				PASSIVE DEFENCE PASSIVT SKYDD						RECUPERATION ÅTERHÄMTNING/ÅTERSTÄLLNING										
Utbildning	Förbandssammansättning	Fortskydd	IT-Säk, Info Säk, Säkanalys	Brandskydd	Tillträdesbegränsning	Sensorer för detektion	Vapensystem	Personskydd	Motmedel, varnare	Shelter	Personlig utr, Kroppsskydd	NBC Skydd	Splitterskyddade transporter	Minsökning, Röjning, Räddning	EOD/IED Förmåga	MEDEVAC	SAR/CSAR	NBC Sanering	STRATEVAC	ROLE 1	ROLE 2	ROLE 3	Primärvård	Plan för masskadesituation	Rep- och Bärgningsförmåga	Personalvård	Vägtrafiksäkerhet
3								3	4		3				4	3				2	2	1					
3						5			5		2		4		4	3				2	2	1					
2		3		4	2	4			5	2		2			4	3				2	2	1					

RISKANALYSVERKTYG - EXEMPEL BOGALAND
Geografiskt område: SWEBN AOR
Tidsperiod: April - Oktober 2007

SANNOLIKHET (1-10) (att hotet realiseras) Bedöms gemensamt	**KONSEKVENS (1-10)** (skalan fastställs av riskhanteraren) Bedöms gemensamt	**RISKNIVÅ (1-5)** (utläses ur riskanalysmatris)	**CHEFSBESLUT** a) Risken accepteras b) Vidtar egna skyddsåtgärder c) Hemställ om stöd
2	6	Förhöjd risk	A
4	6	Hög risk	B + C
2	8	Hög risk	C

Bilaga 2: Grafisk jämförelse

En grafisk jämförelse av några av de undersökta modellerna. Säkerhetspolisens modell är på en övergripande nivå så lik Försvarsmaktens modell att den ej togs med här. Vägverkets studerade metod innefattar inte själva risk- och sårbarhetsanalysen och finns därför inte heller med i figuren. De streckade linjerna ska inte ses som kopplingar mellan olika steg utan symboliserar samhörigheten mellan respektive steg i respektive modell.



Bilaga 3: Ordlistor

Akronymer

AIRMIC	The Association of Insurance and Risk Managers
ALARM	The National Forum for Risk Management in the Public Sector
ASEK	Arbetsgruppen för samhällsekonomiska kalkyl- och analysmetoder
ENISA	European Network and Information Security Agency
FERMA	Federation of European Risk Management Associations
FM	Försvarsmakten
FOI	Totalförsvarets forskningsinstitut
G2	Underrättelsefunktionen på armétaktisk nivå
IBERO	Instrument för beredskapsvärdering av områdesansvar
IED	Improvised explosive device
IRM	The Institute of Risk Management
ISAF	International Security Assistance Force. Det internationella militära samarbetet i Afghanistan.
J2	Underrättelsefunktionen på operativ nivå
J3	Genomförandefunktionen på operativ nivå
KBM	Krisberedskapsmyndigheten
KFOR	The Kosovo Force. Det internationella militära samarbetet i Kosovo.
LUCRAM	Lunds Universitets centrum för riskanalys och risk management
M3	Planeringsfunktionen på marintaktisk nivå
MEDEVAC	Medical evacuation
MUST	Militära underrättelse- och säkerhetstjänsten
NBG	Nordic Battle Group
PSYOPS	Psychological operations

RPS	Rikspolisstyrelsen
RSA	Risk- och sårbarhetsanalys
SIKA	Statens institut för kommunikationsanalys
SRV	Statens räddningsverk
STRATEVAC	Strategic air transport evacuation
SWECON	Swedish contingent / svenska kontingenten
Säpo	Säkerhetspolisen
ÖB	(Försvarsmaktens) Överbefälhavare

Ordförklaring

Förklaring till ord som förekommer i rapporten. Definitionerna är hämtade från standarder (ISO/IEC Guide 73, ISO/IEC 13335-1) samt organisationer (ENISA, Nato) och myndigheter (CIAO[68], Försvarsmakten, KBM och Vägverket). I de fall där förklaringen är specifik för en viss verksamhet är detta angivet.

Term	Förklaring
Acceptabel risk	Nivån på den kvarvarande risken som har beslutats vara en resonabel nivå för potentiella förluster/skador. (CIAO/ENISA, 2007)
Aktörsdrivet hot	En mänsklig aktörs möjligheter att medvetet förorsaka en oönskad händelse med negativa konsekvenser. (FM, 2007)
Dödad individ	*Vägverket*: Person som avlider inom 30 dagar till följd av en trafikolycka. (VV, 2008b)
Force Protection	Alla åtgärder och medel för att minimera sårbarheten hos personal, lokaler, utrustning och operationer till varje hot och i alla situationer, för att bibehålla handlingsfrihet och styrkans operativa effektivitet. (Nato, 2007b)
Hot	Alla omständigheter eller händelser med potential att orsaka fientlig påverkan på en tillgång. (ENISA, 2007)
	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten. (ISO/IEC 13335-1)
Icke aktörsdrivet hot	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten, vilken ej är förorsakad av en mänsklig aktörs avsiktliga gärningar. (FM, 2007)
Konsekvens	Utfallet av en (negativ) händelse. (ISO/IEC Guide 73)
Krishantering	Att hantera konsekvenserna av en allvarlig störning i sådan verksamhet som alltid måste upprätthållas. (KBM, 2007)
Kvarvarande risk	Risk som återstår efter förebyggande åtgärder. (ISO/IEC Guide 73)

