KBM:S FORSKNINGSSERIE | NR 2

Marcus Abrahamsson
Sven Erik Magnusson

Risk- och sårbarhetsanalyser

UTGÅNGSPUNKTER FÖR FORTSATT ARBETE

KRISBEREDSKAPS MYNDIGHETEN

KBM:S FORSKNINGSSERIE | NR 2

Risk- och sårbarhetsanalyser

UTGÅNGSPUNKTER FÖR FORTSATT ARBETE

Marcus Abrahamsson och
Sven Erik Magnusson

KBM:S FORSKNINGSSERIE

NR 1 Är den inre säkerheten hållbar?

NR 2 Risk- och sårbarhetsanalyser
Utgångspunkter för fortsatt arbete

Titel: Risk- och sårbarhetsanalyser. Utgångspunkter för fortsatt arbete
Utgiven av Krisberedskapsmyndigheten (KBM)
Upplaga: 1 000 ex

ISSN: 1652-3717
ISBN: 91-85053-20-1
KBM:s dnr: 1090/2003
Grafisk form: AB Typoform
Tryck: Edita Ljunglöfs, Stockholm, mars 2004

Skriften kan erhållas kostnadsfritt från Krisberedskapsmyndigheten
E-post: bestallning@krisberedskapsmyndigheten.se

Skriften kan laddas ned från Krisberedskapsmyndighetens webbplats
www.krisberedskapsmyndigheten.se

KBM:S FORSKNINGSSERIE NR 2

Innehåll

Förord

Vi lever i dag i ett samhälle där många verksamheter är beroende av varandra för att kunna fungera. Samhällspusslet är stort och komplext, och avsaknaden av en pusselbit innebär att bilden blir ofullständig. För att förbättra samhällets samlade förmåga att förhindra eller minska effekterna av en kris är en av förutsättningarna att kunna avgöra vilka riskerna är, liksom var i samhället sårbarheterna finns.

En av KBM:s uppgifter är att skapa en samlad helhetsbild av de sårbarheter som finns i samhället. Ett underlag är de risk- och sårbarhetsanalyser som myndigheterna sedan två år genomför och lämnar till regeringskansliet. Ytterligare underlag ges bland annat av de sammanställningar och övergripande bedömningar KBM gör av myndigheternas analyser, av de samverkansansvariga myndigheternas egna bedömningar av förmågor och resultaten av de fördjupade genomgångarna.

För att kunna skapa en helhetsbild krävs det en fortsatt utveckling av innehållet i och utformningen av rapporteringen om myndigheternas risk- och sårbarhetsanalyser. Vidare krävs en utvecklad arbetsprocess för de efterföljande åtgärder som de samverkansansvariga myndigheterna vidtar baserade på resultaten av analyserna och de utvecklingsbehov m.m som myndigheterna själva identifierat. Denna forskarrapport utgör tillsammans med de risk- och sårbarhetsanalyser som myndigheterna lämnade i februari 2004, erfarenheterna från arbetsprocessen och KBM:s övergripande analyser en utgångspunkt för det fortsatta utvecklingsarbetet.

Rapporten är skriven av Marcus Abrahamsson och Sven Erik Magnusson, som är forskare vid Lunds universitets centrum för riskanalys och riskhantering (LUCRAM). Författarna påpekar att krishanteringen är en viktig och integrerad delmängd av riskhanteringen. De anser att det är svårt att beskriva risk- och sårbarhetsanalysens roll i krishanteringen utan att ta hänsyn till myndighetens riskhantering generellt. I andra

skrifter framställs risk- och sårbarhetsanalyser som en del i krishanteringen utan att myndighetens riskhantering nämns. Under KBM:s fortsatta utvecklingsarbete med risk- och sårbarhetsanalyser ska dessa olika synsätt behandlas. I rapporten nämns ledningssystemens betydelse vid riskhantering, vilket också utgör en viktig del av utvecklingsarbetet.

Författarna svarar för innehållet i rapporten.

Ingrid Pettersson
Forskningssamordnare
Krisberedskapsmyndigheten

Del I. Bakgrundsmaterial

1. Bakgrund

I regeringens proposition 2001/02:158 *Samhällets säkerhet och beredskap* (s 38) föreslås att

"Varje statlig myndighet bör för att stärka sin krishanteringsförmåga ha till uppgift att genomföra en analys av den sårbarhet eller de risker som kan finnas inom myndighetens ansvarsområde och som mycket allvarligt kan nedsätta förmågan hos verksamheten inom området (sårbarhetsanalys). Den bör årligen uppdateras och redovisas till Regeringskansliet. Sårbarhetsanalysen skall avse sådana tillstånd som kan uppstå när en eller flera händelser utvecklar sig eller trappas upp till att omfatta flera delar av samhället. Tillståndet skall vara av en sådan omfattning att det uppstår allvarliga störningar i viktiga samhällsfunktioner och kräver att insatser från flera olika myndigheter och organ samordnas för att kunna hantera situationen och därmed begränsa konsekvenserna."

Propositionen resulterade så småningom i förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap vars 3 § och 4 § innebar en viss konkretisering av ordalagen i propositionen. Enligt nämnda förordning skall statliga myndigheter årligen analysera om det finns sådan sårbarhet och sådana risker inom myndigheternas respektive ansvarsområden som synnerligen allvarligt kan försämra förmågan till verksamhet inom området, se citat 3 § nedan:

"Risk- och sårbarhetsanalys

3 § *Varje myndighet skall i syfte att stärka sin krishanteringsförmåga årligen analysera om det finns sådan sårbarhet och sådana risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området. Vid denna analys skall myndigheten särskilt beakta*

1. *situationer som uppstår hastigt, oväntat och utan förvarning,*
2. *situationer som kräver brådskande beslut och samverkan med andra samhällsorgan,*
3. *situationer som allvarligt påverkar samhällets funktionsförmåga eller tillgång på nödvändiga resurser, och*

4. *förmågan att hantera mycket allvarliga situationer inom myndighetens ansvarsområde.*

Myndigheten skall värdera och sammanställa resultatet av arbetet i en risk- och sårbarhetsanalys. Analysen skall lämnas till Regeringskansliet vid samma tidpunkt som gäller för inlämnande av årsredovisningen."

Utöver detta har ett antal myndigheter utpekats med särskilt ansvar för fredstida krishantering och ålagts att planera och vidta förberedelser för att förebygga, motverka och begränsa identifierade sårbarheter inom sex angivna samverkansområden. Dessa myndigheter har ett särskilt ansvar för att samverka med varandra samt med länsstyrelserna, övriga statliga myndigheter, kommuner, landsting, sammanslutningar och näringsidkare som är berörda, se citat 4 § nedan:

"Särskilt ansvar för fredstida krishantering

4 § Myndigheterna som anges i bilagan till denna förordning skall planera och vidta förberedelser för att förebygga, motverka och begränsa identifierad sårbarhet och risker inom de samverkansområden som anges i bilagan. Myndigheterna skall därvid särskilt

1. *samverka med länsstyrelserna i deras roll som områdesansvarig myndighet,*
2. *samverka med övriga statliga myndigheter, kommuner, landsting, sammanslutningar och näringsidkare som är berörda,*
3. *beakta behovet av forsknings- och utvecklingsinsatser och annan kunskapsinhämtning, och*
4. *beakta säkerhetskraven för de tekniska system som är nödvändiga för att de skall kunna utföra sitt arbete."*

Enligt författarnas synsätt kan formuleringen *planera och vidta förberedelser för att förebygga, motverka och begränsa identifierad sårbarhet och risker* ovan anses vara en beskrivning av begreppet riskhantering, d.v.s. författarna anser att de aktuella myndigheterna, för att kunna uppfylla intentionen i förordningen, måste ha en väl utvecklad organisation för riskhantering avseende risker med potential att vara åtminstone en bidragande orsak till att en svår påfrestning uppkommer. För ett klargörande av skillnaden mellan krishantering och generell riskhantering, se kommentaren till figur 4.2. Vad detta kan innebära utvecklas vidare i senare delar av denna rapport.

2. Rapportens målsättning, förutsättningar och begränsningar

Denna rapport är avsedd att redovisa möjliga utgångspunkter för KBM:s fortsatta arbete inom området risk- och sårbarhetsanalyser, samt i görligaste mån förtydliga/konkretisera vissa begrepp, förutsättningar och frågeställningar avseende dessa risk- och sårbarhetsanalyser. Det har funnits två primära målsättningar:

1. Att beskriva rådande kunskapsläge avseende risk- och sårbarhetsanalyser samt det underlag och den metodik som tillämpas nationellt och internationellt för att producera sådana analyser.
2. Att ange en möjlig och praktiskt användbar metodik för att uppfylla kraven i förordningen 2002:472.

Det stod från början klart att målsättningen bara kunde uppfyllas i begränsad omfattning. Vad gäller den första målsättningen är den existerande kunskapsmassan av kolossalformat, ostrukturerad och under stark utveckling. Inte minst livlig är debatten angående vilken roll risk- och sårbarhetsanalyser generellt kan spela inom den totala krishanteringsprocessens ram och inför utvecklingen av de delvis nya hot och risker som det moderna samhället har att bemästra.

Inom varje tekniksektor existerar ett antal vägledningar och manualer med skiftande struktur och innehåll, utgivna av bl.a. nationella och internationella myndigheter och organisationer. Möjligheten att ge en användbar och lättöverskådlig översikt minskas av att strategier för risk- och sårbarhetshantering varierar från sektor till sektor. Det är alltså orealistiskt att försöka generellt definiera en ”state-of-art” som skall kunna omsättas i entydiga rekommendationer.

Ett annat problem har varit att försöka klargöra sambanden mellan myndigheternas generella riskhantering och organisationen av krishanteringen. Självklart innebär inte förordningen 2002:472 ens implicit något krav på myndigheternas generella riskhantering. Samtidigt anser vi att

kraven i förordningens 4 § svårligen kan uppfyllas utan att myndigheter organiserar sin krishantering i en struktur med stora likheter med ett formellt ledningssystem, d.v.s. med policy, rutiner och instruktioner (se närmare definition av begreppet ledningssystem i avsnitt 9.4). Myndighetens totala riskhantering täcker avseende målsättningar, riskkategorier och allmän organisatorisk omfattning ett område avsevärt större än krishanteringen. Dock är krishanteringen en viktig och integrerad delmängd av riskhanteringen. Mot bakgrund av detta är det svårt att beskriva risk- och sårbarhetsanalysens roll i krishanteringen utan att ta hänsyn till myndighetens riskhantering generellt. Vi har därför valt att i någon utsträckning redovisa utvecklingen internationellt avseende kraven på myndigheters totala riskhantering, samt mycket översiktligt beskriva huvuddragen i några standards och vägledningar som producerats. Orsaken är givetvis att struktur på och innehåll i risk- och sårbarhetsanalyser för krishantering uppvisar mycket stora likheter med motsvarande analyser för den allmänna riskhanteringen. Även om författarna anser att det vore till klar fördel om myndigheterna utformade sin riskhantering som ett bland andra strategiska ledningssystem förutsätter resten av detta dokument inte på något sätt existensen av ett generellt sådant system för riskhanteringen.

Vi har valt att, avseende myndigheters riskhantering, i stor utsträckning använda källor från regeringskansliet i Storbritannien. Vi har bl.a. adopterat synsättet (något modifierat) att definiera tre generiska risknivåer: strategisk nivå, program/projektnivå samt operativ/anläggningsnivå. Ramverk för risk- och krishantering beskrivs och betydelsen av fungerande ledningssystem för dessa aktiviteter betonas.

Referenser eller webbadresser ges till ett antal vägledningar och manualer, speciellt avseende sårbarhetsanalyser av infrastruktursystem utsatta för externa hot. Dessa referenser innehåller ett antal checklistor för specifika system och hotbilder. Generella checklistor för utvärdering av risk- och krishanteringsprocessen listas i appendix.

Metoder att genomföra risk- och sårbarhetsanalyser diskuteras, bl.a. redovisas en allmängiltig metodik att generera riskmatriser/riskprofiler, byggd på den s.k. grovanalysmetoden (preliminary hazard analysis). Ett förslag på innehållet i en risk- och sårbarhetsanalys enligt förordning 2002:472 redovisas. Författarna står för innehållet i förslaget och det kan möjligen ses som ett komplement till den struktur som ges i vägledningen (KBM, 2003a).

Det är vår förhoppning att erfarenheter baserade på de risk- och sårbarhetsanalyser som sänds till regeringskansliet under våren 2004 skall ge underlag för en förbättrad version av detta dokument, vilket vi ser som ett i hög grad levande dokument, samt till KBM:s fortsatta arbete inom området risk- och sårbarhetsanalyser.

3. Genomförande

3.1 Bakgrundsstudie

Rapporten utgör i huvuddrag en syntes och sammanfattning av en studie som genomförts vid Lunds Universitets Centrum för Riskanalys och Riskhantering, LUCRAM, under perioden april–oktober 2003 (Abrahamsson & Magnusson, 2004). Studien bestod av två tätt sammanlänkade delar, dels en allmän områdesöversikt och sammanställning av en kunskapsbakgrund utifrån litteraturstudier etc., dels en intervjustudie involverande nio centrala myndigheter där syftet var att föra inledande samtal kring, samt genomföra en översiktlig genomgång av, metodik, metoder och procedurer använda av myndigheterna i deras risk- och krishanteringsarbete. För intervjustudien hänvisas till Abrahamsson & Magnusson (2004).

3.2 Disposition av rapport

Rapporten är uppbyggd av två huvudsakliga delar. Del I omfattar kapitel 1–9 och utgör väsentligen en bakgrundsbeskrivning till del II, som behandlar det praktiska genomförandet av risk- och sårbarhetsanalyser.

Del I

Kapitel 4 är avsett att diskutera några grundläggande begrepp och definitioner. Betydelse och utformning av risk- och sårbarhetsanalyser kan bara utvärderas inom den totala krishanteringens ram. I avsnitt 4.2 ges därför ett par kompletterande definitioner av krishanteringens faser. Slutligen berörs de omständigheter som främst efter 11 september 2001 ändrat vår syn på den totala hotbilden och på krishanteringens roll och funktion.

I kapitel 5 diskuteras vidare några mer operativa definitioner. Terminologi och allmänna förfaringssätt avseende riskanalys och risk-

hantering berörs, liksom allmänna kvalitetskrav avseende riskanalyser. Olika aspekter på begreppet sårbarhet belyses och slutligen diskuteras relationen mellan begreppen sårbarhet, hot och risk.

Vi har bedömt det som viktigt att i viss utsträckning redovisa olika myndighetsroller med avseende på skydd av allmänheten, samt skissera hur en krishanteringsfunktion kan vara en integrerad del av myndighetens verksamhet. En summarisk beskrivning ges i kapitel 6. I kapitel 7 presenteras en översikt av olika typer av myndighetsföreskrifter på säkerhetsområdet samt redovisas mycket kortfattat ett ramverk för bestämmelseskrivande, regelverk och kontroll/tillsyn.

I kapitel 8 ges en beskrivning av tre huvudsakliga kategorier eller typer av grundorsaker/riskkällor till svåra påfrestningar som vi anser måste beaktas i risk- och sårbarhetsanalyserna. Typ 1 kan betecknas ”organisatoriska” olyckor (se avsnitt 8.1 för en redogörelse av vad som kan innefattas i begreppet ”organisatoriska” olyckor), typ 2 utgörs i huvudsak av naturkatastrofer av olika slag och typ 3 slutligen utgörs av terroristangrepp och annan påverkan med avsikt att skada ett system. I avsnittet 8.5 berörs kortfattat några teorier om olyckors och katastrofers uppkomst och hur dessa teorier kan leda till att olika delar av krishanteringen bör prioriteras för att effekten av denna hantering skall bli optimal.

Kapitel 9 utgår från vår bedömning att även om en myndighets riskhantering primärt är en allmän förvaltningsuppgift kan den inte särskiljas från beredskaps- eller krishanteringsuppgiften. Kapitlet ger därför en allmän översikt över organisationers riskhantering, samt betydelsen av att riskhantering ses som en ledningsuppgift bland andra och sköts via ett specifikt ledningssystem. En diskussion hålls om riskhantering på tre olika nivåer, strategisk nivå, program/projektnivå samt operativ/anläggningsnivå. Från Storbritannien har vi hämtat en beskrivning av innehållet i handlingsprogram (strategiskt ramverk) för myndigheters riskhantering. Kapitlet avslutas med en sammanfattning av huvuddragen i kapitel 1–9.

Del II

I denna del av dokumentet diskuteras översiktligt praktiska metoder att genomföra risk- och sårbarhetsanalyser. Vi följer den riskhierarki som tidigare skisserats med en uppdelning i strategiska risker, program-/projektrisker, risker på operativ nivå och på nivån tekniska system. Att skyddsvärda kapaciteter skall analyseras avseende risker på den lägsta nivån är mer eller mindre självklart. Det är oklart i vilken utsträckning förordningen 2002:472 över huvud har som mål att 3 § skall omfatta

de två övre risknivåerna, d.v.s. strategisk nivå och program-/projektnivå. Författarna har valt att tolka 3 § som att samtliga risker som synnerligen allvarligt kan försämra förmågan till verksamhet skall beaktas i analysen, d.v.s. även risker på de två övre nivåerna.

Kapitel 10 diskuterar metodik för att behandla strategiska risker generellt, kapitel 11 risker på program- och projektnivå som kan leda till en svår påfrestning. Kapitel 12–14 redovisar metoder att analysera risker inom de skyddsvärda kapaciteterna och riktar sig primärt till myndigheter berörda av förordningens 4 §. Kapitel 15 redovisar hur risk- och sårbarhetsanalysens struktur kan förändras när huvudmålet är att beakta avsiktliga hot och attacker samt ger webbadresser till ett antal manualer och vägledningar. Slutligen presenteras i kapitel 16 ett förslag på möjligt innehåll i risk- och sårbarhetsanalyserna enligt förordning 2002:472 samt ges hänvisningar till checklistor för utvärdering av den övergripande riskhanterings- och krishanteringsprocessen.

4. Begreppen svår påfrestning och krishantering

I den fortsatta behandlingen behöver ett antal termer preciseras. Det är värt att nämna att begreppsförvirringen inom området ibland kan vara svår och att entydiga och allmänt accepterade definitioner ofta saknas. En förklaring till denna situation kan vara att det i stor utsträckning rör sig om företeelser och händelser som till sin art kan vara mycket olika men ändå rymmas inom samma begrepp.

4.1 Begreppet svår påfrestning

Begreppet svår påfrestning har i detta dokument använts för att beskriva den typ av tillstånd som krisberedskapen är avsedd att förhindra/motverka. Begreppet beskrivs i KBM-dokumentet *Planeringsinriktning för samhällets krisberedskap 2005* (KBM 2003b) enligt följande:

"En svår påfrestning på samhället i fred utgör inte någon enskild händelse i sig, exempelvis en olycka eller ett sabotage, utan är ett tillstånd som kan sägas uppstå när en eller flera händelser gemensamt eskalerar och konsekvenserna av dessa händelser omfattar stora delar av samhället. /.../ Tillståndet är av sådan omfattning att det uppstår allvarliga störningar i viktiga samhällsfunktioner eller hotar grundläggande värden av olika slag i samhället. För att hantera situationen och därmed begränsa konsekvenserna krävs samordning av insatserna från flera olika myndigheter och organ."

Ett primärt syfte med denna rapport är att redovisa metoder och angreppssätt att analysera eskaleringsförloppet från situationerna i 3 § i förordning 2002:472 till tillståndet "svår påfrestning".

4.2 Begreppet krishantering

Krishantering är ett centralt begrepp för denna rapport och en mängd olika definitioner och tolkningar av begreppet existerar i litteraturen på området. Sundelius m.fl. (1997) beskriver innebörden av begreppet ”nationell kris” enligt följande:

Nationell kris innebär för oss att de centrala aktörerna uppfattar situationen som att:

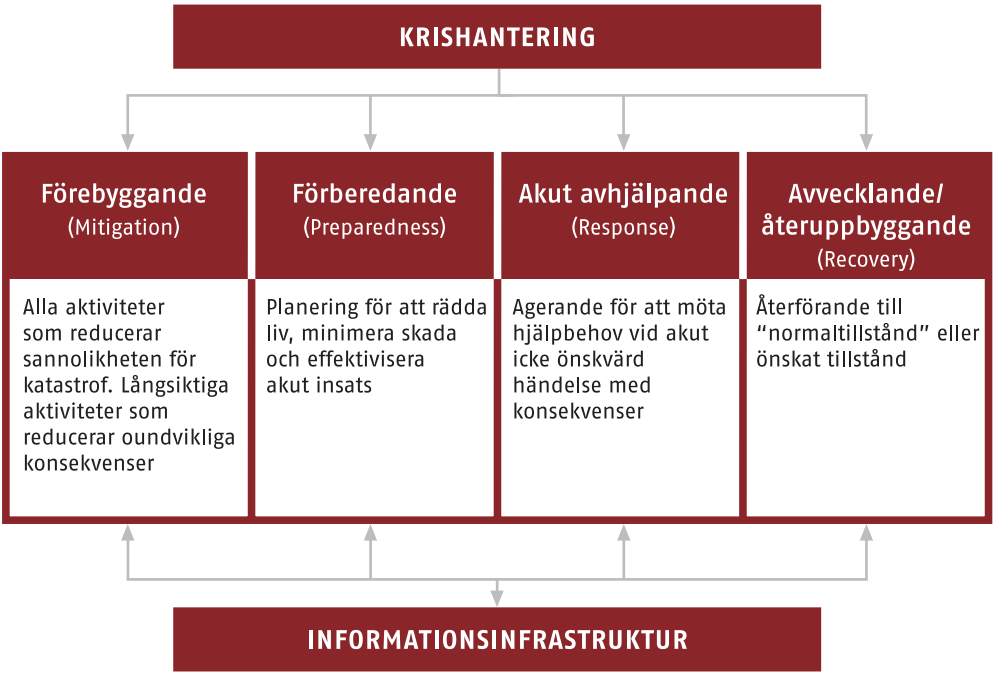
1. *betydande värden står på spel (hotas),*
2. *begränsad tid står till förfogande,*
3. *omständigheterna präglas av betydande osäkerhet.*

Vi har valt att definiera begreppet ”krishantering” genom att återge en modifierad form av FEMA-definitionen (FEMA = US Federal Emergency Management Agency), samt en kompletterande beskrivning av krishanteringens olika faser som de beskrivs i dokumentet *Crisis and Emergency Management: A Guide for Managers of the Public Service of Canada* (CCMD, 2003).

Vi gör dessutom ett försök att antyda något om de utmaningar som den nationella krishanteringen möter inför den nya och utökade hotbild som framträtt eller fått en ökad betydelse under den senaste femårsperioden. Den sistnämnda redovisningen är högst fragmentarisk, för en mer fullständig översikt refereras exempelvis till en rad artiklar i tidskriften *Journal of Contingencies and Crisis Management* under senare år samt till referenserna i Boin (2003).

4.2.1 FEMA ramverk för krishantering

I figur 4.1 nedan ges en standardiserad definition av krishanteringens olika delar enligt FEMA. De olika faserna överensstämmer väl med den indelning som ges i dokumentet ”Strategi för forskning för samhällets beredskap” (KBM, 2003c), s. 13.



Figur 4.1 *Krishanteringens olika delar enligt FEMA (US Federal Emergency Management Agency)*

För att illustrera begreppen ovan ges några exempel.

Förebyggande Det kontinuerliga arbetet med att reducera katastrofers effekt på människor och egendom. Exempel på åtgärder kan vara att förhindra att byggnader uppförs nära vatten i översvämningshotade områden, förse lasarett med reservkraft, regelbundna inspektioner för att förhindra dammbrott, beräkning av rökfyllnadstiden vid brand i byggnad med stort antal människor. Riskanalyser, riskbedömningar och åtgärder för riskreduktion (baserade på genomförda riskanalyser) utgör en väsentlig komponent av denna del av krishanteringen.

Förberedande Planering täcker en rad aktiviteter som genomförs innan en kris inträffat. Exempel utgör övning och utbildning av personal inom krisberedskapen, utveckling av insatsplaner och utveckling av datorprogramvara för beslutsstöd i en insatssituation.

Akut avhjälpande Innebär en omedelbar insats för att skydda liv och egendom. Kräver definitionsmässigt ett skyndsamt agerande och en koordinerad användning av tillgängliga resurser i en omfattning som överskrider den rutinmässiga. Fasen kan innehålla ageranden innan händelsen inträffat som en reaktion på varningssignaler.

Avvecklande/återuppbyggande Inkluderar aktiviteter både för att på kort sikt återskapa funktionen hos livsviktiga försörjningssystem och mer långsiktiga aktiviteter för att återställa infrastruktursystem till läget före katastrofen.

Informationsinfrastruktur Begreppet skall ses i vid bemärkelse och utgör en viktig del av krishanteringsplanen. Viktiga komponenter är system för detektion av vad som skulle kunna leda till oönskade händelser, ”early warning system”, samt procedurer för kommunikation och återkoppling mellan de olika delarna av krishanteringsprocessen, exempelvis hur insikter från risk- och sårbarhetsanalyser (förebyggande) kan användas i de övriga delarna (som underlag för övningar etc.).

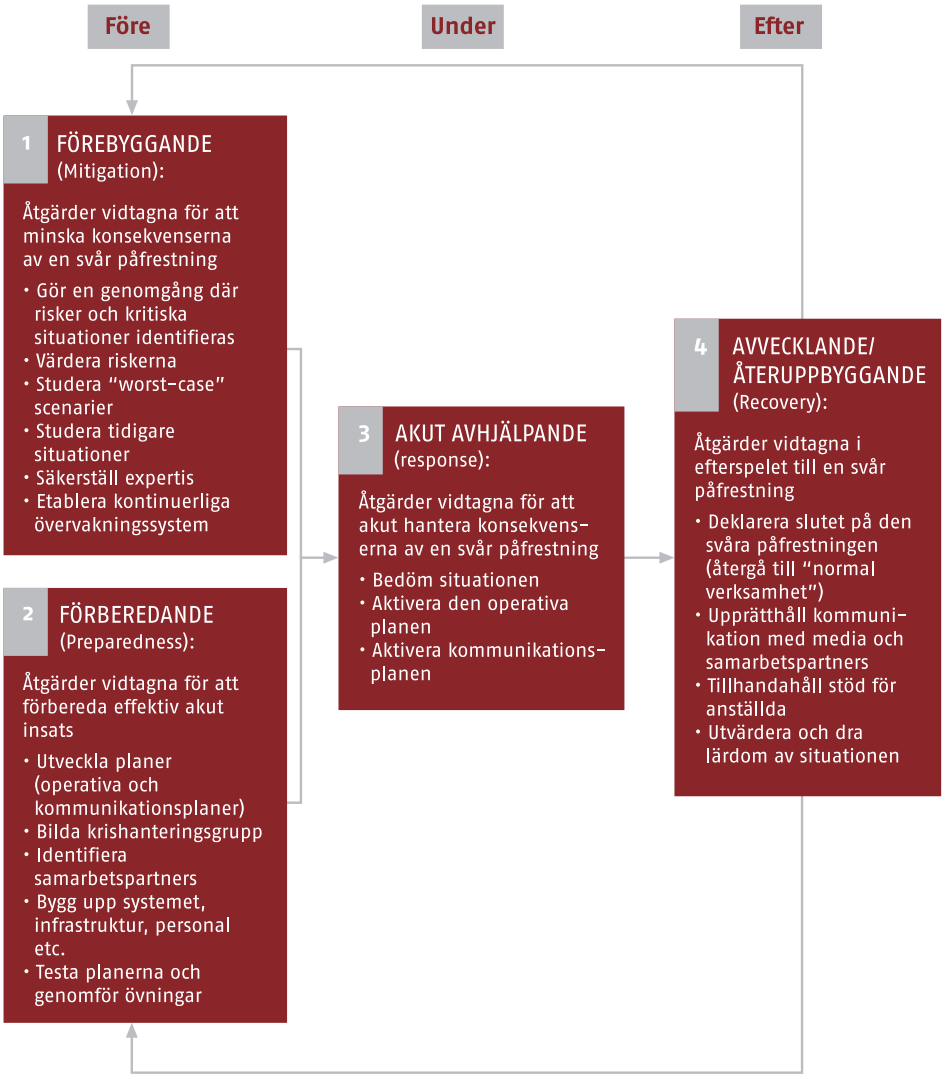
4.2.2 CCMD–ramverk för krishantering

Som nämnts tidigare finns ingen entydig allmängiltig definition av begreppet krishantering och i figur 4.2 nedan visas ett alternativt sätt att beskriva krishanteringsprocessen som används av Canadian Centre for Management Development (CCMD, 2003). Framställningen har många beröringspunkter med FEMA-definitionen och kan ses som ett komplement till denna med exempel på något annorlunda infallsvinklar till problemställningen.

Åtgärderna i boxen ”Förebyggande” ingår i organisationens generella riskhantering. De risker som avses i detta sammanhang är dock endast en delmängd av den totala riskexponeringen, närmare bestämt risker med potential att vara åtminstone en bidragande orsak till att en svår påfrestning uppkommer. En annan skillnad är att den generella riskhanteringen traditionellt sett i hög utsträckning fokuserar på att minska sannolikheten för uppkomst av svår påfrestning medan krishanteringen traditionellt haft sin tyngdpunkt på konsekvensreducerande åtgärder; se vidare avsnitt 8.5 för en inledande diskussion kring dessa frågor.

4.2.3 Krishantering och den nya hotbilden

Synen på krishantering har genomgått en radikal förändring de senaste åren. Tag SARS-epidemin som exempel. ”Epidemin” illustrerar problemet att med rimlig säkerhet bedöma hotets omfattning och möjliga sprid-



Figur 4.2 *Krishanteringsprocessen enligt CCMD (Canadian Centre for Management Development*

ning, möjligheten att skapa en tillförlitlig överblick över hur allvarligt problemet är, samt den traditionella riskhanteringens och nationalstatens ifrågasatta förmåga till effektiva insatser. SARS-epidemin innebar en relativt begränsad hälsorisk men övergick trots detta till att bli en ekonomisk störningskälla med enorm förstöringspotential. SARS medförde bl.a. mycket kraftiga störningar i den globala lufttrafiken och turismen samt isolering av världsstäder. Ingen vet om den i skrivande stund kan betraktas som nedkämpad.

Den moderna krisen diskuteras bl.a. i Boin (2003) från vilken publikation vi återger följande synpunkter. Utgångspunkten är att ett antal nya kriskategorier avtecknar sig vid horisonten: cyberterrorism, andra typer av terrorism med biologiska och/eller kemiska vapen, transnationella kollapser i tekniska försörjningssystem, genmodifierade livsmedel och kris relaterad till allmänhetens tilltro till livsmedelsindustri och tillsynsmyndigheter, globala klimatförändringar etc. Den moderna krisens komplexitet motstår ofta vår förmåga att identifiera orsaker, att förstå eskaleringsmekanismer och att genomföra effektiva motåtgärder. Den kan ofta inte beskrivas på traditionellt vis med hjälp av parametrar som anger början och slut, intensitet och geografisk utbredning. Det är en i samhället inbyggd sårbarhet som bryter fram, tycks försvinna men återkommer, ibland i muterad form. Konsekvenserna av den moderna krisen anges inte främst i antalet dödade eller sårade; det som angrips är statens själva legitimitet och dess förmåga att ge det skydd som åtminstone i fredstid har betraktats som självklart.

Frågan uppstår om vi har analytiska verktyg att förstå orsaker, mönster, händelseutvecklingar och slutliga skadeeffekter vad gäller dessa nya hot och faror. För en sammanfattande beskrivning av några utvecklingslinjer avseende riskanalytiska metoder generellt, se Abrahamsson & Magnusson (2004).

5. Begreppen riskanalys och sårbarhetsanalys

5.1 Inledning

En rapport med målsättningen att diskutera utgångspunkter för KBM:s fortsatta arbete inom området risk- och sårbarhetsanalyser har att redovisa en diskussion om terminologi för nyckelbegrepp som hot, risk, sårbarhet, riskanalys och sårbarhetsanalys, samt föreslå definitioner som underlättar det praktiska arbetet med kraven i förordningen 2002:472. Detta är viktigt inte minst från synpunkten att de utförda analyserna bör ha samma begreppsapparat om det totala materialet skall kunna sammanställas, analyseras och syntetiseras med rimlig arbetsinsats.

5.2 Risk, riskanalys och riskhantering

5.2.1 Risk och riskperspektiv

Definitionen av risk har i modern tid sitt ursprung i ett *tekniskt "objektivistiskt"* förhållningssätt där man intagit ett strikt naturvetenskapligt förhållningssätt till riskproblematiken. Risk kan rent tekniskt förstås som en sammanvägning av sannolikheten för att en händelse skall inträffa samt de (negativa) konsekvenser händelsen i fråga kan anses leda till. Kaplan (1997) menar att risk rent tekniskt kan definieras som svaret på tre frågor:

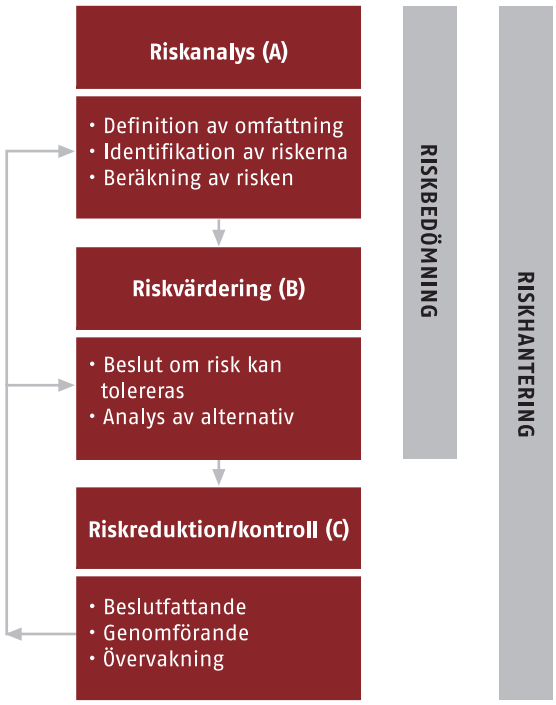
- Vad kan hända (vilka scenarion, S, kan uppstå)?
- Hur troligt är det att det händer (sannolikhet, L)?
- Vilka är konsekvenserna, X, av händelsen?

Denna tekniska definition av risk ger dock en förhållandevis okomplicerad bild av riskproblematiken. Den svarar inte på frågor varför vissa händelser kan anses oönskade. Den svarar inte heller på varför individer

har olika uppfattning om vad som är en risk och betydelsen av denna risk. Forskning som fokuserar frågor av denna art brukar ofta sägas utgå från ett *socialkonstruktivistiskt perspektiv*. För en mer ingående beskrivning av detta synsätt hänvisas till Abrahamsson & Magnusson (2004).

5.2.2 Riskanalys och riskhantering

I figur 5.1 nedan ges en generisk beskrivning av riskhanteringsprocessen enligt IEC (International Electrotechnical Commission, 1995).



Figur 5.1 *Riskhanteringsprocessen.*
Källa: International Electrotechnical Commission, IEC 1995

I praktiken är det naturligtvis så att olika teknologigrenar och olika verksamhetsgrenar allmänt sett har sina egna standardiserade processer för såväl riskanalys som riskhantering i stort. Här ges endast en övergripande bild av de huvudsakliga elementen. Det skall nämnas att processen i figur 5.1 avser riskanalys av tekniska system. Motsvarande generiska modeller existerar givetvis även för analys av andra typer av verksamheter och system.

5.2.3 Riskanalyser och allmänna kvalitetskrav

Att utföra en riskanalys är ofta ett av de första stegen i en process som kommer att utmynna i att ett beslut skall fattas. Beslutet kan handla om huruvida den aktuella risken är acceptabel eller inte, samt vilka alternativ som skall väljas för att reducera eller kontrollera risken. För att kunna fatta ett så bra beslut som möjligt i en fråga krävs det att beslutsfattaren har tillgång till så fullständig och korrekt information som möjligt. Ett ganska självklart påpekande kan tyckas, men ändå viktigt att betona då beslutssituationer ofta kännetecknas av ett komplext och ofullständigt bakgrundsmaterial. Innebörden i detta är att beslut måste fattas under stor osäkerhet. Morgan & Henrion (1990) anser, med anledning av den ovan beskrivna situationen, att vissa krav bör ställas på en analys för att den skall leda till beslut som är så bra som möjligt med hänsyn tagen till den aktuella kunskapen, dess begränsningar och dess innebörd. De sammanfattar dessa kriterier som tio ”budord”.

1. Studera adekvat litteratur, konsultera experter och praktiker inom ämnet.
2. Låt analysen vara probleminriktad.
3. Gör analysen så enkel som möjligt men inte för enkel.
4. Identifiera alla antaganden som kan anses signifikanta.
5. Var tydlig beträffande beslutskriterier och policy.
6. Var tydlig om den osäkerhet som gäller.
7. Utför en systematisk känslighets- och osäkerhetsanalys.
8. Se problemformulering och analys som en iterativ process.
9. Gör en tydlig och fullständig dokumentation
10. Underkasta analysen en peer-review

För en mer utförlig beskrivning av den praktiska innebörden i dessa ”budord” hänvisas till Abrahamsson & Magnusson (2004) eller till ursprungsreferensen Morgan & Henrion (1990). För en diskussion kring kvalitetskrav avseende analyser av olycksrisker hänvisas till Räddningsverket (2003).

5.3 Olika aspekter på sårbarhetsbegreppet

Sårbarhet är ett begrepp med många betydelser och många användningar. Vi skall här koncentrera oss på definitioner av begreppet som är användbara i krishanteringssammanhang. I vägledningen (KBM, 2003a) ges en definition av begreppet sårbarhet som är av mycket generell natur:

"Sårbarhet betecknar hur mycket och hur allvarligt ett system påverkas av en händelse. Graden av sårbarhet bestäms av förmågan att förutse, hantera, motstå och återhämta sig från händelsen."

När vi försöker att något differentiera och exemplifiera denna definition väljer vi tre användningsområden: sårbarhet och naturkatastrofer, sårbarhet i tekniska system i allmänhet och som ett nyckelbegrepp för skydd av infrastruktursystem mot externa hot och attacker, samt slutligen för social sårbarhet och krishantering i allmänhet.

Sårbarhet speciellt länkad till naturkatastrofer

Weichselgartner (2001) har gjort en sammanställning av ett 25-tal definitioner, de flesta länkade till området sårbarhet och naturkatastrofer. Låt oss citera två exempel:

Timmerman (1981): ”Sårbarhet betecknar den omfattning med vilken ett system reagerar negativt på en exponering från en utlöst riskkälla. Omfattning och styrka av den negativa reaktionen bestäms av systemets motståndsförmåga (ett mått på systemets förmåga att absorbera och återhämta sig från påverkan efter händelsen).”

Watts & Bohle (1993): ”Sårbarhet definieras i termer av exponering, kapacitet och handlingsmöjligheter. Härav följer att åtgärdsstrategin för att kontrollera sårbarhet är att reducera exponering, öka förmågan att hantera påfrestningen, förstärka återhämtningspotentialen och effektivisera skadekontrollen via offentliga och privata medel”.

Sårbarhet enligt denna definition är alltså både en beskrivning av tillståndet hos ett skyddsvärt system (exempelvis elförsörjning) innan händelsen utlösts och en beskrivning av förmåga till akut avhjälpande insatser, social motståndskraft och robusthet när riskkällan aktiverats. Länken mellan sårbarhetsanalys och krishantering framgår således klart av definitionen från Watts & Bohle ovan.

Sårbarhetsanalys av tekniska system, planerade och oplanerade hot

Det kan vara ändamålsenligt att särskilja sårbarhet i tekniska system och sårbarhet länkad till krishantering i allmänhet. Exempelvis har Einarsson

& Rausand (1998) utvecklat en scenariobaserad metodik för sårbarhetsanalys av komplexa industriella system. I artikeln används termen sårbarhet för att beskriva de egenskaper hos ett industriellt system som kan påverka systemets möjligheter att överleva och fullfölja sin uppgift under närvaro av hot. Analysen utförs i ett antal steg (Einarsson 1999, Einarsson & Rausand 1998) som bl.a. innefattar identifikation av riskkällor med hjälp av checklistor, identifikation av olycksscenarier (bl.a. med hjälp av händelseträd), bortgallring av scenarier med låg sannolikhet, uppskattning av de kvarvarande scenariernas effekter på människor, egendom och affärsliv, identifikation och utvärdering av skadereducerande resurser samt identifikation och utvärdering av resurser för att återuppbygga och återskapa företaget. En kortfattad beskrivning av metodiken ovan återfinns i Abrahamsson & Magnusson (2004).

Vid planerade hot kan sårbarheten definieras som ”svagheter i (det tekniska) systemet som kan utnyttjas av en inkräktare för att få tillgång till en kritisk resurs. Sårbarheter kan omfatta, men är inte begränsade till, byggnaders egenskaper, egenskaper hos utrustning, närvaro av personal, operativa och organisatoriska rutiner/instruktioner” (CCPS, 2002).

Social sårbarhet

Om svåra påfrestningar inträffar, drabbas civilbefolkningen nästan utan undantag i någon form. Det kan omfatta allt i fråga om fysiska påfrestningar, men också gälla olika former av sociala och psykiska belastningar. I och med en ny och breddad risk- och sårbarhetssituation, samt svårigheterna att förutse och hantera den, har social sårbarhet blivit ett centralt begrepp inom krishantering. En viktig fråga gäller hur sårbarheten fördelas i tid och rum hos den befolkning som berörs. Analysmetoder saknas för närvarande för att på ett systematiskt sätt bedöma social sårbarhet. För en något mer utförlig diskussion kring social sårbarhet hänvisas till Magnusson & Abrahamsson (2004).