[68] Critical Infrastructure Assurance Office, USA

Lindrigt skadad individ	*Vägverket*: Person med personskada, till följd av trafikolycka, som inte innefattas i ”svårt skadad”. (VV, 2008b)
Materiella kostnader	*Vägverket*: Sjukvårdskostnader, administrativa kostnader, egendomsskadekostnader och nettoproduktionsbortfall som uppstår då en person dödas eller skadas i trafiken. (VV, 2008b)
Olycksvärdering	Riskvärdering + materiella kostnader. (VV, 2008b)
Risk	Potentialen att ett givet hot kommer exploatera sårbarheterna hos en tillgång och därmed orsaka skada på organisationen. (ISO/IEC PDTR 13335-1)
	Produkten av sannolikheten för att ett givet hot realiseras och därmed uppkommande skadekostnad. (ISO/IEC Guide 73).
Riskanalys	Systematisk användning av information och/eller kunskap för att identifiera källor och uppskatta risken. (ISO/IEC Guide 73)
	Process som identifierar säkerhetsrisker och bestämmer deras betydelse (ISO/IEC Guide 73).
Riskbedömning	Processen bestående av riskidentifiering, riskanalys och riskvärdering. (ENISA, 2007)
Riskhantering	Samordnade aktiviteter för att styra och kontrollera en organisation med avseende på risk. (ISO/IEC Guide 73)
Riskidentifiering	Processen att hitta, lista och karaktärisera riskelement. (ISO/IEC Guide 73)
Risknivå	*Försvarsmakten*: Mått på hur stor risken är, på en femgradig skala där 1 = ingen synbar risk och 5 = mycket hög risk. (FM, 2007)
Riskreducering	Handlingar gjorda för att minska sannolikheten, de negativa konsekvenserna eller både sannolikhet och konsekvens, associerad med en risk. (ISO/IEC Guide 73)
Riskskattning	Processen för att bestämma sannolikheten och konsekvensen av en risk. (ISO/IEC Guide 73)
Riskvärdering	*Allmänt*: Processen då den uppskattade risken jämförs

med givna riskkriterier. (ISO/IEC Guide 73)

Vägverket: Individens betalningsvilja för att minska sin risk att dödas eller skadas i trafiken. (VV, 2008b)

Role (1-4)

Används för att beskriva de fyra nivåer som medicinskt stöd är indelat i, i operativ verksamhet. En ”roll” definieras på grundval av kompetens och resurser, och är inte specifik för särskilda medicintyper. En övergripande operativ medicinsk struktur har normalt inslag av alla fyra rollerna.

Role 1. Medicinskt stöd ges för rutinmässig primärvård, specialiserad första hjälpen, behovsprövad prioritering, återupplivning och stabilisering. Role 1 är ett nationellt ansvar och är integrerad i eller tilldelad till en mindre enhet.

Role 2 utgör en mellanliggande kapacitet för mottagande och behovsprövad prioritering av skadade samt kan utföra återupplivning och behandling av chock på en högre teknisk nivå än Role 1. Kan även innehålla viss intensivvård (damage control surgery), akut tandvård, psykiatri, m m. Role 2 är ett nationellt eller ledande nations ansvar, vanligtvis allokerad vid en brigad eller större enheter.

Role 3 är utformat för att ge sekundär vård inom de restriktioner som finns för evakuering från insatsområde. Medicinskt stöd i nivå 3 ges vid fältsjukhus och de delar som behövs för att stödja ett sådant. I detta ingår missionsspecifika förmågor inklusive primär kirurgi och diagnostiskt stöd. Role 3 är ett nationellt eller ledande nations ansvar, kan vara multinationellt, och erbjuder medicinskt stöd på divisionsnivå eller högre.

Role 4 tillhandahåller hela skalan av definitiv medicinsk vård som inte kan utföras i insatsområdet eller är för tidskrävande för att utföras där. Det tillhandahålls normalt i hemlandet eller i en allierads hemland. I många Nato-länder ges Role 4 inom den nationella civila sjukvården. (Nato, 2007a)

Sannolikhet	Grad av vilken en händelse är trolig att inträffa. (ENISA, 2007)
Skyddsåtgärd	Handling, procedur eller tekniskt arrangemang som, genom att minska sårbarheten möter identifierat hot. (ISO/IEC 13335-1)
Statistiskt liv	Befolkningens vilja att betala för en i något avseende ökad säkerhet. (VV, 2008b)
Svårt skadad individ	*Vägverket*: Person som till följd av en trafikolycka erhållit brott, krosskada, sönderslitning, allvarlig skärskada, hjärnskakning eller inre skada. Dessutom räknas som svår personskada annan skada som väntas medföra intagning på sjukhus. (VV, 2008b)
Sårbarhet	Brist i skyddet av en tillgång exponerad för hot. (ISO/IEC 13335-1)
Tillgång	Allt som är av värde för organisationen (ISO/IEC 13335-1)