Exemplifieringen ovan avser att demonstrera att det i risk- och sårbarhetsanalyser kan vara fördelaktigt att dela upp begreppet sårbarhet i två delar:

- En inre sårbarhet i ett (tekniskt) system som härrör från interna brister och som medför att om en oförutsedd eller riskmedvetet accepterad händelse/hot realiseras uppstår en allvarlig felfunktion eller ett sammanbrott. Sårbarheten kan vara av fysisk, teknisk eller operativ art.
- Yttre, social sårbarhet.

Begreppen återkommer i del II av detta dokument.

5.4 Relationen sårbarhet, hot och risk

Relationen mellan begreppen sårbarhet, hot och risk diskuteras i regeringens proposition 2001/02:158 *samhällets säkerhet och beredskap* och där framhålls bl.a. att det inte är ändamålsenligt att diskutera ett systems eller samhällets allmänna sårbarhet enskilt i den meningen att denna sårbarhet i sig skulle utgöra ett hot eller en risk och därmed vara ett tillräckligt underlag för beslut om åtgärder etc.

I propositionen betonas att en diskussion av sådana frågor även måste beakta sannolikheten för att en potentiell riskkälla realiseras eller att någon har avsikt och förmåga att verkställa ett hot, samt konsekvenserna av den händelse som kan inträffa.

Som en direkt följd av detta konstateras vidare att man, för att kunna erhålla ett underlag som gör det meningsfullt att diskutera huruvida åtgärder måste vidtas, måste genomföra en samlad analys av samtliga dessa aspekter. Som exempel på olika typer av åtgärder framförs såväl förebyggande, där avsikten är att eliminera eller kraftigt reducera risken (vilket man definierar som riskhantering), som åtgärder som syftar till att bättre kunna hantera situationen om den ändå skulle inträffa (vilket man definierar som krishantering).

Den operativa användningen av de begrepp och definitioner som diskuterats i kapitlet kommer att redovisas i inledningen av del II av detta dokument. I nästa kapitel fortsätter bakgrundsbeskrivningen i form av en diskussion kring olika roller som myndighetssektorn kan sägas ha avseende skydd för allmänheten, följt av en beskrivning av en tänkbar modell för myndigheters krishanteringsverksamhet.

6. Myndighetsroller samt en modell av krishanteringens uppbyggnad

Det nämndes i avsnitt 4.2.3 att den ändrade hotbilden gör att nationalstatens förmåga att skydda sina medborgare har kommit att ifrågasättas. Det förefaller lämpligt att översiktligt antyda hur detta skydd är strukturerat och organiserat. Betydelsen för denna rapport, och en mycket viktig sådan, är slutsatsen att myndigheternas risk- och sårbarhetsanalys enligt författarna bör omfatta det totala ansvarsområdet, d.v.s. dels den interna verksamheten, dels alla externa verksamheter som lyder under myndighetens föreskrifter och/eller tillsyn. Slutligen skisseras en möjlig modell för myndigheternas krishantering.

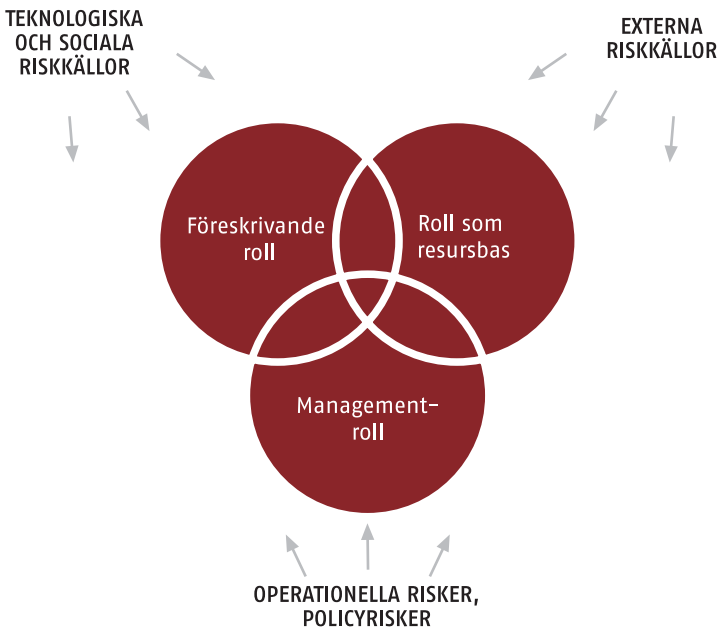
6.1 Myndigheters olika roller

Myndighetssektorn kan schematiskt sägas ha tre olika roller i relation till skyddande av allmänheten (Strategy Unit, 2002).

- Föreskrivande och tillsynsutövande. Verktyg för myndighetsutövning inom denna roll inkluderar lagstiftning/föreskrifter, kontroll, inspektion, tillståndsgivning, råd och anvisningar, information, etc.
- Som en bas eller källa för resurser (räddningstjänst, polis, sjukvård, etc.) att användas för skydd mot externa risker – naturkatastrofer, epidemier, stora olyckor i tekniska system, etc.
- Som ansvariga för riskhanteringen av den egna verksamheten och för skyddande av den egna resursbasen.

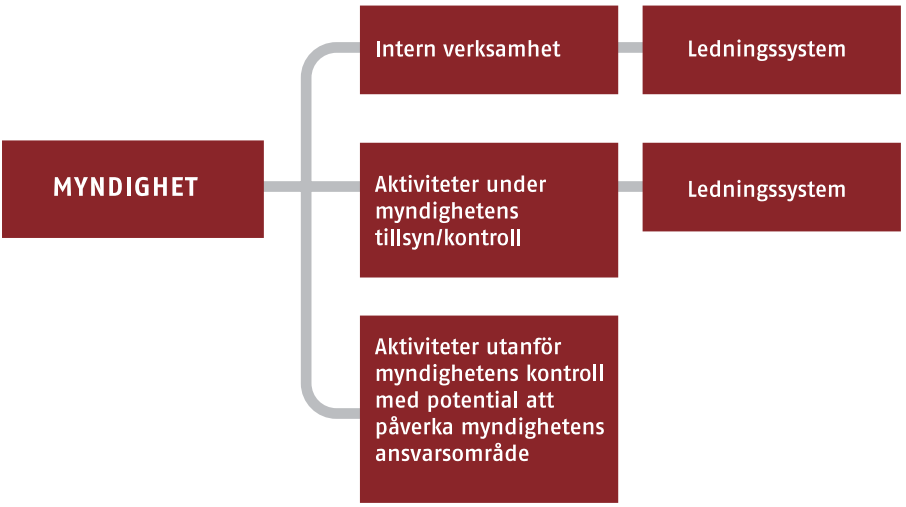
De olika rollerna, som är delvis överlappande, illustreras av figur 6.1 nedan. För en närmare diskussion hänvisas till publikationen Strategy Unit, 2002.

Figur 6.1 *Myndigheters olika roller (Strategy Unit, 2002)*



6.2 En modell av myndigheters krishanteringsverksamhet

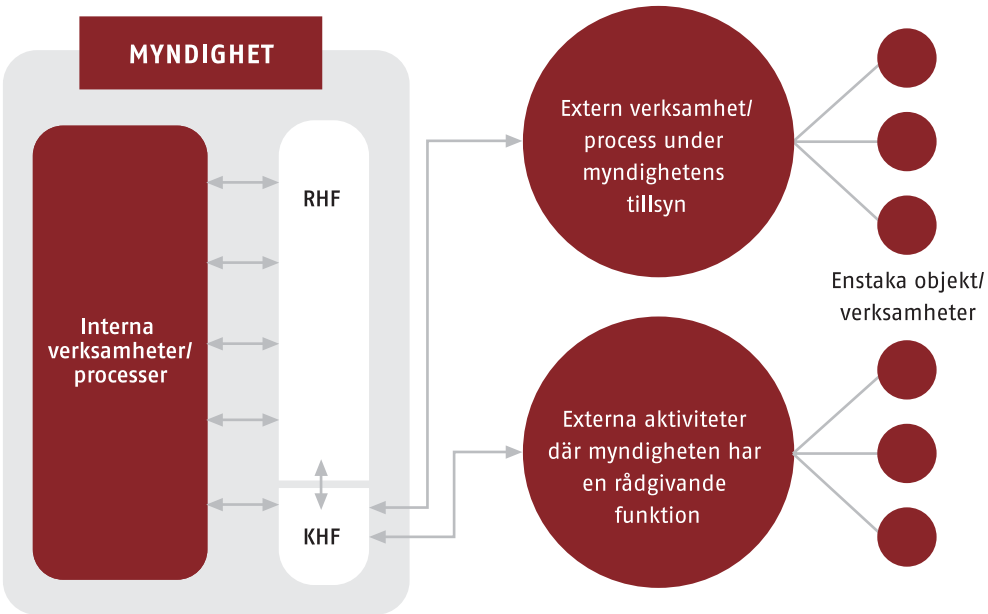
I kapitel 1 återgavs 3 § i *förordning (2002:472) om åtgärder för fredstida krishantering och höjd beredskap* där varje myndighet åläggs att analysera sårbarhet och risker inom respektive *ansvarsområde*. I figur 6.2 nedan redovisas en indelning i tre delområden som vi anser bör beaktas i analysen enligt 3 §: intern verksamhet, aktiviteter under myndighetens tillsyn/kontroll samt aktiviteter utanför myndighetens kontroll men som ändå kan påverka verksamhet inom myndighetens ansvarsområde.



Figur 6.2 *Delområden som bör beaktas i analysen: intern verksamhet, aktiviteter under tillsyn/kontroll, samt aktiviteter utanför formell kontroll med potential att påverka myndighetens ansvarsområde.*

Vi har tidigare även konstaterat att ordalydelsen i förordningens 4 § indikerar att de myndigheter som omfattas av paragrafen bör ha en väl utvecklad organisation för krishantering inklusive hantering av risker med potential att vara åtminstone en bidragande orsak till att en svår påfrestning uppkommer. Detta inkluderar i vår mening fungerande ledningssystem för hantering av nämnda risker. Riskerna kan finnas dels inom den interna verksamheten, dels inom de verksamheter som står under myndighetens tillsyn/kontroll. Ledningssystem för riskhantering diskuteras vidare i avsnitt 9.4.

Nedanstående figur (6.3) utgör ett försök att beskriva *en* modell för hur krisberedskapen och krishanteringen inom en myndighet kan fungera. Vi vill betona att figuren beskriver en *möjlig* och starkt förenklad organisationsstruktur och att existerande strukturer kan vara helt eller delvis avvikande. Figuren är avsedd att beskriva en principiell uppbyggnad som kan användas som diskussionsunderlag.



***Figur 6.3** En **möjlig** modell för myndigheters krishanteringsverksamhet (RHF = Riskhanteringsfunktion, KHF = Krishanteringsfunktion)*

Förordningen 2002:472 omfattar i sin 3 § ca 400 myndigheter och det är självklart att krishantering i förordningens mening utgör ett problem och ett verksamhetsområde av mycket varierande betydelse. Alla myndigheter torde emellertid uppleva att verksamheten får stora problem om exempelvis el- och IT-försörjningen slås ut under längre perioder. Slutsatsen blir att i stort sett samtliga myndigheter måste planera för avbrott av denna typ; d.v.s. ha en krishanteringsplan. Mot denna bakgrund föreslår författarna att myndigheterna inrättar en krishanteringsfunktion (KHF), se figur 6.3.

Författarna tolkar detta som ett fundament för att intentionen i förordningen skall kunna uppfyllas: att varje myndighet upprättar en funktion för krishantering med väl specificerad uppgift (inklusive exempelvis reviderbar egenkontroll). Grundläggande för KHF är bl.a. att samla information, analysera och syntetisera denna information, upprätta en krishanteringsplan, genomföra nödvändiga åtgärder och kon-

trollera deras effektivitet. KHF har att arbeta utifrån två perspektiv, ett inre och ett yttre, se figurerna 6.1 och 6.3. Det inre innebär ansvar för krishanteringen av den egna verksamheten och skyddande av den egna resursbasen. Det yttre perspektivet innebär tillsyn, kontroll, inspektion, rådgivning och information rörande krishantering för externa aktiviteter och organisationer inom myndighetens ansvarsområde.

Som en del av risk- och sårbarhetsanalysen bör enligt författarna ingå:

- Redovisning av uppbyggnad av krishanteringsfunktionen (KHF)
- Redovisning av aktiviteten inom KHF
- Redovisning av eventuell krishanterings- eller beredskapsplan.

Med andra ord: det bör ingå en strukturerad analys av hur de processer/aktiviteter som översiktligt beskrivs i figurerna 6.1 och 6.3 genomförs vid myndigheten.

7. Myndighetsföreskrifter på säkerhetsområdet: något om struktur och utveckling

7.1 Inledning

I avsnitt 6.2 talades om begreppet *ansvarsområde* enligt 3 § i förordningen 2002:472 och att verksamheter som omfattas av en myndighets föreskriftsrätt och tillsyn/kontroll bör ingå i detta ansvarsområde. I detta kapitel ges en kortfattad beskrivning av olika typer av föreskrifter och tillsyn/kontrollverksamhet inom säkerhetsområdet.

Samverkan mellan myndigheter är en av grundförutsättningarna i det nya nationella krishanteringssystemet, se exempelvis KBM (2003b). Samverkan skall ske på lokal, regional och nationell nivå. Som bas för denna samverkan ligger de föreskrivande och tillsynsutövande funktionerna främst på nationell nivå.

För att närmare kunna beskriva och förstå funktionen av ovan nämnda föreskrivande och tillsynsutövande funktioner över det breda registret av samverkansmyndigheter bör en del grundläggande problemställningar belysas. Exempel på sådana frågor är:

- Vilka olika former av föreskrifter/kontroll används och hur effektiva är de?
- Hur påverkar utformningen av föreskrifter det praktiska myndighetsarbetet? Fördelar och nackdelar med olika utformningar.
- På vilket sätt bestäms valet av typ av myndighetsföreskrift av den aktivitet som skall regleras?
- Vad kan överföras från ett myndighetsområde till ett annat med en annan typ av teknologi, aktivitet, risk eller jurisdiktion?
- Slutligen: i vilken utsträckning kan föreskrifterna/kontrollen baseras på eller länkas till genomförda risk- och sårbarhetsanalyser?

Avsnitt 7.2 är avsett att ge bakgrundsinformation för diskussion av dessa frågor.

7.2 Något om olika typer av föreskrifter och kontrollverksamhet

I detta avsnitt ges en mycket kortfattad beskrivning av olika typer av föreskrifter och kontrollverksamhet på säkerhetsområdet. För den som vill fördjupa sig inom området ges en utförligare beskrivning i ursprungsreferensen Hale et al (2002).

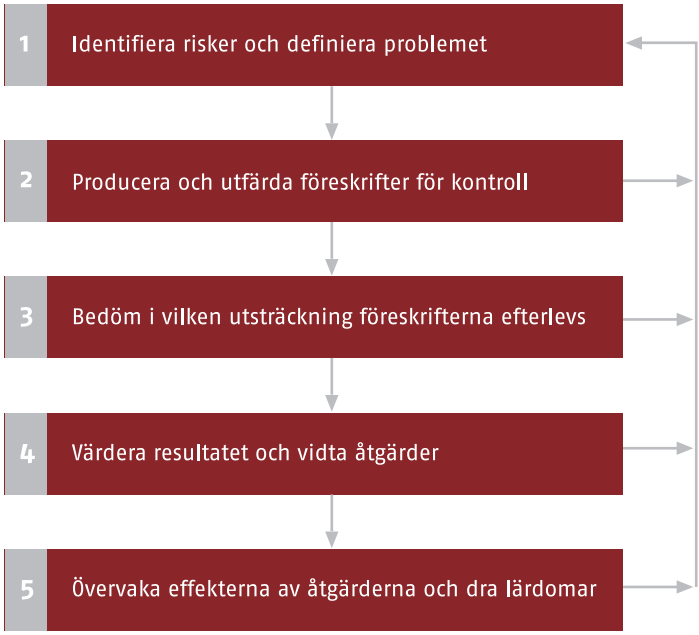
7.2.1 Olika typer av föreskrifter

Generellt sett kan sägas att det inom säkerhetsområdet växt fram tre huvudsakliga grupper av myndighetsföreskrifter:

- **Preskriptiva föreskrifter**, d.v.s. ofta mycket specifika tekniska krav avseende exempelvis utrustning, arbetsmiljö o.s.v. Denna föreskriftsregim växte fram i och med den industriella revolutionen och fick stor genomslagskraft på flera områden. Angreppssättet har dock inom många områden, bl.a. som en följd av den ökade utvecklingstakten, kommit att uppfattas som alltför otympligt för att kunna användas i praktiken.
- **Målorienterade/funktionsbaserade** föreskrifter framkom under 60- och 70-talen som en reaktion på de alltför ohanterliga preskriptiva föreskrifter som dominerat under ett antal decennier. Mycket allmänt kan sägas att lagstiftningen gick från att ha specificerat standards och procedurer för att höja säkerheten till att föreskriva de säkerhetsmål verksamheten skulle uppfylla. Hur dessa mål skulle kunna uppnås överläts, åtminstone i princip, till verksamhetsansvariga att utforma. Problemet för myndigheterna är naturligtvis att för det första ange säkerhetsmål, för det andra definiera kriterier för vad som anses vara en acceptabel säkerhetsnivå/tolerabel risknivå.
- **Metoder byggda på ledningssystem för säkerhet och säkerhetsrapporter** är en typ av föreskrifter som kräver att den reglerade verksamheten demonstrerar för ansvarig myndighet att organisationen har identifierat, bedömt och kan kontrollera viktigare riskkällor, vilket givetvis bl.a. förutsätter att en riskanalys har genomförts. I ökande grad krävs att arbetsgivare och anläggningsansvariga introducerar ledningssystem för säkerhet.

7.2.2 Ett ramverk för bestämmelse-skrivande, regelverk och kontroll

I avsnitt 7.2.1 identifierades tre modeller för innehållet i säkerhetsföreskrifter: teknisk beskrivning, funktionsbaserat regelsystem och lagstiftning baserad på säkerhetsrapport och säkerhetsledningssystem. För var och en av de tre föreskriftsregimer som nämns ovan kan aktiviteten beskrivas som en cyklisk process i fem steg:



Figur 7.1 *Process för föreskrivande och säkerställande av efterlevnad (översättning från Hale et al 1997)*

Vad som intresserar oss här är främst stegen 2–3. Hale et al (2002) konstruerade en matris där aktiviteter för stegen 2 och 3 indikeras för de tre föreskriftsregimerna, se figur 7.2 nedan.

NIVÅ	PRODUCERA OCH UTFÄRDA FÖRESKRIFTER	KONTROLLERA EFTERLEVNAD
Mål/funktions-baserade bestämmelser	**A.** Etablera acceptabla risknivåer	**B.** Kontrollera att utdata från verksamheten idikerar måluppfyllnad
Bestämmelser byggda på krav på säkerhets-ledningssystem/ säkerhetsrapport	**C.** Skriv regler för säkerhets-ledningssystem och säkerhets-rapporter och hur dessa kontrollerar risker	**D.** Kontrollera struktur på och funktion av ledningssystemet
Direkt riskkontroll, preskriptiv metod	**E.** Utforma detaljregler för operativ nivå och processutformning	**F.** Kontrollera att detaljregler för operativ nivå efterföljs

Figur 7.2 *Aktiviteter vid produktion och utfärdande av föreskrifter, samt kontroll av efterlevnad för de tre föreskriftsregimerna (översättning från Hale et al, 2002)*

I det refererade arbetet betonas att de sex uppgifterna A–F ovan för given typ av verksamhet i regel måste genomföras samtidigt för att riskerna skall anses kontrollerade.

I en bedömning av sårbarhetsläget inom en given sektor eller verksamhet bör enligt författarna ingå en utvärdering av i vilken utsträckning gällande föreskrifter och utförd kontroll (tillsyn) inklusive egenkontroll är en acceptabel bas för minimering av sektorns sårbarhet. Vad gäller tillsynen konstaterar SOU 2001:41, *Säkerhet i en ny tid*, i kapitel 11 att det finns skillnader i tillsynsorganens förutsättningar att effektivt lösa sin uppgift. En del av dessa skillnader kan förmodligen återkopplas till figuren 7.2 med dess tre föreskriftsregimer med åtföljande krav på utformning av tillsynsarbetet. Som betonats tidigare måste i regel samtliga sex aktiviteter A–F genomföras samtidigt för att erhålla en heltäckande kontroll av riskerna i en verksamhet.

Detta ger upphov till en rad (intressanta) frågeställningar:

- Vilken aktör utför de enskilda uppgifterna A–F för den reglerade sektorn eller aktiviteten? Myndighet på nationell, regional eller lokal nivå? Verksamhetsägare? Tredje part?
- I den mån myndigheter är inblandade, hur fördelas ansvaret mellan nationell, regional och lokal nivå och vilka otydligheter i ansvarsfördelningen medför detta?
- Är en sådan områdesuppdelning optimal för en minimering av sårbarheten?

Myndigheter använder i ökande omfattning ackreditering och (tredje parts) certifiering som ett partsoberoende och transparent medel att tillse att organisationer följer föreskrifterna. Möjliga följdproblem inkluderar:

- Att konsumenter och fackföreningar utesluts från inflytande.
- Myndigheternas möjligheter att tillse efterlevnad inskränks.
- Riksdagens lagstiftningsmakt minskar i de konkreta fallen.

Detta är en utveckling som accelererar till följd av den snabba och dynamiska utvecklingen inom nya teknologier och som inte borde lämnas obeaktad.

7.3 Risk- och sårbarhetsanalyser och de tre olika föreskriftsregimerna

I de risk- och sårbarhetsanalyser som myndigheterna skall producera bör enligt författarna ingå en analys av myndighetens funktion och en möjlighet att specificera exempelvis:

- Vem som ansvarar för regelsystem (rutiner, instruktioner) på operativ nivå
- Vem som kontrollerar efterlevnad på operativ nivå
- Vem som utfärdar föreskrifter för säkerhetsledningssystem och ledningssystem för krishantering
- Vem som utvärderar effektiviteten av ledningssystemen
- Vem som etablerar nivå för acceptabel risk
- Vem som kontrollerar att denna nivå uppfylls,

samt en genomgång av de problem och dilemman som svaren på frågeställningarna ovan eventuellt skapar.

8. Olika typer av grundorsaker till svåra påfrestningar

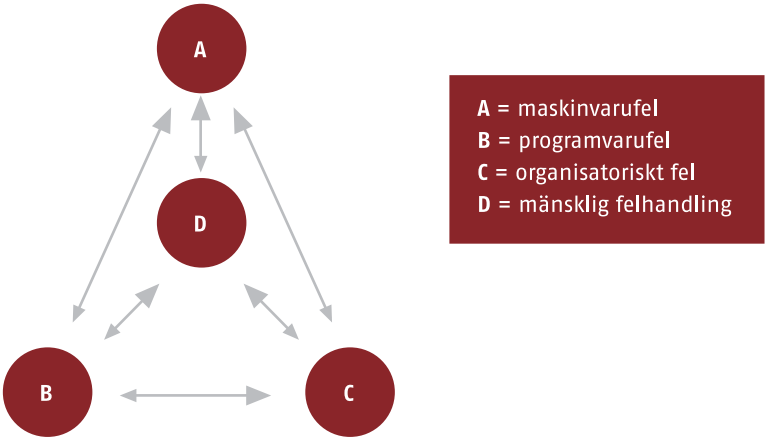
Det är naturligtvis en truism att konstatera att en svår påfrestning kan ha en rad olika grundläggande orsaker och vara resultatet av händelsekedjor med vitt skilda karakteristika. Vi har valt att särskilja tre typer av grundläggande orsaker:

- **Typ 1:** kan efter Reason (1997) benämnas organisatoriska olyckor. Orsakerna till dessa olyckor kan vara av mänskligt, organisatoriskt eller tekniskt ursprung. De inträffar relativt sällan, men är ofta katastrofartade om de väl inträffar, i exempelvis kärnkraftverk, kommersiell flygtrafik, petrokemisk industri, kemisk processindustri, transport på järnväg och hav, bankväsendet och samlingspunkter för ett stort antal människor (idrottsanläggningar, diskotek etc.). Till denna grupp kan vi också hänföra fenomen av typen ”allvarlig smittspridning” genom att organisatoriska brister (tillsyn, kontroll) kan anses skapa förutsättningar för uppkomst av svår påfrestning.
- **Typ 2:** naturkatastrofer av olika slag.
- **Typ 3:** terroristangrepp och andra typer av avsiktlig påverkan. Vi refererar här kortfattat några synpunkter från en storskalig amerikansk utredning initierad p.g.a. WTC-katastrofen.

Utelämnade är därmed exempelvis påfrestningar som beror på finansmarknadens kollaps, internationella konflikter, etc.

8.1 Grundläggande orsaker till svåra påfrestningar enligt typ 1

Felorsaker för en svår påfrestning av denna kategori kan generellt grupperas enligt figur 8.1 nedan (Haimes, 1998):



Figur 8.1 *Felorsaker*

En rad undersökningar har visat att ca 80 % av riskrelaterade oönskade händelser och förlopp beror på faktorn C, d.v.s. organisatoriska fel. Innebörden är att om målsättningen med förordning 2002:472 skall kunna uppfyllas bör enligt författarna myndigheternas risk- och sårbarhetsanalyser innehålla en bedömning av den egna förmågan att förhindra att organisatoriska brister bidrar till att en ”normal” riskkälla utlöser en händelsekedja som i slutändan innebär en svår påfrestning. Detta krav gäller också de externa aktiviteter/organisationer som ligger inom myndighetens kontroll- och/eller tillsynsuppgift eller allmänna ansvarsområde.

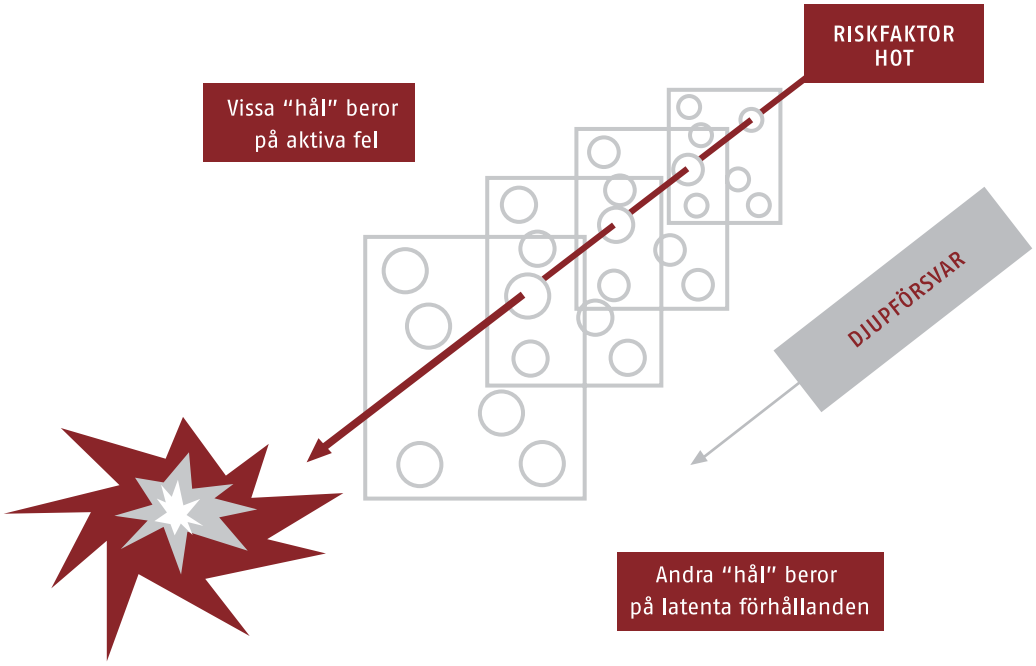
Några typiska orsaker till organisatoriska fel (C ovan) är:

- Förbisedda eller ignorerade defekter.
- Dröjsmål med att korrigera defekter.
- Sammanbrott i kommunikation.

- Missade signaler eller annan typ av data till följd av försummad inspektion eller undermåligt underhåll.
- Olösta konflikter mellan ledning och arbetskraft.
- Döljande av misstag på grund av exempelvis konkurrens.
- Effekter av ”down-sizing” och ”outsourcing”.
- Generellt sett undermålig säkerhetskultur (se avsnitt 8.1.3).

8.1.1 Olyckor av typ 1: en förklaringsmodell

En ”normal” slumpartad händelse eskalerar till en katastrof genom brister i de olika barriärer d.v.s. försvarssystem och skyddsåtgärder som upprättats. Bristerna kan uppkomma genom aktiva fel och latenta förhållanden (Reason, 1997), se figuren nedan.



Figur 8.2 *Reasons "schweizerostmodell" (översatt från Reason, 1997)*

I dagens samhälle finns stora komplexa sociotekniska system med potential att åstadkomma allvarliga kriser som kan leda till svåra påfrestningar i samhället. Det finns ofta försvar mot att enstaka händelser skall kunna orsaka sådana kriser. Ofta finns olika typer av försvar som verkar i olika delar av orsaksträdet – det finns ett djupförsvar (defense-in-depth). Krisen uppstår när alla barri-ärerna bryts igenom. I följande resonemang utgår vi från Reasons (1997) schweizerostmodell (se figur 8.2) för att diskutera organisatoriska olyckor, så stora att de medför svåra påfrestningar. Epitetet ”organisatoriska” betyder att man hittar orsakerna på olika nivåer i en organisation – i ett system – som kan innefatta hela kedjan från lagstiftare, via tillsyn, strategisk ledning, taktisk ledning till process. Försvarsbarriärerna illustrerade i figur 8.2 är av olika typ. Här följer ett exempel som illustrerar vilka typer det kan vara.

- Verksamheter som skall öka förståelsen och medvetenheten om faror.
- Stöd för säker styrning/hantering av en process.
- Larm och varningssignaler.
- Metodik eller automatik som återför systemet i ett säkert tillstånd om det hamnat utanför en säker zon.
- Fysiska barriärer mellan riskkällan (energin i vid bemärkelse) och riskobjektet (target = människor, miljö, infrastruktur) om tillämpligt.
- Arrangemang för att innesluta och eliminera energin om den passerat de fysiska barriärerna – om tillämpligt.
- Möjligheter att fly undan faran.

Barriärerna har emellertid brister illustrerade med hålen i ostskivorna (figur 8.2). I modellen kan var och en av skivorna med hål i röra sig i sid- och höjdled, vilket innebär att det kan inträffa att barriärerna intar ett sådant läge att en utlöst riskkälla eller hot inte ”fångas upp” av någon av de barriärer som konstruerats för att bryta förloppet, vilket i nästa steg leder till negativa konsekvenser på systemet och dess omgivning.

Hålen och rörelserna orsakas av s.k. aktiva fel och latenta förhållanden. Medvetna fel och fel med avsikt att skada kan naturligtvis också i hög grad bidra till att barriärerna inte fyller sin funktion.

Aktiva fel är fel som personer gör i direkt kontakt med processen – det kan t.ex. vara en operatör som trycker på fel knapp p.g.a. förväxling eller felbedömning. Det aktiva felet utlöser olyckan/krisen, men det är ofta kontraproduktivt att skylla händelsen på operatörens fel. Människor gör fel. System måste konstrueras så att ett mänskligt fel eller en kombination av några mänskliga fel inte skall kunna utlösa en stor olycka.

Latenta förhållanden är förhållanden som skapats av beslutsfattare och konstruktörer. De har oftast funnits under lång tid före olyckan. De kan bidra till att det aktiva felet görs eller till att det aktiva felet får katastrofala effekter. Latenta fel kan även medföra katastrof utan något aktivt fel (t.ex. Challengerolyckan). Typer av latenta förhållanden är:

- Dålig utformning av människa – tekniksystem.
- Brister i ledningen.
- Brister i underhållet.
- Brister i utbildning och träning.
- Icke-adekvata verktyg/hjälpmedel.

En organisatorisk olycka kan således ha sitt ursprung i strategiska beslut och processer i organisationen som budgetering, annan allokering av resurser, planering, schemaläggning, kommunikation, ledning, revisioner m.m. – processer färgade av organisationskulturen, speciellt säkerhetskulturen. Under olyckliga omständigheter, oftast inkluderande aktiva fel, fungerar plötsligt inga barriärer och olyckan är ett faktum – under mycket olyckliga omständigheter blir det en svår påfrestning.

För en proaktiv krishantering är det viktigt att identifiera de beslutsfattare/beslutande organ som kan påverka ett händelseförlopp som kan sluta i en svår påfrestning. Eftersom vi inte kan förutse allt – speciellt svårt är det med komplexa system – måste vi också skapa adaptiva system med återkopplingar/lärande som är mindre känsliga för störningar och snabbt styr mot ett säkert mål. Goda ledningssystem och en god säkerhetskultur är viktiga ingredienser.

8.1.2 Interdependens i tekniska infrastruktursystem; speciellt el- och vattenförsörjning

En mycket viktig undergrupp av förhållanden som kan leda till svår påfrestning av typ 1 är komplexitet och interdependens i tekniska infrastruktursystem. Låt oss betrakta infrastrukturen för el- och vattenförsörjning. Elenergi- och vattenförsörjningen är vitala för samhällets förmåga att fungera. En allvarlig störning på något av dessa system innebär en krissituation som kan ha stora konsekvenser för samhället. Störningen på systemet kan ha mycket olika bakgrund, allt ifrån terrorism och sabotage till tekniska kollapser, naturkatastrofer eller angrepp på informations- och automationssystem. Det finns en mycket nära koppling mellan el- och vattenförsörjningen samt tele- och IT-stöd.

8.2 Grundläggande orsaker till svåra påfrestningar enligt typ 2: naturkatastrofer

Samhällets krisberedskap och krishantering har historiskt sett haft denna typ av svåra påfrestningar som ett av sina huvudansvar. Metodiken att klara dess uppgifter är väl utprovad och beskriven i ett mycket stort antal publikationer. Avseende den förebyggande fasen (mitigation) av krishanteringen utgör FEMA (1997) ett mycket gott exempel på framtagen vägledning.

Vi nöjer oss med att här mycket kort redovisa de huvudsakliga dragen i ett examensarbete från 2001, där Andersson och Kinnerberg (2001) behandlar naturkatastrofers bidrag till riskbilden i EU. Med begreppet katastrof avses i det refererade arbetet situationer där de lokala räddningsresurserna har varit otillräckliga eller då konsekvenserna överstigit vissa nivåer. Naturkatastrofer delas in i följande kategorier: laviner, stormar och tornados, skogsbränder, jordbävningar, vulkaner och skred, dammbrott, översvämningar och flodvågor, torka, och slutligen värmeböljor.

Bland de slutsatser som drogs från arbetet kan nämnas att antalet naturkatastrofer ökar över tiden och ökningen kan förväntas fortsätta i framtiden, att översvämningar och flodvågor samt stormar och tornados är de två kategorier av naturkatastrofer som är vanligast förekommande inom EU, att jordbävningar, vulkaner och skred samt extremtemperatur är de kategorier av naturkatastrofer som kräver flest liv per inträffat tillfälle, samt att utvecklingen medför att samhället blir alltmer sårbart p.g.a. fler avancerade tekniska system och ökad bebyggelse.

8.3 Grundläggande orsaker till svåra påfrestningar enligt typ 3: terrorism och andra typer av avsiktlig påverkan eller skada

Avsiktliga attacker mot exempelvis infrastrukturer kan bara avvärjas om hotet upptäcks i tid och/eller försvarsmekanismer byggts upp som neutraliserar hotet. Självklara begränsningar i tillgängliga resurser innebär, i kombination med den mycket breda hotbilden, att prioriteringar måste göras, d.v.s. kvantifiering i någon form är nödvändig. Problemet är att för ett givet system kategorisera spektrat av existerande hot, finna systemets svagaste punkter och prioritera insatser för förstärkning.

I stort sett omedelbart efter 11 september 2001 påbörjade i USA de ledande vetenskapsakademierna, National Academy of Sciences,

National Academy of Engineering och Institute of Medicine, koordinerade av National Research Council (NRC, 2002) en utredning om de tre frågeställningarna:

- Hur identifieras hotbilden?
- Hur identifieras systemets svagaste punkt eller länk?
- Hur prioriteras användning av tillgängliga resurser för att förstärka systemet?

Ett annat perspektiv var att klargöra hur vetenskap och teknologi kan användas för att förstärka försvaret mot terrorism samt de FoU-insatser som bör prioriteras. Utredningen, som hade stora personella resurser till förfogande, delade in arbetet i följande hot/riskområden:

1. Nukleära och radiologiska hot.
2. Smittsamma sjukdomar och spridning av farliga biologiska gifter.
3. Toxiska kemikalier och explosiva ämnen.
4. Informationsteknologi.
5. Energisystem.
6. Transportsystem.
7. Urban bebyggelse och fasta infrastruktursystem.
8. Terrorhandlingar och allmänhetens reaktion.
9. Komplexa och interdependenta system.

För varje delområde gjordes en genomgång av hotbilden, en lägesbeskrivning av sårbarheten, konkreta åtgärder för att minska densamma, en bedömning av vetenskapens och teknologins roll i sammanhanget samt förslag till utvecklingsåtgärder. För en utförlig beskrivning hänvisas till ursprungsreferensen (NRC, 2002).

8.4 Fenomenet extrema händelser

Begreppen ”extrem händelse” och ”svår påfrestning” har en tydlig koppling. I detta avsnitt diskuteras därför generellt ”extrema händelser” både i avseendet att den utlösande orsaken till den slutliga skadan i sig är av katastrofal storlek och/eller extrem natur (typexempel naturkatastrofer) samt förlopp där den slutliga konsekvensen är av extrem natur.

”Extrema händelser” (vilket kan omfatta samtliga tre typer av grundorsaker till svåra påfrestningar) definieras genom att vara sällsynta, ha mycket allvarliga konsekvenser och vara utanför vad som normalt förväntas inträffa inom systemet ifråga. Detta innebär inte nödvändigtvis att de fysiska skadorna i sig är katastrofala; verkan kan förstärkas och förstoras i det allmänna medvetandet genom att händelsen förknippas med en hög grad av fruktan, osäkerhet och ofrivillighet.

Extrema händelser orsakas ofta av icke-linjära fenomen sådana att en relativt liten ändring i en ingångsparameter leder till en stor ökning i konsekvenserna. Byggnadskollapser, dammbrott, härdsmälta i kärnreaktor är exempel på extrema olyckor där en liten ökning i en miljöfaktor (belastning, vattennivå, härdtemperatur) kan resultera i en snabb övergång från en nästan-olycka till en katastrof. Synergistiska effekter är ofta medverkande: vattenmättad mark i kombination med nya kraftiga regn leder till att en ”normal” översvämning blir katastrofartad. Sociala gruppers beteenden kan ibland modelleras som icke-linjära, dynamiska förlopp av den typ som nämnts ovan.

Litteraturen om extrema händelser och metoder för riskanalys är omfångsrik; vi nöjer oss med att referera den översikt som gavs i Bier et al (1999). Författarna påpekar att extrema händelser allvarligt testar den traditionella riskanalysens användbarhet och värde som beslutsunderlag. Speciellt bekymmersam är avsaknaden av tillförlitliga indata, särskilt vad gäller olika felorsakers frekvens. Sett mot bakgrund av riskanalysens generella målsättning att ge en sannolikhetsfördelning för möjliga skador/konsekvenser är detta naturligtvis ett problem. Bier et al. påpekar att analysen kan förenklas till att bestämma sannolikheten för ett tröskelvärde; d.v.s. ett enstaka, diskret värde. Som exempel kan nämnas bankkonkurs. Vet vi att en förlust av en viss storlek leder till ett sammanbrott behöver vi inte bekymra oss om sannolikheten för en konsekvens av ännu större förluster. Samma resonemang kan naturligtvis appliceras på en mängd analysområden.

I referensen diskuteras riskanalysens allmänna praktiska användbarhet i generella termer och dessutom beskrivs metoder att förbättra giltigheten. Exempel på sådana metoder är extremvärdesteori, Bayesiansk uppdatering av sannolikheter, metoder att behandla imprecisa sannolikheter, systematisk känslighetsanalys, identifiering av scenarier via metoder som bygger på dekomposition av det aktuella systemet etc.

8.5 Några teorier om krisers orsaker och uppkomst: sambandet riskhantering – krishantering

Det ramverk för krishantering som visas i figuren 4.2 bygger på en helhetssyn som växt fram under det senaste årtiondet. Figuren demonstrerar en process i fyra olika steg eller faser. Krishanteringen har traditionellt varit koncentrerad till faserna 2 – 4 medan fas 1, som väsentligen är en process för risk- och sårbarhetsanalys, ofta har spelat en undanskymd och implicit roll. Till detta har säkert bidragit att två grundläggande frågor får anses outredda:

- I vilken utsträckning kan effekten av stora olyckor och katastrofer över huvud reduceras genom preventiva åtgärder?
- Hur åstadkoms en optimal avvägning mellan åtgärder som hör till fas 1 och åtgärder som definieras av faserna 2 – 4?

Med utgångspunkt från de ”situationer” som anges i 3 § av förordning 2002:472 skall vi här översiktligt försöka skissera den vetenskapliga basen för en diskussion kring frågeställningarna ovan.

Grovt förenklat kan vi urskilja fyra teoribildningar om orsaken till att olyckor och katastrofer inom främst teknologiska system uppkommer.

- Reason’s ”schweizerostmodell” som skisserades i avsnitt 8.2.
- Perrow’s ”Normal Accident Theory” (NAT) redovisad i standardverket från 1984 och i en reviderad version från 1997 (Perrow, 1984; Reason, 1997).
- Modell för ”High Reliability Organisations” (HRO), (La Porte, 1981).
- Turners arbete om ”Man-Made Disasters” och ”Disaster Incubation Theory” (DIT) från 1978 och 1996 (Turner och Pidgeon, 1997).

Ovanstående referenser hänvisar bara till vissa ursprungsarbeten, för andra nödvändiga referenser och en introduktion hänvisar vi till Rijpma (2003).

Perrow’s NAT introducerade den nu välkända hypotesen att stora olyckor är oundvikliga i vissa teknologiska system. System kännetecknade av en interaktiv komplexitet och en tät koppling mellan systemdelarna har denna egenskap. Komplexiteten orsakar oundvikliga och oväntade interaktioner mellan oberoende felkällor. Den täta kopplingen medför att initiella störningar snabbt eskalerar till ett systemsammanbrott.

HRO-skolan intar en nära nog diametralt motsatt attityd: det är fullt möjligt att utforma organisatoriska åtgärder och strategier som i stort sett eliminerar sannolikheten för uppkomst av stora olyckor. Denna

slutsats är baserad på undersökningar av och observationer från aktiviteter/organisationer som flygledarcentraler, hangarfartyg och elektrisk kraftproduktion. Fyra egenskaper definieras som karakteristiska: ledningen ser säkerhet och tillförlitlighet som en prioriterad uppgift; tillräcklig redundans i tekniska och personella resurser för att kompensera uppkomna fel; en stark organisationskultur på området tillförlitlighet och, slutligen, ett kontinuerligt organisatoriskt lärande med erfarenhetsåterföring och proaktiva simuleringsövningar.

Turners grundläggande tes (DIT) är att katastrofer framkallas av oförmågan att insamla och tolka information och varningssignaler samt att med utgångspunkt från dessa förutse framtida händelser. Under lång inkubationsperiod ignoreras eller missförstås signaler om framtida hot och faror till dess att katastrofen inträffar. Fast grundad övertygelse om att ingenting kan gå fel kombinerad med fragmentarisk information och en svag och otillräcklig ledningsfunktion leder förr eller senare till en olycka. Ackumulerings- eller inkubationstiden kan sträcka sig över många år.

De olika teoriansatserna ovan ger upphov till olika strategier för förhindrande av uppkomst av svåra påfrestningar och för att minimera den totala skadeeffekten. Som antytts är det ännu outrett vilken teori som bäst ”förklarar” uppkomsten av de situationer som beskrivs i 3 § i förordning 2002:472. Några allmänna slutsatser kan emellertid dras.

- Tre av hypoteserna ovan (Reason, HRO, DIT) innebär en betoning av metoder/åtgärder av typen risk- och sårbarhetsanalyser, kontroll och tillsyn, organisatoriska ledningssystem och revisionsmetoder, förbättring av säkerhetskultur. Innebörden är en ökad betydelse av åtgärder inom ruta 1 av figuren 4.2. Om NAT-synsättet visar sig vara bästa förklaringsgrunden ökar i motsvarande grad betydelsen av faserna 2 – 4 i figur 4.2.
- Den utveckling som antyddes i avsnitt 4.2.3 avseende 2000-talets kriser antyder att förmågan till effektiva förebyggande åtgärder kan komma att bli mer begränsad, d.v.s. faserna förberedande, akut avhjälpande och återställande ökar i betydelse.
- Den för författarna avgörande slutsatsen är emellertid denna: Vid analys av många stora olyckor har man funnit att management och organisatoriska förhållanden (inklusive säkerhetskultur) haft avgörande betydelse för olyckornas uppkomst, t.ex. Bhopal (1984), Tjernobyl (1986), Herald of Free Enterprise (1987), King’s Cross-stationen (1987), Estonia (1994) och diskoteksbranden i Göteborg (1998).

Management och organisatoriska förhållanden kan påverka sannolikheten för olycka med flera 10-potenser (Kirwan, 1994). Vi kan inte vänta på att få mer kunskap från katastrofer av dessa magnituder utan måste av etiska skäl arbeta proaktivt. Brister i ledningssystem, management och organisatoriska förhållanden måste åtgärdas.

8.6 Några slutsatser vad gäller risk- och sårbarhetsanalys enligt förordning 2002:472

Av kapitel 8 kan vi dra åtminstone följande slutsatser:

- De tre olika grupperna av risker och hot som beskrivits ovan bör enligt författarna samtliga behandlas i risk- och sårbarhetsanalyserna om dessa skall kunna användas som beslutsunderlag. De kräver också olika åtgärdsstrategier. Oerhört förenklat kan påstås att typ 1 motverkas genom att det normala riskhanteringssystemet fungerar, typ 2 genom att samhällets totala krishantering är effektiv, typ 3 genom speciella åtgärder som förstärkning av skydd mot intrång, etc.
- Författarna vill framhålla den uppenbara länken mellan generell riskhantering och krishantering avseende risker och hot av typ 1 ovan.

9. Standards samt ramverk för riskhantering

Vi har tidigare konstaterat (avsnitt 8.1) att det vore en fördel om myndigheters evaluering av sannolikheten för uppkomst av en svår påfrestning byggde på en bedömning av ifrågavarande verksamhets totala riskhantering.

Generella krav på svenska myndigheters riskhantering har fram till nu bestämts av förordningen 1995:1300 *om statliga myndigheters riskhantering* som bl.a. innehåller följande passus:

"Riskanalys och skadeförebyggande åtgärder

3 § Varje myndighet skall identifiera vilka risker för skador eller förluster som finns i myndighetens verksamhet. Myndigheten skall värdera riskerna och beräkna vilka kostnader som staten har eller kan få med hänsyn till dessa risker. Resultatet skall sammanställas i en riskanalys. Varje myndighet skall vidta lämpliga åtgärder för att begränsa risker och förebygga skador eller förluster."

Det huvudsakliga syftet med förordningen tycks vara att reglera myndigheternas riskfinansiering och speciellt då försäkringsfrågor. Vi har funnit få exempel på att förordningen använts för att organisera och genomföra en myndighets riskhantering i vid bemärkelse.

Författarna anser att statens passivitet ter sig förvånande om man noterar den aktivitet som rått internationellt främst under den senaste 5-årsperioden. I en rad länder har statsmakten (ofta i samarbete med näringslivet) producerat vägledningar, standards, etc. för organisationernas riskhantering. Vi nöjer oss här med att hänvisa till dokument från Storbritannien. I förordet till rapporten från Strategy Unit (2002) konstaterar premiärministern bl.a.:

"The report sets out how government should think about risk, and practical steps for managing it better. It proposes principles to guide handling and communication of risks to the public – on which we are seeking views from all interested parties."

Risk management – getting the right balance between innovation and change on the one hand, and avoidance of shocks and crises on the other – is now central to the business of good government.

Samtidigt kan påpekas att Svenska Kommunförbundet bl.a. genom sin vägledning ”Verksamhetsanalys och säkerhetssamordning” (Kommunförbundet, 2001) har lagt grunden för en förbättrad riskhantering på det lokala planet.

Nedanstående mycket kortfattade sammanfattning av existerande vägledningar på området är främst hämtade från dokument utfärdade av ministerier i Storbritannien (eller av kabinettet). Bland källorna kan nämnas:

- Strategy Unit report – ”Risk: Improving government’s capability to handle risk and uncertainty” (Strategy Unit, 2002).
- HM Treasury – ”Management of Risk – A Strategic Overview” (Orange book) (HM Treasury, 2001).
- UK Department for Environment, Food and Rural Affairs — ”Risk Management Strategy”, (DEFRA, 2002).

Det bör nämnas att utvecklingen på myndighetsområdet har föregåtts av motsvarande utveckling inom näringslivet. Ett aktuellt exempel utgörs av:

- The Committee of Sponsoring Organizations of the Treadway Commission – *Enterprise Risk Management Framework*, (COSO, 2003).

9.1 Vad är ett ramverk för riskhantering?

Vi har tidigare visat ett ramverk för krishantering, se avsnitt 4.2. Dessutom påpekade vi i kapitel 1 och avsnitt 6.2 att formuleringen av krisberedskapsförordningens § 4 föranleder att de myndigheter som omfattas av paragrafen rimligen bör ha etablerat ett ramverk för riskhantering för att intentionen i paragrafen skall kunna anses uppfylld.

En organisations strategi för riskhantering måste vara konsistent och balanserad över organisationens totala verksamhetsområde. Ett ramverk för riskhantering definierar den kontext inom vilken risker hanteras: hur de identifieras, analyseras, kontrolleras, övervakas och bedöms i en fortgående revisionsprocess. Ramverket måste vara konsistent med och förankrat i de processer som ingår i den kontinuerliga ledningen av organisationen; det beskriver hur:

- risker identifieras
- information hämtas in beträffande sannolikhet och potentiella utfall

- de kan kvantifieras eller rangordnas med hänsyn till osäkerheter och tillgång till expertråd
- möjliga metoder att hantera riskerna identifieras
- riskbeslut fattas
- riskbeslut implementeras
- effektiviteten av olika åtgärder/beslut utvärderas
- lämpliga kommunikationsmekanismer sätts upp och implementeras.

Det sätt på vilket olika myndigheter behandlar sina risker är naturligtvis delvis unikt. Det finns emellertid ett antal element som alla myndigheter behöver förbättra för att effektivisera sin riskhantering; se figuren 9.1 nedan:

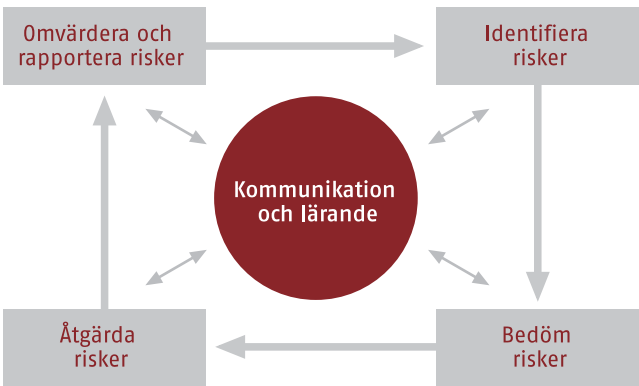
Figur 9.1 *Ramverk för att hantera risk och osäkerhet. (Översättning från Strategy Unit, 2002)*

En uppföljning av elementen i ramverket innebär bl.a.

- att alla stora policy- och programbeslut tar explicit hänsyn till risk-aspekten och balansen risk/nytta
- att system, processer och incitament för en effektiv riskhantering finns tillgängliga
- att det finns mekanismer för att säkerställa att risker hanteras på den nivå detta sker mest effektivt

- att en riskhanteringskompetens skapas bland beslutsfattare och experter
- att klara kvalitetsstandards och kvalitetssäkringsmetoder har införts
- intern och extern kommunikation om valda metoder att hantera risker bidrar till att öka anställdas och allmänhetens förtroende för fattade beslut
- att hela processen drivs och kontrolleras från myndighetens högsta ledning.

Elementen i figur 9.1 ovan kan lämpligen konkretiseras i ett cykliskt ramverk för riskhantering, se figur 9.2 nedan.



Figur 9.2 *Process för riskhantering*
(Översättning från Strategy Unit, 2002)

9.2 Riskhanteringens tre nivåer, speciellt behandling av strategiska risker

Författarna anser att myndigheter i enlighet med modellen från Storbritannien måste kunna hantera risk på åtminstone tre nivåer: strategisk nivå, program/projektnivå och operativ-/anläggningsnivå. Figur 9.3 nedan illustrerar riskhierarkin med en indikation på osäkerheter förknippade med de olika nivåerna.

Figur 9.3 *Olika nivåer av riskhantering. (Översättning från Strategy Unit, 2002)*

Risk- och sårbarhetsanalyser på de olika nivåerna kommer att diskuteras i del II av detta dokument, här ges bara några kommentarer till begreppet ”strategiska risker”.

Allmänt innebär en god riskhantering på denna nivå att ledning och styrelse kan påvisa att policybeslut och andra viktiga beslut fattas efter en strukturerad och väl underbyggd analys av risker och osäkerheter förknippade med de olika alternativen för handlande. I krishanteringssammanhang avser dessutom ett beaktande av strategiska risker bl.a. att procedurer finns för att säkerställa att risker på lägre nivå inte eskalerar till den nivå som beskrivs i 3 § av förordningen 2002:472 samt att krishanterings- och krisberedskapsaspekter beaktas vid val av policyalternativ. Detta innefattar planering för att kunna upprätthålla kritiska aktiviteter, exempelvis kontinuitetsplanering och insatsplanering, samt för att kunna hantera frågor som rör relationen till allmänheten, exempelvis förtroende och trovärdighetsaspekter. Vid utvärderingen av krishanteringens och krisberedskapens effektivitet bör speciellt dominoeffekter av risker och sårbarhet inom andra myndigheters ansvarsområden beaktas.

9.3 Några kommentarer till den generella riskhanteringsprocessen

Nedan följer några kortfattade kommentarer till figurerna i kapitel 9.1.

Etablera ramverket

Minimikraven på ett ramverk för riskhantering är att:

- fastställa myndighetens riskpolicy
- identifiera huvudsakliga problemägare och övriga berörda personer
- klarlägga målsättningen för riskhanteringen
- definiera metoder/angreppssätt för att identifiera risker, bedöma och avrapportera dessa, olika typer av åtgärder
- definiera ansvar för riskhanteringen och avrapportering till högre ledningsnivå. Speciellt gäller detta risker som skär tvärs över enheter av myndigheter
- etablera metoder för kvalitetssäkring som säkerställer att riskhanteringen följer god sed för sådan säkring.

Det är dessutom viktigt att identifiera ”ägare” till/ansvariga för

- att policydokument produceras
- riskhanteringsprocessen på olika nivåer – strategisk nivå, programnivå och operativ nivå
- genomförande av fattade riskhanteringsbeslut
- interdependenta risker som skär tvärs över myndigheten.

Identifiera riskkällor, främst för myndighetsintern verksamhet

Risker som inte blir identifierade blir inte heller analyserade. Riskidentifieringen är alltså avgörande för riskanalysens kvalitet. Vi kommer senare att ange ett antal checklistor för samma ändamål. Vi nöjer oss här med att ange ett antal mycket allmänna kategorier av risk hämtade från HM Treasury (2001). Jämför också med de riskkategorier som anges i figur 6.1.

	Kategorier	Exempel
A. EXTERNA		
1.	Infrastruktur	Samtliga försörjningssystem
2.	Ändringar i ekonomiska förhållanden	Faktorer som inflation, räntenivå
3.	Lagstiftning	Ökade omkostnader
4.	Miljö	Ökade omkostnader
5.	Politiska förhållanden	Ny regering
6.	Marknaden	Konkurrensförhållanden
7.	Externa yttre händelser	Brand, översvämning, extrema väderförhållanden
B. FINANSIELLA		
8.	Budgetmässiga	
9.	Bedrägerier, stöld	
10.	Försäkringar	
11.	Investeringsbeslut	Felaktiga beslut
12.	Ansvarsfrågor	Möjligheten att stämma eller bli stämd
C AKTIVITETER		
13.	Policy	Kvalitet på policybeslut
14.	Operativa risker	Rutiner och instruktioner för att fullfölja vissa uppgifter
15.	Information	Kvalitet på information
16.	Anseende, tilltro	
17.	Transfererade risker	Felaktiga beslut i försäkringsfrågor
18.	Teknologi	Användning av fel teknologi eller felaktig användning av teknologi
19.	Projekt	Relaterade till projektplanering och ledningsprocedurer
20.	Innovation	Felaktig exploatering
D MÄNSKLIGA RESURSER		
21.	Personal	Förlust av nyckelpersoner
22.	Hälsa och säkerhet	

Tabell 9.1 Kategorier av risk (från HM Treasury, 2001)

De uppräknade riskkategorierna är inte oberoende och naturligtvis inte heltäckande. Det kan dessutom i praktiska fall vara tveksamt om en aktivering av riskkällan över huvud taget kan leda till en process som eskalerar till en kris.

Identifiera riskägare

Betydelsen i riskhanteringsprocessen ligger inte bara i att identifiera de problemområden dit resurser måste tillföras i riskhantering, utan också i att formellt ansvar tilldelas för identifierade risker. Innebörden är att en delegering måste ske till lämplig person på lämplig ledningsnivå och att detta dokumenteras. Organisationen bör alltså etablera en seniorstruktur för ägande av identifierade risker.

Evaluera riskerna

Riskevaluering innebär att bedöma sannolikhet och påkänning på organisationen/verksamheten från individuella risker med hänsyn tagen till interdependenser eller andra faktorer inte omedelbart förknippade med den ursprungliga riskkällan. För några typer av risker, som finansiella risker och vissa säkerhetsrisker från storskaliga teknologiska anläggningar kan numeriska värden ansättas, emedan de flesta, som exempelvis negativ publicitet, bara kan beskrivas subjektivt. Det rekommenderas att resultatet redovisas i en s.k. riskmatris , se exempelvis figur 14.2.

I figur 14.2 bedöms konsekvenserna av en svår påfrestning dock endast med avseende på hälsa, miljö och ekonomi. För vissa verksamheter är det rimligt att anta att ett antal konsekvensdimensioner får tillföras, beroende på analyserad risktyp och medföljande skade- eller påkänningstyp. De flesta myndigheter torde kunna gruppera sina riskkonsekvenser i några av följande grupper:

- Politiska (t.ex. besvärande interpellationer i riksdagen)
- Finansiella (smittspridning medför skadeståndsansvar för slaktade djur)
- Sociala (t.ex. långvariga avbrott i viktiga grundläggande försörjningssystem, ryktesspridning till följd av salmonella)
- Operativa (CSN exempelvis, service kan ej levereras)
- Juridiska (skadestånd)
- Miljö
- Rykte, anseende (förlust av allmänhetens förtroende)

Denna kategoriuppdelning av konsekvenser återkommer i figur 13.1.

Acceptabel risk

Skapandet av en riskprofil möjliggör en meningsfull diskussion om huruvida en riskkälla är acceptabel eller måste åtgärdas. Beslutet kommer vanligtvis att bero på den upplevda betydelsen av den identifierade

risken och är därmed i hög grad politiskt. Är det exempelvis fråga om en begränsning i serviceutbudet och vilken exponering myndigheten kan acceptera avgörs detta, förutom av den skada och det besvär som åsamkas allmänheten, av ett antal parametrar såsom effekten på övriga delar av organisationen, värnandet om myndighetens anseende, politiska följder etc.

Respons på risk

Med riskprofilen som bakgrund kan lämpliga åtgärder diskuteras. Dessa kan delas in i fyra kategorier.

Överföra För vissa risker kan den optimala åtgärden vara en transferering. Detta kan åstadkommas genom försäkring eller genom att betala en tredje part för att ta ansvar för risken.

Tolerera Förmågan att göra något åt riskkällan med tillgängliga resurser kan vara begränsad eller riskminskningen inte proportionell mot kostnaden.

Åtgärda Det absolut största antalet identifierade risker hör hit. Målsättningen är vanligen inte att eliminera riskkällan utan att hålla risken på en acceptabel nivå. Organisationens aktiviteter med detta syfte kallas ”internkontroll”.

Avslut Några risker förknippade med en specifik aktivitet är av sådan natur att de kan hanteras bara genom att aktiviteten upphör. Jfr dock exempelvis räddningstjänst, ordningsmakt.

Utvärdering av åtgärd

När ett ramverk har utvecklats och kontrollåtgärder satts in är det viktigt att åtgärdernas effektivitet utvärderas. Det rapporteringssystem och det system för egenkontroll som är nödvändigt utgör en betydelsefull del av säkerhetsledningssystemet, se vidare avsnitt.

9.4 Exempel på strategiskt ramverk: begreppet säkerhetsledningssystem

Vi har tidigare framhållit att ledningssystem för säkerhet utgör ett viktigt element i riskhanteringsarbetet såväl för den myndighetsinterna verksamheten som ute i verksamheter som står under myndighetens tillsyn/kontroll. Detta gäller främst påfrestningar av typ 1 enligt avsnitt

8.1. Bakgrunden är givetvis att flera analyser och utredningar av tidigare inträffade svåra olyckor/påfrestningar har visat att brister i ledning av verksamheten är en av de vanligaste bidragande orsakerna. I följande citat från Kemikontoret (1997) ges en motivering till varför ledningssystem för dessa frågor är en nödvändighet för företag inom kemisk industri, en beskrivning som mycket väl kan överföras till myndighetssektorn:

"Att styra SHM[1]-frågor i ett företag på ett professionellt sätt bör vara lika självklart som att styra produktions-, marknads-, personal- och ekonomifrågor. Därför behövs formella system och verktyg för detta bland företagets övriga övergripande ledningssystem.

SHM-frågorna finns ofta mer eller mindre formellt reglerade i ett företag, ofta genom spridda instruktioner eller kanske en övergripande policy. En del företag har genom långvarig tradition byggt upp en kultur inom ett eller flera av SHM-områdena.

För flertalet företag finns ett behov av att samla och reglera SHM-frågorna på ett strukturerat sätt i ett härför särskilt utarbetat system."

Uppbyggnaden av ett ledningssystem inom olika områden kan se ut på många olika sätt och vi redovisar här endast en mycket övergripande struktur från Kemikontoret (1997).

"Ett SHM-ledningssystem bör byggas upp enligt principen:

1. *Policy*
2. *Rutiner*
3. *Instruktioner*

Policyn anger företagets övergripande syn och mål inom området. Rutinerna ger en klar uppfattning om vad som skall göras och i allmänhet också när, var, hur och av vem. I vissa fall behöver rutinerna kompletteras med detaljerade instruktioner om framför allt hur och av vem aktiviteter skall utföras. I vissa fall kan det vara lämpligt att beskriva systemet övergripande i en s k manual eller att samla rutinerna i en handbok."

I Abrahamsson & Magnusson (2004) exemplifieras ett strategiskt ramverk för riskhantering, där ledningssystem för säkerhet utgör en grundförutsättning, genom att kortfattat referera innehållet i ett EU-direktiv om allvarliga olyckshändelser på kemikalieområdet (Seveso II-direktivet).

1. Kemikontorets handbok avser ledningssystem för Säkerhet, Hälsa och Miljö, SHM. Principen är densamma även om ledningssystemet inte omfattar just dessa tre områden.

Exemplet ovan är hämtat från industrins riskhantering. Författarna anser det naturligt att myndigheter gör motsvarande insatser för att kontrollera sina risker.

9.5 Sammanfattning av kapitlen 1–9

Ett försök att sammanfatta hittills diskuterat material följer.

1. Vi har valt att dela in grundorsakerna till svåra påfrestningar i tre kategorier eller typer:
   - Typ 1 kan betecknas ”organisatoriska” olyckor.
   - Typ 2 är huvudsakligen naturkatastrofer av olika slag.
   - Typ 3 utgörs av terroristangrepp och andra typer av påverkan med avsikt att skada.

2. Det till regeringskansliet inlämnade materialet bör enligt författarna omfatta:

   - Risker i myndighetsinterna aktiviteter.
   - Risker förknippade med externa verksamheter under myndighetens tillsyn och kontroll. Bedömning av effektivitet i föreskrifter och kontroll- och tillsynsprocessen avseende att förhindra uppkomst av svår påfrestning bör ingå.
   - Risker förknippade med externa aktiviteter och skeenden utanför myndighetens ansvarsområde men som kan påverka myndighetens ansvarsområde, exempelvis internationella politiska förhållanden, snabba marknadsförändringar, naturkatastrofer, utslagning av försörjningssystem och funktionssvikt hos andra myndigheter.

   De tre analysområdena kan givetvis vara beroende och överlappande. Med ”risker” avses ovan risker med potential att vara åtminstone en bidragande orsak till att en svår påfrestning uppkommer.

3. Det kan enligt författarna vara ändamålsenligt att gruppera risker/riskkällor i en riskhierarki: strategiska risker, program-/projektrisker samt operativa risker/risker knutna till ett specifikt tekniskt system eller teknisk anläggning.

   Orsaken till indelningen är att riskidentifieringsprocessen på de tre olika nivåerna åtminstone delvis kräver olika metodik och medverkan av personal på olika nivåer. Indelningen förutsätter att risker på lägre nivå vid en viss storlek behandlas på högre nivå.

4. Som den definieras i figuren 4.1 är krishanteringens första fas, den förebyggande fasen (mitigation), grundläggande för den totala processen. I denna första fas ingår identifiering, bedömning och rangordning av riskkällor, liksom evaluering av risk- och sårbarhetsreducerande åtgärder. Formuleringen ovanför utgör den sedvanliga definitionen på ”normal” riskhantering och återfinns till stora delar i 4 § i förordning 2002:472. Implikationen är att denna krishanteringens första del, åtminstone vad gäller risker av typ 1, förutsätter en väl fungerande generell riskhanteringsprocess hos myndigheten. De risker som avses är fortfarande sådana med potential att vara åtminstone en bidragande orsak till att en svår påfrestning uppkommer. Vidare är det givetvis så att den totala krishanteringen kräver processer och rutiner utöver den ordinarie riskhanteringen. Författarna anser att § 4 implicit innebär ett krav på väl fungerande risk- och krishanteringsprocesser med tillhörande ledningssystem och rutiner för kvalitetskontroll och internkontroll. I bilaga 1 redovisas exempel på checklistor för evaluering (revision) av nämnda risk- och krishanteringsprocesser.

Del II. Metoder att genomföra risk- och sårbarhetsanalyser

Del II. Metoder att genomföra risk- och sårbarhetsanalyser

I denna del av dokumentet diskuteras översiktligt praktiska metoder att genomföra risk- och sårbarhetsanalyser. Vi följer den riskhierarki som tidigare skisserats med en uppdelning i strategiska risker, program-/projektrisker, risker på operativ nivå och på nivån tekniska system. Att skyddsvärda kapaciteter skall analyseras avseende risker på den lägsta nivån är mer eller mindre självklart. Det är oklart i vilken utsträckning förordningen 2002:472 över huvud har som mål att 3 § skall omfatta de två övre risknivåerna, d.v.s. på strategisk- och program-/projektnivå. Författarna har valt att tolka 3 § som att samtliga risker som synnerligen allvarligt kan försämra förmågan till verksamhet skall beaktas i analysen, d.v.s. även risker på de två övre nivåerna.

Kapitel 10 diskuterar metodik att behandla strategiska risker generellt, kapitel 11 risker på program- och projektnivå som kan leda till en svår påfrestning. Kapitel 12–14 redovisar metoder att analysera risker inom de skyddsvärda kapaciteterna och riktar sig primärt till myndigheter berörda av förordningens 4 §. Kapitel 15 redovisar hur risk- och sårbarhetsanalysens struktur kan förändras när huvudmålet är att beakta avsiktliga hot och attacker samt ger webbadresser till ett antal manualer och vägledningar. Slutligen presenteras i kapitel 16 ett förslag på möjligt innehåll i risk- och sårbarhetsanalyserna enligt förordning 2002:472 samt ges hänvisningar till checklistor för utvärdering av den övergripande riskhanterings- och krishanteringsprocessen.

10. Identifiering och evaluering av strategiska risker

Allmänt om identifieringsprocessen

På denna nivå kan olika riskkategorier behandlas med en i stort sett generell metodik. Fokus ligger på att upptäcka och identifiera nyckelrisker avseende fullföljandet av myndighetens huvudsakliga mål och uppgifter, det vill säga bl.a. de risker och sårbarheter som avses i 3 § av förordningen 2002:472. De frågeställningar som bör tas upp avser myndighetens framtida målsättningar, hur dessa skall uppnås och, i extremfallet, hur den framtida existensen skall säkras. Risker och sårbarheter på denna nivå hotar funktionen hos viktiga delar av myndigheten. Bland riskkategorierna kan nämnas osäkerheter avseende framtida och politiska faktorer, kvaliteten på service till allmänheten, allmänhetens tilltro till myndigheten etc. Risker på lägre nivåer bör vid behov flyttas till den strategiska nivån genom att bedömas mot på förhand definierade eskaleringskriterier, som att skadeverkningar bedöms som oacceptabla, utanför överenskomna gränser, har potential att påverka strategiska målsättningar etc.

Riskidentifieringen kräver kreativitet, påhittighet och ett brett deltagande (inte minst från ledningen) för att säkerställa att nyckelrisker upptäcks. Vanligen krävs en strukturerad omvärldsanalys. Några av de externa faktorer som bör beaktas inkluderar:

Politiska: inflytande från internationella och transnationella myndigheter/regeringar.

Ekonomiska: den nationella och internationella marknaden, globalisering.

Sociala: huvudsakliga demografiska och sociala trender, nivå på medborgarnas engagemang.

Teknologiska: framtida utveckling på viktiga teknologiområden.

Interna faktorer inkluderar kvalitetssäkring av det totala ledningssystemet, speciellt av ledningssystemet för inre kontroll och riskhantering etc., se

vidare figuren 9.1. Riskkategorierna i tabell 9.1 bör kunna tjäna som checklista och utgångspunkt för identifieringsprocessen. Relevansen av riskkategorierna i tabellen varierar givetvis starkt mellan olika myndigheter.

Den krävda omvärldsanalysen kan ske med hjälp av en rad olika metoder, exempelvis:

- Delfipanel (en metod att samla information och bedömningar från expertpaneler).
- Scenariometoder (metoder att framställa och granska möjliga framtida tillstånd).
- Andra typer av workshops och strukturerade gruppdiskussioner.
- Kvalitativa och kvantitativa trendanalyser.

Det existerar en rik litteratur på området, för en översikt se exempelvis ”A Futurists Toolbox” (Performance and Innovation Unit, 2001).

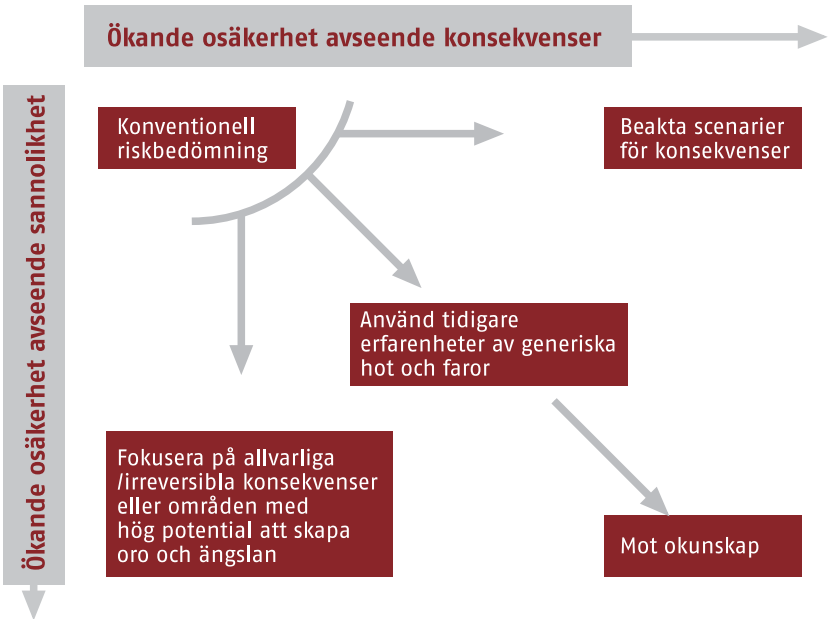
- Evaluering av risk och sårbarhet. Inverkan av osäkerheter

Många av de identifierade riskerna kan bara med stor osäkerhet kvantifieras med avseende på konsekvens och sannolikhet. En avgörande faktor är att det ofta är inverkan av allmänhetens riskperception och utformning av myndighetens riskkommunikation som avgör den slutliga skadans storlek.

Figuren 10.1 nedan, hämtad från Strategy Unit (2002), visar hur en konventionell bedömning av denna typ av risker måste förändras när osäkerheten ökar. Riskkällor som har potentialen att orsaka en svår påfrestning ligger i ytterområdet vad gäller osäkerheter både för sannolikhet och skada. Det kan i sammanhanget vara värt att nämna att den objektiva skadeeffekten kan vara begränsad, men ryktesspridning, inklusive spridning via media, kan ändå medföra en svårartad krissituation (jfr exempelvis SARS och BSE).

För de fall osäkerheterna ter sig hanterbara kan riskmatrisen i figur 14.2 användas för att skapa en riskprofil. Eventuellt kan den kvantitativa matrisen i figur 14.2 ersättas med en kvalitativ sådan där sannolikhet och konsekvens bedöms på exempelvis en tredelad skala (låg, medium, hög).

Den vetenskapliga bakgrunden för att klassificera risktyper, riskevalueringsmetoder och riskhanteringsstrategier sammanfattas mycket kortfattat i bakgrundsstudien (Abrahamsson & Magnusson, 2004); se även de referenser som ges i sistnämnda rapport.



Figur 10.1 *Riskbedömning och osäkerhet (från Strategy Unit, 2002)*

Svår påfrestning genererad genom interdependens mellan myndigheters ansvarsområden

Definitionen av svår påfrestning som *ett tillstånd som kan sägas uppstå när en eller flera händelser gemensamt eskalerar och konsekvenserna av dessa händelser omfattar stora delar av samhället* innebär att potentialen för svår påfrestning ej kan bedömas enbart på grundval av konsekvenserna av att den egna myndighetsfunktionen allvarligt försvagas. Dels måste inverkan på andra myndigheters ansvarsområden beaktas, dels måste den kombinerade effekten av att allvarliga eller extraordinära händelser samtidigt och oberoende inträffar inom annan myndighet studeras.

Worst case scenarios

Eftersom vi här är intresserade av krishanteringsaspekter anser vi att risk- och sårbarhetsanalysen bör bygga på trovärdiga ”worst case scenarios”, jämför med figur 4.2. Återigen är omvärldsanalyser av typen scenarioplanering och ”brainstorming” användbara metoder.

11. Risker på program- och projektnivå

På program- och projektnivå är ledningen ansvarig för att överföra tagna strategibeslut till (nya) metoder och vägar att arbeta för att öka myndighetens nytta och effektivitet. Typiska risker ligger inom det finansiella och organisatoriska området, omfattar säkerhets- och kvalitetsfrågor, processer för krishantering etc. På området projektrisker tillkommer dessutom personella, tekniska, kostnadsmässiga, resursmässiga och kvalitetsmässiga frågeställningar. Andra risker ligger inom området kvalitetssäkring, tillförlitlighet hos underleverantörer, beroendet av samarbete med andra myndigheter och organisationer etc. På programnivå kan en avgörande riskfaktor vara styrning av interdependens och samband mellan de projekt som tillsammans utgör programmet. På projektnivå är dessutom målsättningen att hålla oönskade projektutfall på en minimal nivå. Vikten av att projektriskhantering ingår som en naturlig del i den normala projektledningen uttrycks exempelvis i vägledningsdokument från Project Management Institute (2000).

Liksom för strategiska risker är de huvudsakliga hjälpmedlen strukturerade gruppdiskussioner av typen brainstorming, workshops, Delfipaneler etc. Bl.a. rapporten från Strategy Unit (2002) rekommenderar en kombination av ”top-down”- och ”bottom-up”- metoder; exempelvis att kombinera en risköversyn utförd av seniorledning eller ett speciellt utvalt team med en bedömning genomförd av de direkt involverade och säkerställa att utfallet från den kombinerade bedömningen når myndighetens ledning.

Eventuellt kan riskidentifieringen ovan förbättras med användning av traditionella systemanalysverktyg som beslutsträd, PERT (Program Evaluation and Review Technique) och CPM (Critical Path Method), kostnad/nyttoanalys, Monte Carlo-simulering, influensdiagram etc.

Som avslutning kan sägas att utveckling av praktiskt användbara checklistor för identifiering och evaluering av risker på program- och projektnivå borde vara både möjligt och till mycket stor nytta. Riskkategorierna i tabell 9.1 borde kunna utgöra en utgångspunkt för ett sådant arbete.

12. Förslag på struktur för risk- och sårbarhetsanalyser av exempelvis skyddsvärda kapaciteter

Kapitel 12 riktar sig i första hand till myndigheter som omfattas av 4 § i förordning 2002:472. För att den process som leder till svår påfrestning skall kunna analyseras måste förloppet renodlas och struktureras. Vi har valt att göra detta enligt figur 12.1. Utgångspunkten är att vi studerar en s.k. skyddsvärd kapacitet (se Krisberedskapsmyndighetens forskningsstrategi, KBM 2003c) exempelvis:

- Elektroniska informations- och kommunikationstjänster
- Energiförsörjning
- Transport och logistik
- Vatten och annan livsnödvändig försörjning
- Skydd, undsättning och katastrofmedicin
- Betalningsförmedling och finansiella tjänster
- Tvärsektoriell ledning, information och styrelse
- Hälso- och sjukvård, särskilt medicinsk analyskapacitet

För att göra analysen hanterlig är den normala proceduren att dela upp analysobjektet i ett antal delprocesser eller delsystem. För varje delsystem definieras här en analysprocess med två huvudsteg.

Huvudsteg 1, från R1 till R2 (fig. 12.1)
Inventering av felorsaker, initierande händelser, hot och andra riskkällor som kan starta utvecklingen mot svår påfrestning. Inventeringen omfattar felorsaker av typ A – D enligt figur 8.1 och bör bygga på existerande checklistor och erfarenheter av inträffade händelser. En orsaksanalys klargör potentialen för att starta en händelsekedja som leder till en skade-

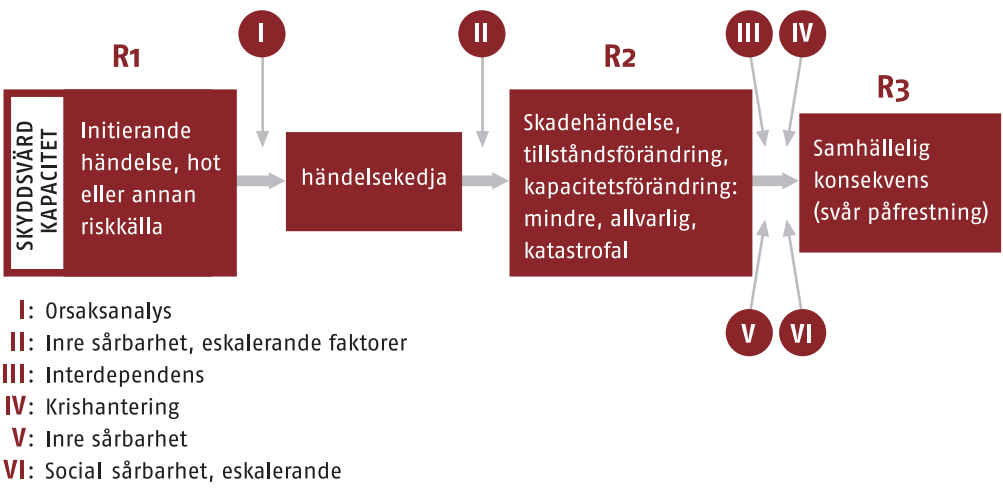
händelse eller tillståndsförändring. Systemets inre sårbarhet avgör skadehändelsens storlek. Vi har valt att definiera tre kategorier av skadehändelser/tillståndsförändringar:

- mindre
- allvarliga
- katastrofala

Vi kommer att återvända till dessa tre kategorier och diskutera hur storleken på skadehändelsen kan komma att påverka den fortsatta analysens utformning. Det bör nämnas att en grundligt genomförd analys av detta steg, som kanske främst riktar sig mot ”typ 1-risker” enligt kapitel 8, är mycket arbetskrävande och oftast faller inom den ”normala” riskhanteringen, se vidare de fem punkterna på nästa sida. Vi har valt att anlägga synsättet att de skadehändelser/tillståndsförändringar som anges i ruta R2 motsvarar de ”situationer” som anges i 3 § i förordning 2002:472.

Huvudsteg 2, från R2 till R3 (fig. 12.1)
innebär att beräkna eller bedöma den slutliga samhällskonsekvensen av skadehändelsen. Bedömningen omfattar eskaleringspotential, inverkan av krishanteringsåtgärder och av den sociala sårbarheten för påfrestningen i fråga.

Figur 12.1. *En möjlig beskrivning av en generisk process som leder till svår påfrestning*



Utvecklingen från det att händelsekedjan startar eller initieras till att en svår påfrestning inträffat är en komplex och interdependent process behäftad med stora osäkerheter. Det går därför inte att med en förenklad figur som figur 12.1 invändningsfritt klargöra skeendet generellt. Figuren får ses som en möjlig beskrivning. Vår förhoppning är att den skall kunna utgöra startpunkten för en mer kvalificerad och detaljerad diskussion av det enskilda fallet. Därvid bör bl.a. punkterna 1 – 5 nedan beaktas.

1. En risk- och sårbarhetsanalys för krishantering startar förmodligen oftast i ruta 2, R2, d.v.s. med utgångspunkten att en skadehändelse eller tillståndsförändring har inträffat, d.v.s. att man befinner sig i en sådan situation som avses i 3 § i förordning 2002:472.
2. Hur processen eskalerar från R1 till R2 studeras, när det gäller krishantering, främst avseende hur systemet påverkas av externa och avsiktliga hot. Denna sårbarhetsanalys kan ha en speciell utformning som vi återkommer till i kapitel 15.
3. Skadehändelsen/tillståndsförändringen i R2 kan i sig själv vara av katastrofal natur; exempel utgör dammbrott och vissa typer av naturkatastrofer (extrema snöfall, etc.).
4. Skadehändelsen/tillståndsförändringen i R2 kan i sig vara av relativt obetydlig omfattning men kan ändå medföra stora konsekvenser i samhället genom exempelvis ryktesspridning, allmänhetens riskperception etc. och därmed utgöra grunden för svår påfrestning. Exempel utgörs av SARS-epidemin, där skadehändelsen i sig var av relativt begränsad omfattning men påverkan på samhället, exempelvis flygindustrin, var enorm.
5. För studier av processer som går från vänster till höger blir metodiken vad som kan betecknas som ”händelseträdsbaserad”, d.v.s. studier av olika tänkbara scenarier från R2 för att bedöma slutliga konsekvenser i R3. Studeras händelser från höger till vänster kan ofta någon form av felträdsanalys användas, d.v.s. man utgår från skadehändelsen i R2 eller de samhälleliga konsekvenserna i R3 och försöker finna den kedja av bakomliggande händelser och orsaker som kan leda fram till dessa skadehändelser och samhälleliga konsekvenser. Om skadehändelsen i R2 i sig är av katastrofal natur borde sådan analys vara relevant för uppfyllelse av förordning 2002:472. En metodik att göra detta med förslag på hur säkerhet, hälsa och miljö kan beskrivas i ekonomiska termer visas i kapitel 14.

Sammanfattningsvis gäller att figur 12.1 ger möjlighet att definiera ett antal procedurer för risk- och sårbarhetsanalys. Ur dessa har vi valt att närmare diskutera två analysfall:

- Att skadehändelsen R2 är av ”mindre” eller ”allvarlig” art och att vi studerar den potentiella eskaleringen från R2 till R3 (kapitel 13).
- Att skadehändelsen R2 i sig innebär en svår påfrestning (är av katastrofal natur) och att vi använder ett mer direkt angreppssätt att identifiera och karakterisera denna (kapitel 14).

Avseende de två ovan angivna analysfallen har vi i kapitel 13 och 14 försökt att beskriva ett par angreppssätt som kan vara användbara för ett antal myndigheter, kanske främst för sådana med begränsad erfarenhet av att producera risk- och sårbarhetsanalyser. Självklart är inte avsikten att på något sätt föreslå att de myndigheter som kanske sedan lång tid har en väl inarbetad och fungerande metodik ersätter eller ändrar denna. Det skall också nämnas att det inte är praktiskt genomförbart och inte heller nödvändigt att föreskriva på metodnivå hur risk- och sårbarhetsanalyserna bör genomföras. Lämpliga metoder varierar beroende på vilken typ av verksamhet som är aktuell. Många myndigheter använder som nämnts ovan redan idag metoder som är väl anpassade till respektive myndighets verksamhetsområde.

De övergripande angreppssätt som skisseras i kapitel 13 och 14 får ses som förslag för analysarbetet under kommande år, samt som underlag för diskussion och vidareutveckling. Givetvis är det av vikt att ta tillvara de praktiska erfarenheter som erhålls vid myndigheternas analysarbete under de kommande åren för att styra den vidare metodutvecklingen.

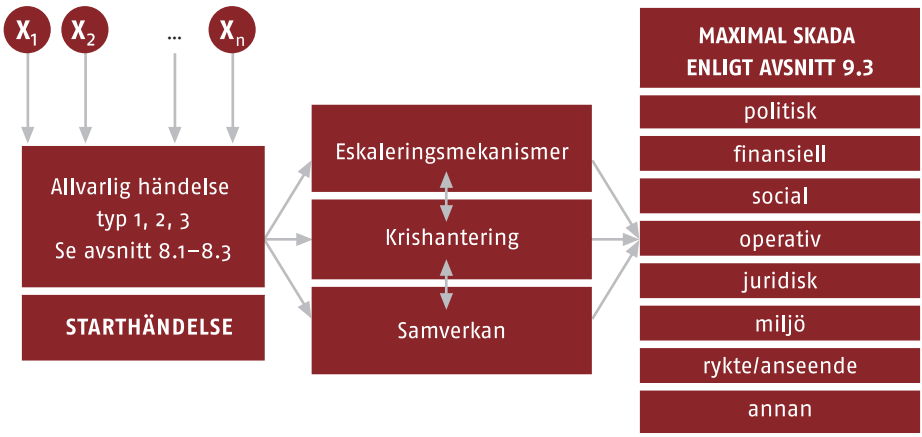
13. Att analysera steget från allvarlig händelse till svår påfrestning

Startpunkten är figur 12.1 och eskalering av ”skadehändelse/tillståndsförändring” till ”svår påfrestning” (R2 till R3). Vi utgår återigen från att den primära konsekvensen av skadehändelsen/tillståndsförändringen, exempelvis i form av direkt påverkade människor, påverkan på miljö etc. kan vara av ”mindre”, ”allvarlig” eller ”katastrofal” omfattning enligt den kategorisering som gavs i kapitel 12. Vi vill här återigen framhålla att de ”skadehändelser” eller ”tillståndförändringar” vi talar om anses korrespondera väl med de ”situationer” som avses i 3 § i förordning 2002:472.

13.1 Allmän analysstruktur

I figur 13.1 nedan skisseras den huvudsakliga strukturen i ett möjligt angreppssätt att genomföra analysen. För att exemplifiera strukturen utgår vi från att en ”allvarlig” händelse har inträffat[2], d.v.s. där den primära konsekvensen av skadehändelsen/tillståndsförändringen är av ”allvarlig” karaktär. Ett krav på ”allvarlig händelse” skulle kunna vara att den kräver aktivering av det totala samverkansområdets krishantering. Figur 13.1 ger en översiktsbild av processen. X1, … , Xn är de riskfaktorer/orsaker/hot som kan ge upphov till en ”allvarlig händelse”.

2. Strukturen blir i huvudsak densamma i det fall själva skadehändelsen/tillståndsförändringen är av mindre allvarlig karaktär, med bl.a. den skillnaden att större uppmärksamhet ägnas åt potentiella eskaleringsmekanismer relaterade till allmänhetens och inblandade aktörers uppfattning om situationen etc. Angreppssättet är även tillämpbart i de fall skadehändelsen/tillståndsförändringen i sig själv är av katastrofal art, även om fokus då förmodligen kommer att ligga mer på den operativa krishanteringens effektivitet.



Figur 13.1 *Översiktsbild. Allmän analysstruktur, angreppssätt 1*

Angreppssättet bygger vidare på att man för identifierade ”allvarliga händelser” studerar vilka förutsättningar som krävs för att dessa skall kunna leda till en svår påfrestning på samhället. Konsekvenskategorierna har tidigare angivits i avsnitt 9.3.

Angreppssättet innebär alltså två steg,

- **Steg 1:** Definiera och beskriv ett antal ”allvarliga händelser”. Lista de faktorer eller omständigheter X1, … , Xn som bidrar till den allvarliga händelsens inträffande.
- **Steg 2:** Definiera de omständigheter och händelsekedjor eller scenarier som leder till att en svår påfrestning inträffar, exempelvis potentiella eskaleringsmekanismer kopplade dels till det ”fysiska” skeendet, dels till hur detta skeende uppfattas av allmänheten och inblandade aktörer. Beakta speciellt krishanteringssystemets påverkan, särskilt då samverkan med andra myndigheter lokalt, regionalt och nationellt.

13.2 Steg 1: Identifiering av allvarliga händelser

Problemet är alltså att som utgångspunkt för vidare analys definiera ett antal ”allvarliga händelser” som kan inträffa:

- genom att en eller flera skyddsbarriärer brutits genom efter att en initierande händelse inträffat eller en riskfaktor utlösts
- genom att en extrem yttre händelse inträffat
- genom att terroraktion, sabotage, eller intrång av annan typ genomförts.

Dessa utgångspunkter skall sedan användas för att studera eventuell vidare eskalering och krishanteringens effektivitet; d.v.s. för att genomföra sårbarhetsanalys avseende den yttre sårbarhet som diskuteras i avsnitt 5.3. Speciellt viktig faktor är samverkan över myndighetsgränserna.

En ”allvarlig händelse” kan ofta hänföras till någon av riskkategorierna i tabell 9.1. En del av risktyperna i tabellen avser strategiska risker, andra kategorier kan länkas till en allvarlig händelse på program- eller projektnivå. Erfarenheten visar att det är mer sällan som felhandling på operatörsnivå är en grundläggande orsak till en ”allvarlig händelse”.

Med tanke på det breda spektrum av såväl verksamheter över det totala myndighetsområdet som riskkategorier är det inte möjligt att specificera direkt vilken metod som bör användas vid identifieringen av tänkbara allvarliga händelser utan här ges endast några generella exempel.

På den strategiska nivån är huvudmålet att balansera risk (inklusive sannolikheten att en svår påfrestning inträffar) och möjlighet; d.v.s. man behöver metoder att identifiera framtidsrisker. Bland de metoder som är möjliga kan nämnas kvantitativ trendanalys, kvalitativ trendanalys, Delphipaneler (expertpanel), scenariometoder, workshops, fokusgrupper etc. (se t.ex. Performance and Innovation Unit, 2001).

På lägre nivåer finns ett stort antal analysmetoder för riskidentifiering i allmänna tekniska och sociotekniska system inkluderande samverkan människa – teknik – organisation. Publikationen ”Handbok för riskanalys” (Räddningsverket, 2003) redovisar ett 20-tal sådana metoder, exempelvis felträdsanalys, grovanalys och HAZOP. En generell struktur för riskidentifieringsprocessen beskrivs summariskt i Abrahamsson & Magnusson (2004).

Steg 1 bör emellertid resultera i en lista med ”allvarliga händelser” och ett angivande av de faktorer/orsaker/hot som generellt är förutsättningar för att respektive händelse skall inträffa. Drivs analysen något vidare bör det vara möjligt att strukturerat diskutera den samverkan mellan X1, … , Xn som resulterar i den allvarliga händelsen.

13.3 Steg 2: Från allvarlig händelse till svår påfrestning: scenariobeskrivning via händelseträd

Baserat på utfallet av riskidentifieringen ovan, d.v.s. ett antal ”allvarliga händelser”, blir sedan det naturliga steget att genomföra någon form av beskrivning av konsekvenserna givet att en ”allvarlig händelse” realiserats.

För att en allvarlig händelse skall utvecklas till en svår påfrestning behövs ofta att en serie omständigheter skall inträffa. Dessa kan med fördel illustreras med hjälp av s.k. händelseträd. Vi ser det som lämpligt att man med utgångspunkt i en given identifierad allvarlig händelse genomför en händelseträdsanalys som visar bedömningarna av sannolikheter för att en händelsekedja skall utvecklas till de valda scenarierna. För genomförande av analysen hänvisas till Räddningsverket (2003).

Inom de olika aktuella verksamheterna finns ofta traditioner att göra riskanalyser enligt vissa metoder. Sannolikt kan dessa även fortsättningsvis användas som huvudsakliga verktyg att genomföra de risk- och sårbarhetsanalyser som krävs enligt förordningen. De måste emellertid i en del fall utvidgas och/eller omformas för att få fram den i sammanhanget relevanta informationen.

14. Identifiering av svår påfrestning med grovanalytisk metod (preliminary hazard analysis)

I kapitel 13 utgick vi från att en ”skadehändelse” eller ”tillståndsförändring” hade inträffat och målsättningen var att studera under vilka förutsättningar (eskaleringsmekanismer, den operativa krishanteringens effektivitet etc.) den situation som då uppstod kan komma att utvecklas till en svår påfrestning på samhället, d.v.s. en form av ”bottom-up”-angreppssätt. Här kommer vi i stället att ha som utgångspunkt att en svår påfrestning inträffat och anlägga ett mer ”top-down”-baserat synsätt.

Figuren 14.1 nedan illustrerar det fall då man utgår från att en fullskalig kris, d.v.s. svår påfrestning, inträffat och man är intresserad av att direkt bestämma de faktorer/händelser/hot som orsakat krisen. Angreppssättet innebär alltså en direkt identifiering av de faktorer/omständigheter som leder till en svår påfrestning i samhället, speciellt brister eller svagheter i krishanteringssystemet, inklusive samverkan mellan myndigheter.

Fig. 14.1 *Angreppssätt 2, "direkt" angreppssätt*

Grovanalytisk metod

Målet är alltså att direkt identifiera och beskriva ett antal högprioriterade svåra påfrestningar med hänsyn till inverkande faktorer Xi och konsekvensens storlek.

Identifieringen av svåra påfrestningar föreslås ske via en process där varje avdelning, enhet, projekt, program etc. genomför sin egen evaluering, oftast under ledning av personal från RHF/KHF, se avsnitt 6.2. Att låta extern personal som exempelvis expertkonsulter medverka kan effektivisera processen. Som bas för arbetet används tillgängligt material om tidigare inträffade incidenter och händelser, genomförda riskanalyser, intervjuer med personal etc. För ett antal tekniska områden (olika typer av transport, processanläggningar, kärnkraft etc.) finns extensiva databaser med data och beskrivningar om felaktiga komponenter och olycksförlopp.

En svår påfrestning kan ofta hänföras till någon av riskkategorierna i avsnittet om riskidentifiering i avsnitt 9.3.

Som nämnts tidigare är det inte möjligt att föreskriva generellt användbara metoder för risk- och sårbarhetsanalyserna. Det finns emellertid behov av en enhetlig form för rapportering av resultaten av analyserna för att dessa skall kunna jämföras och för att ge underlag för prioriteringar och åtgärder. Därför rekommenderar vi att som basmetod för detta angreppssätt använda det som brukar kallas grovanalys. Grovanalysen fokuserar större skadehändelser eller störningar med tillhörande scenarier. Vid arbete med framtagande av scenarier i en grovanalys arbetar man oftast med en grupp erfarna personer från olika discipliner. Metoden kan därför sägas vara expertbaserad. Den innehåller normalt också alla sorters aspekter, såväl tekniska som alla ”mjuka” frågor.

Grovanalys, eller preliminär riskanalys, beskrivs i Räddningsverket (2003) enligt följande. ”En översiktlig s.k. grovanalys eller preliminär riskanalys görs tidigt i ett projekts planeringsstadium, eller vid en översiktlig inledande granskning av en existerande verksamhet. Metoden går ut på att granska verksamheten i stora drag, identifiera riskkällor och möjliga skadehändelser. Checklistor används ofta för att underlätta en systematisk genomgång av typiska riskfaktorer. En grov uppskattning av sannolikheter och konsekvenser bör göras för att underlätta en systematisk värdering av riskerna. Förslag till möjliga åtgärder för att eliminera eller reducera riskerna noteras och eventuella krav på fördjupade analyser ställs.”

Checklistor, riskmatris

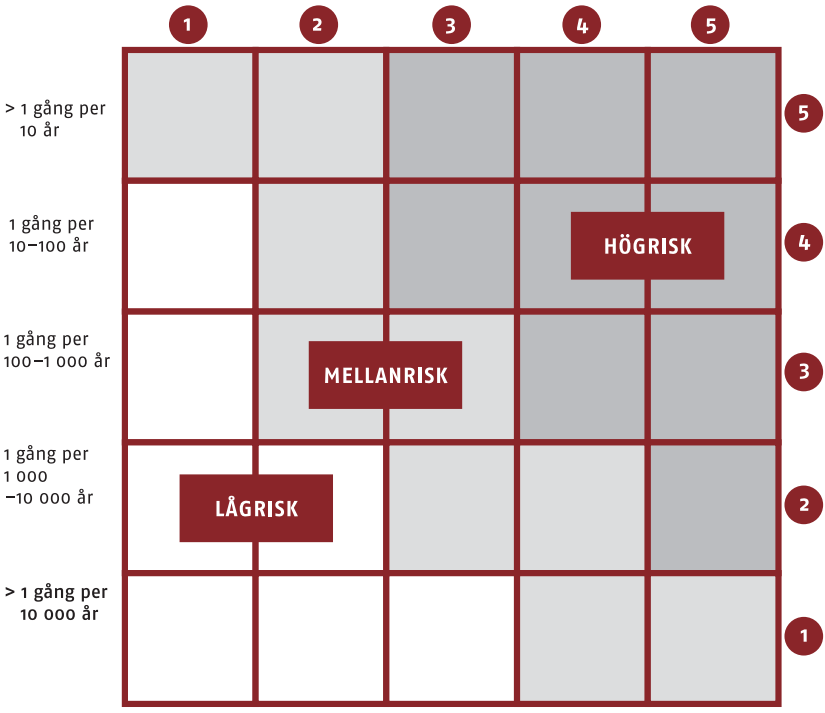
Grovanalysmetoden är alltså ofta baserad på checklistor. Allmänna checklistor för analys av kommunal verksamhet från säkerhetssynpunkt redovisas i skriften ”Verksamhetsanalys och säkerhetssamordning” (Kommunförbundet, 2001). Naturligtvis existerar det en mängd checklistor för ändamålet inom olika områden. Inom företagssektorn finns publikationer med ett stort antal checklistor, ett exempel utgörs av skrif-

ten ”Säkra företagets flöden” (ÖCB, 1999). Avseende checklistor eller manualer för specifika tekniska system hänvisar vi här endast till ”Basnivå för IT-säkerhet (BITS)” (KBM 2003d), samt verktyget ”SBA-Check” (Dataföreningen, 2002) avsett att användas vid analys av en organisations informationssäkerhet.

Grovanalysen ger i sin klassiska utformning svar på både omfattningen av konsekvenserna av en skadehändelse och sannolikheten/frekvensen av motsvarande händelse. Konsekvenserna uttrycks oftast i påverkan på liv och hälsa, på miljö och på kostnader för att ersätta egendom och för produktionsbortfall. Givetvis gäller för många av de situationer och händelser som analyseras att det finns andra typer av konsekvenser, såväl kvantifierbara som ej direkt kvantifierbara, som måste tas i beaktande. Exempelvis skulle konsekvenserna av ett långvarigt elavbrott vara svåra att beskriva i endast de termer som nämns ovan. En utmaning ligger alltså i att identifiera de olika typer av konsekvenser som kan tänkas uppkomma.

En relaterad utmaning är kopplad till möjligheten att göra jämförelser mellan olika analyser och olika typer av konsekvenser, d.v.s. att finna någon form av gemensam mätskala för olika typer av konsekvenser. Ett synsätt, dock inte ovedersägligt, innebär att man som ett mått på konsekvensen bör ta fram den totala kostnaden för en analyserad skadehändelse eller störning sedd i ett samhällsperspektiv. Tanken är alltså att exempelvis avbrott i viktiga samhällsfunktioner och dylikt kan omvandlas till ekonomisk förlust. I bedömningen av ekonomisk konsekvens skall då alla relevanta kostnader ingå, exempelvis direkta egendomsskador och produktionsförlust, förlust av framtida försäljning, diverse immateriella kostnader etc. Även om risk- och sårbarhetsanalysen inte primärt ger resultat i form av förlust av pengar eller liv/hälsa eller miljö, finns alltid följdverkningar någonstans som kan uppskattas i ekonomiska termer. Denna mer eller mindre grova uppskattning skulle kunna göras för att överföra resultatet av en primär risk- och sårbarhetsanalys till något som kan användas i jämförelser med resultaten från andra verksamheter.
För att konkretisera resonemanget finns i figur 14.2 ett exempel på klassificering av riskerna med en 5-gradig skala för sannolikheten/frekvensen för händelsen och ävenledes en 5-gradig skala för konsekvensen mätt i:

- Ekonomi
- Liv och hälsa
- Miljö



Ekonomi	< 10 milj kr	10–100 milj kr	100–1 000 milj kr	1 000–10 000 milj kr	> 10 000 milj kr
Hälsa	Enstaka dödsfall och/eller flera svårt skadade	Flera dödsfall och/eller många svårt skadade	10–100 dödsfall och/eller tusentals svårt skadade	100–1000 dödsfall och/eller tusentals svårt skadade	Mer än 1 000 dödsfall och/eller tiotusentals svårt skadade
Miljö	Mindre skadeeffekter; varaktighet < 1 år. Liten till stor utbredning. Oftast enkel sanering.	Större skadeeffekter; varaktighet 1–10 år. Liten utbredning (< 10 km²). Oftast svår eller omöjlig sanering.	Allvarliga skadeeffekter; varaktighet 10–100 år. Stor utbredning (hundratals km²). Oftast svår eller omöjlig sanering.	Mycket allvarliga skadeeffekter; varaktighet 10–100 år. Stor utbredning (hundratals km² eller mer). Oftast svår eller omöjlig sanering.	Mycket allvarliga, permanenta skador. Mycket stor utbredning (landsdelar). Omöjlig sanering.

Figur 14.2 *Riskmatris för ekonomi, hälsa och miljö*

15. Externa hot och sårbarhets-analys av kritiska försörjnings-system och infrastrukturer

15.1 Allmänt

För en allmän bakgrundsbeskrivning hänvisas till avsnittet 3.2.4 *Samhällviktig infrastruktur och grundläggande resurser* i skriften *Samhällets Krisberedskap 2005. Planeringsinriktning* (KBM, 2003b).

Att alla myndigheter har att redovisa sårbarhet, hot och risker avseende samhällsviktig infrastruktur inom respektive ansvarsområde i analysen enligt 3 § i förordningen 2002:472 är självklart. Dessutom gäller enligt 4 § i förordningen att samverkansansvariga myndigheter skall *beakta säkerhetskraven för de tekniska system som är nödvändiga för att de skall kunna utföra sitt arbete.*

15.2 Struktur på analysen: tillgängliga manualer

Internationellt sett har ett stort antal ansvariga myndigheter utfärdat standards, manualer, vägledningar etc. avseende hur sårbarhetsanalys av infrastruktursystem exponerade för främst externa hot skall utföras. Generellt ingår ett antal delsteg i processen:

1. Identifiera kritiska resurser (KR) i form av komponenter, noder, etc.
2. Identifiera vad som skyddar och stöder KR.
3. Identifiera och kategorisera hoten.
4. Identifiera och analysera sårbarheter.
5. Bedöm risk och bestäm prioritering för skydd av KR.
6. Identifiera åtgärder, kostnader och trade-offs.

De manualer och vägledningar som nämns ovan har ofta en volym på 50–100 sidor eller mer; d.v.s. sårbarhetsanalysen är utpräglat detaljerad och specifik. I några fall finns nationella arbeten på området. Vi har valt att ge webbadresser till ett antal manualer främst från USA.
Exempel är:

IT-sektorn

- *Basnivå för IT-säkerhet (BITS)*, KBM (2003d)
  http://www.krisberedskapsmyndigheten.se/verksamhet/information/bas_it-sakerhet_bits_rekomm2003-2.pdf (2004-01-12).
- *IT och sårbarhet – Kritiska beroendeförhållanden i den nationella IT-infrastrukturen*, KBM (2003e)
  http://www.krisberedskapsmyndigheten.se/verksamhet/information/it_sarbarhet_2003.pdf (2004-01-12).

Elförsörjningens infrastruktur

- *Vulnerability Assessment Methodology – Electric Power Infrastructure* US DoE (Department of Energy) (2002a).
  http://www.esisac.com/publicdocs/assessment_methods/VA.pdf (2004-01-12).

  Innehåller bl.a. ett stort antal arbetsblad/checklistor för att kontrollera interdependensen mellan olika infrastrukturer.

Infrastruktur för energiförsörjning

- *Energy Infrastructure Vulnerability and Risk Assessment Checklists for State Governments* US DoE (2001).
  http://www.appanet.org/operations/checklist.pdf (2004-01-12).
- *Energy Infrastructure Risk Management Checklists for Small and Medium Sized Facilities* US DoE (2002b).
  http://www.esisac.com/publicdocs/assessment_methods/Risk_Management_Checklist_Small_Facilities.pdf (2004-01-12).

Vattenförsörjning

- *Instructions to Assist Community Water System in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002* US EPA (Environmental Protection Agency) (2003).
  http://www.epa.gov/safewater/security/util-inst.pdf (2004-01-12).

Processanläggningar

- *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites,* Centre for Chemical Process Safety of the American Institute of Chemical Engineers, New York, (2002). http://www.aiche.org/ccpssecurity/ (2004-01-12).

15.3 Interdependens, speciellt el – tele – it

I en inledande fas förutsätts att denna typ av sårbarhet får behandlas via sönderdelning (dekomposition), samt användning av standards, normer, vägledningar och åtföljande checklistor. Avseende angreppssättet med sönderdelning är dock en nyckelfråga hur ett komplext interdependent system kan uppdelas i subsystem som sedan kan analyseras var för sig utan att dominerande riskkällor negligeras. Avvägningen mellan den vinst i hanterbarhet man kan göra genom en uppdelning av systemet och den information som går förlorad måste göras med eftertanke.

16. Förslag till möjligt innehåll i risk- och sårbarhetsanalyserna enligt förordning 2002:472

I detta kapitel skisseras ett möjligt upplägg avseende innehållet i de risk- och sårbarhetsanalyser som skall inlämnas till regeringskansliet enligt förordning 2002:472. Förslaget är författarnas och bör ses som ett möjligt komplement till den struktur som ges i vägledningen (KBM, 2003a) och som en möjlig utgångspunkt inför kommande års analyser. Givetvis är det även så att det kan skilja sig (väsentligt) mellan olika myndigheter avseende såväl vad som bör inkluderas i redovisningen som redovisningens detaljeringsgrad.

16.1 Möjligt innehåll i risk- och sårbarhetsanalyserna

Vi har valt att redovisa vad vi anser vore lämpligt att inkludera i risk- och sårbarhetsanalyserna under två huvudrubriker: utvärdering av myndighetens funktion och roll, samt upprättande av register över analyserade händelser och situationer (svåra påfrestningar).

16.1.1 A. Utvärdering av myndighetens funktion och roll

Med utgångspunkt i vad som anförts i kapitel 6 – 9 anser vi att det kan vara lämpligt att i analysen inkludera punkt 1 – 5 nedan:

1. Bedömning av föreskrifters effektivitet.
2. Bedömning av tillsynens effektivitet.
3. Bedömning av existerande ramverk för riskhantering (se avsnitt 9.1). Intern verksamhet, extern verksamhet.
4. Bedömning av säkerhetsledningssystemets effektivitet (se checklista i bilaga 1). Intern och extern verksamhet.

5. Redovisning av uppbyggnad av myndighetens krishanteringsfunktion, samt utvärdering av krishanteringsplan (se checklista i bilaga 1). Intern och extern verksamhet.

Vad som är tillämpligt med avseende på punkt 1– 5 ovan varierar naturligtvis från myndighet till myndighet.

Andra frågor som kan vara aktuella att belysa, där så bedöms relevant, omfattar

- Vem som ansvarar för regelsystem (rutiner, instruktioner) på operativ nivå
- Vem som kontrollerar efterlevnad på operativ nivå
- Vem som utfärdar föreskrifter för säkerhetsledningssystem och ledningssystem för krishantering
- Vem som utvärderar effektiviteten av ledningssystemen
- Vem som etablerar nivå för acceptabel risk
- Vem som kontrollerar att denna nivå uppfylls

samt en genomgång av de problem och dilemman som svaren på frågeställningarna ovan eventuellt skapar.

16.1.2 B. Upprättande av register över analyserade händelser och situationer (svåra påfrestningar)

I KBM:s vägledning (KBM, 2003a) ges en struktur för rapporteringen av analysarbetet. Där efterfrågas bl.a. en översikt över analyserade händelser och situationer att användas som bas för att vidare kunna värdera aktuell förmåga, förbättringsåtgärder, samverkansbehov etc. Vi anser att det vore värdefullt om det vore möjligt att rangordna de analyserade händelserna och situationerna, samt upprätta ett register som sedan årligen kan uppdateras. Nedanstående punkter kan ingå:

1. Identifiering av de 5–10 allvarligaste krisscenarierna enligt kapitel 12–14 eller med annan lämplig metodik. Detta avser såväl intern verksamhet som verksamheter under tillsyn.

2. Upprättande av åtgärdsförslag.

3. Kvalitetssäkring av genomförd analys.

De tre typer av riskfaktorer/hot/händelser som nämnts i avsnitt 8.1–8.3 bör behandlas, i de fall dessa är relevanta.

16.2 Checklista för den övergripande riskhanterings- och krishanteringsprocessen

I detta avsnitt nämns endast helt kort ett par exempel på checklistor som kan användas som stöd för att utvärdera riskhanterings- respektive krishanteringsprocessen vid myndigheten. Checklistorna, som är hämtade från Office of Government Commerce (2001), samt CCMD (2003), återfinns på originalspråket i bilaga 1.

Referenser

Abrahamsson, M. & Magnusson, S. E. *Användning av risk- och sårbarhets-analyser i samhällets krishantering – delar av en bakgrundsstudie*, LUCRAM, Lunds Universitet (Kommer att publiceras tidigt under 2004).

Andersson, M. & Kinnerberg, E. *Naturkatastrofers bidrag till riskbilden i EU*, rapport 5089, Brandteknik, Lunds Tekniska Högskola (2001).

Bier, V. M., Haimes, Y.Y., Lambert, J.H., Matalas, N.C. & Zimmerman, R. "A Survey of Approaches for Assessing and Managing the Risk of Extremes", *Risk Analysis*, Vol 19, No 1, (1999).

Boin, A. *Crisis Management in Europe: A Discussion of Key Factors in Improving Safety*, Paper for The NATO/Russia Advanced Research Workshop: Forecasting and Preventing Catastrophes, University of Aberdeen (2003).

CCMD *Crisis and Emergency Management: A Guide for Managers of the Public Service of Canada*, Canadian Centre for Management Development, (2003).

Haimes, Y.Y. *Risk Modeling, Assessment, and Management*, John Wiley & Sons (1998).

CCPS *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*, Centre for Chemical Process Safety of the American Institute of Chemical Engineers, New York, (2002).

COSO, *Enterprise Risk Management Framework*, The Committee of Sponsoring Organizations of the Treadway Commission, (2003). http://www.erm.coso.org/Coso/coserm.nsf/frmWebCOSOHome?ReadForm (2003-09-20).

Dataföreningen *SBA Check – Checklisteverktyg för nulägesanalys med speciell inriktning på informationssäkerhet*, Dataföreningen, Stockholm, (2002). http://www.dfs.se/products/sba/check/ (2003-10-10).

DEFRA *Risk Management Strategy*, UK Department for Environment, Food and Rural Affairs, (2002). http://www.defra.gov.uk/corporate/busplan/riskmanage/riskmanage.pdf (2004-01-13).

Einarsson, S. & Rausand, M. "An Approach to Vulnerability Analysis of Complex Industrial Systems", *Risk Analysis*, Vol 18, No 5, (1998).

Einarsson, S. *Comparison of QRA and Vulnerability Analysis: Does Analysis Lead to More Robust and Resilient Systems?*, Acta Polytechnica

Scandinavica Civil engineering and building construction series no. 114, Espoo, Finland, (1999).

FEMA *Multi Hazard – Identification and Risk Assessment – A Cornerstone of the National Mitigation Strategy*, Federal Emergency Management Agency, USA, (1997).

Haimes, Y.Y. *Risk Modeling, Assessment, and Management*, John Wiley & Sons (1998).

Hale, A. & Hopkins, A. "Issues in the regulation of safety: setting the scene" in Hale A., Hopkins A., Kirwan B. (eds), *Changing Regulation*, Elsevier Science, Oxford, (2002).

Hale, A., Heming, B., Carthey, J. & Kirwan, B "Modelling of safety management systems", *Safety Science*, vol 26, Elsevier, (1997).

HM Treasury *Management of Risk – A Strategic Overview – With supplement guidance for smaller bodies*, HM Treasury (2001). http://www.hm-treasury.gov.uk/media//EC612/orange-book.pdf (2003-09-11)

International Electrotechnical Comission, IEC, *International Standard – Dependabiliy management part 3: application guide – section 9 Risk Analysis of technological systems* (1995).

Kaplan, S. "The Words of Risk Analysis", *Risk Analysis*, Vol 17, No 4, Plenum Press (1997).

KBM *Risk- och sårbarhetsanalyser – Vägledning för statliga myndigheter* (2003a). http://www.krisberedskapsmyndigheten.se/verksamhet/sarbarhet/risk_sarbarhetsana_vagledn_statliga_mynd_rekom_2003-1.pdf (2004-01-09).

KBM *Samhällets Krisberedskap 2005. Planeringsinriktning* (2003b). http://www.krisberedskapsmyndigheten.se/verksamhet/planering/planeringsinriktning_samhallets_krisberedskap_2005.pdf (2004-01-09).

KBM *Strategi för forskning för samhällets krisberedskap* (2003c). http://www.krisberedskapsmyndigheten.se/verksamhet/forskning/forskningsstrategi_20030227.pdf (2003-09-10).

KBM *Basnivå för IT-säkerhet (BITS)* (2003d). http://www.krisberedskapsmyndigheten.se/verksamhet/information/bas_it-sakerhet_bits_rekomm2003-2.pdf (2004-01-12).

KBM *IT och sårbarhet – Kritiska beroendeförhållanden i den nationella IT-infrastrukturen*, (2003e). http://www.krisberedskapsmyndigheten.se/verksamhet/information/it_sarbarhet_2003.pdf (2004-01-12).

Kemikontoret *Integrerat Ledningssystem för Säkerhet, Hälsa och Miljö – en handbok med rutiner, om SHM-ledningssystem*, Kemikontoret (1997).

Kirwan, B. *A Guide to Practical Human Reliability Assessment*. Taylor&Francis (1994)

Kommunförbundet *Verksamhetsanalys och säkerhetssamordning – Metod och vägledning*, Svenska Kommunförbundet, (2001).

La Porte, T.R. "On the Design and Management of Nearly Error-free Organisational Control Systems" in Sills, D.L., Wolf, C.P. and Shelansky, V.B. (eds.), *Accident at Three Mile Island: The Human Dimension*, Westview Press, Boulder, (1981).

Morgan, M. G. & Henrion, M. *Uncertainty – A guide to dealing with uncertainty in quantitative risk and policy analysis*, Cambridge University Press, New York (1990).

NRC, National Research Council *Making the Nation Safer – The Role of Science and Technology in Counterring Terrorism*, The National Academies Press, Washington (2002).

Office of Government Commerce *Draft Guidelines on Managing Risk* (2001). http://www.ogc.gov.uk/sdtoolkit/reference/ogc_library/generic_guidance/risk_hbook.pdf (2004-01-12).

Performance and Innovation Unit, Cabinet Office *A Futurist's Toolbox – Methodologies in Futures Work*, Cabinet Office (2001) http://www.number-10.gov.uk/su/toolbox.pdf (2003-10-27)

Perrow, C. *Normal Accidents: Living with High-Risk Technologies*, Basic Books, New York (1984).

Project Management Institute, *A Guide to the Project Management Body of Knowledge*, Project Management Institute, Newtown Square, Pennsylvania, USA, (2000).

Reason, J. *Managing the Risks of Organizational Accidents*, Ashgate Publishing Limited (1997).

Rijpma, J.A. "Book review essay – From Deadlock to Dead End: The Normal Accidents – High Reliability Debate Revisited", *Journal of Contingencies and Crisis Management*, Blackwell Publishing Ltd. Oxford, (2003).

Räddningsverket *Handbok för riskanalys*, beställningsnummer U30-626/02 Räddningsverket, Karlstad, (2003).

Strategy Unit, Cabinet office Risk: *Improving government's capability to handle risk and uncertainty*, (2002). http://www.number-10.gov.uk/SU/RISK/REPORT/downloads/su-risk.pdf (2003-09-10).

Sundelius, B., Stern, E. & Bynander, F. *Krishantering på svenska – teori och praktik*, Nerenius & Santérus Förlag AB, Stockholm, (1997).

Timmerman, P. *Vulnerability, Resilience and the Collapse of Society*, Institute of Environmental Studies, University of Toronto, Toronto (1981).

Turner, B.A. & Pidgeon, N.F. *Man-Made Disasters* (second edition), Butterworth-Heinemann, Oxford, (1997).

US DoE (Department of Energy) *Energy Infrastructure Vulnerability and Risk Assessment Checklists for State Governments*, (2001). http://www.appanet.org/operations/checklist.pdf (2004-01-12).

US DoE (Department of Energy) *Vulnerability Assessment Methodology – Electric Power Infrastructure*, US DoE, Office of Energy Assurance (2002a). http://www.esisac.com/publicdocs/assessment_methods/VA.pdf (2004-01-12).

US DoE (Department of Energy) *Energy Infrastructure Risk Management Checklists for Small and Medium Sized Facilities*, US DoE, Office of Energy Assurance (2002b). http://www.esisac.com/publicdocs/assessment_methods/Risk_Management_Checklist_Small_Facilities.pdf (2004-01-12).

US EPA (Environmental Protection Agency) *Instructions to Assist Community Water System in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002*, US EPA, Office of Water (2003). http://www.epa.gov/safewater/security/util-inst.pdf (2004-01-12).

Watts, M.J. & Bohle, H.G. *The space of vulnerability: the causal structure of hunger and famine*, Progress in Human Geography, no 17, pp 43-67 (1993).

Weichselgartner, J. "Disaster mitigation: the concept of vulnerability revisited", *Disaster Prevention and Management*, vol 10, number 2, MCB University Press (2001).

ÖCB *Säkra företagets flöden*, Överstyrelsen för civil beredskap, Solna (1999).

Bilaga 1
Checklistor för utvärdering av riskhanterings- och krishanteringsprocessen

Checklista för utvärdering av riskhanteringsprocessen

Hämtad från Office of Government Commerce (2001) s. 29–31.

The checklists provided in the annexes can be used to help to identify those aspects of risk management that are being applied well or those that are not adequately supported. Checklists included are:

A Effective risk management framework and risk process

B Assignment of risk ownership

C Risk identification

D Risk evaluation and assessment of the organisation's willingness to take on risk

E Risk response

F Monitoring and control mechanisms

A. Checklist on effective risk management framework and risk process

- Is there a formal policy on risk? If 'yes', is this clearly documented, endorsed by senior management and communicated to all staff?

- Is there a clear definition of risk that is understood throughout the organisation?
- Is the organisational structure conducive to the management and communication of risk?
- Is a consistent and systematic approach applied to the management of risk at all levels of the organisation?
- Is the organisation demonstrably committed to providing the required level of skills and training to ensure that staff understand and can manage risk effectively?
- Is tolerance of risk understood by managers and applied consistently throughout the organisation?
- Once identified, are risks appropriately monitored and reviewed, at all levels of the organisation?
- Does the organisation's culture support well thought through risk taking and innovation in an appropriate manner?

B. Checklist on assignment of risk ownership

- Have owners been allocated for all the various parts of the complete risk process?
- Has the full scope of the risks been catered for, e.g., suppliers may be tasked with ownership of assessing and evaluating some risk as part of their contracts?
- Are the various roles and responsibilities associated with ownership well defined?
- Do the individuals who have been allocated ownership actually have the authority and capability to fulfil their responsibilities?
- Have the various roles and responsibilities been communicated and understood?
- Are the nominated owners appropriate?
- In the event of a change is ownership reassessed; and if necessary, can it be quickly and effectively re-allocated?
- Are the differences between benefit and delivery risks clearly understood and do each types of risk have appropriate owners (who are likely to be different)?

C. Checklist on risk identification

- Has a clear policy on the application of a risk-oriented management process and the scope of risks to be addressed been set at the highest level?
- Has the scope been directly linked to the context and objectives that have been set?
- Has this been agreed and clearly communicated from the outset and reviewed regularly to ensure it is still appropriate – that is, strategic objectives linked to that of the programme, the projects and operations?
- Are changes that have been made to the project objectives being fed back into the risk process and linked back to the entries in the risk register?
- Are decisions taken at project level at risk of being potentially flawed, because the scope of risks being assessed is incorrect?
- Does the risk process cater for all different types of risk?
- Has a full, comprehensive set of risks been identified?
- Has a range of appropriate identification approaches been adopted?

D. Checklist on risk evaluation and assessment of the organisation's willingness to take on risk

- Has the level of analysis that is required to support the decision process been agreed from the outset, e.g., start of the project, acquisition lifecycle etc?
- Is there a demonstrable correlation between the amount of time, effort and cost expended in risk analysis to the difficulty in obtaining decisions, resources and funding for risk management etc?
- Is the level of analysis, where possible, commensurate with the level of risk? For example are detailed assessments of probabilities being carried out on threats which are known to have little, or no, impact?
- Is a consistent approach being taken to assessing potential impact and probability?
- Is there a good understanding as to the relationship between the potential impact against the probability of the risk occurring?
- Is risk information required communicated effectively to support the necessary decision making process, in a timely and cost effective manner?

- Is there a clear understanding of the difference between a problem/issue management process and the risk process and ensuring a suitable means of transferring from one to the other?
- Is there an understanding and commitment as to what level of risk is acceptable, i.e. risk tolerance and willingness to adopt risk for a project, and the ability to communicate this? Does this reflect the potential for accruing benefits?
- Are the appropriate skills required to carry out the analysis available?
- Are risks being understated when assessed or evaluated, whether for commercial, political or individual reasons?
- Is there adequate commitment at all levels to the process of analysing and evaluating the threats?
- Is the process of analysing and evaluating the threats sufficiently flexible to be able to respond to rapid types of changes? Recent examples of this are where ecommerce developments have required IT developers, or other parts of the business, such as customer relationship management, human resources, facilities etc to gear up to deliver solution to the 'market' within abnormally tight timescales. Three months from strategic concept to delivery of the operation seems to have become the norm.

E. Checklist on risk response

- Have the treatment measures recommended been assessed in terms of:
  - costs compared with the anticipated benefits of treating the risk?
  - the range of responses available?
  - the effectiveness in containing the risk or enhancing the opportunity?
- Do the risks have an adequate description and can be fully understood?
- Have the risk been assessed to see which needs tackling first?
- Has the subsequent required treatment been set?
- Has there been a clear allocation of responsibilities and ownership for actions, decisions etc and the required timescales for completion and review?
- Has the information required for communicating been identified, i.e., to whom, where and when and how?
- Is there a mechanism in place for monitoring and reporting on the effectiveness of the actions being undertaken (see monitoring and reporting)?
- Has adequate contingency been planned ?

F. Checklist of monitoring

- Has appropriate ownership of the status reporting mechanism been achieved (that is, how it will be used, when and by whom as the owners of that process)?
- Has the organisation put in place mechanisms to monitor the adequacy of processes required to ensure that cultural, political and personal pressures do not hinder truthful representation of status of high profile risks?
- Is there confidence in the accuracy of reporting?
- Is the level of commitment to the reporting process adequate or is there a lack of commitment?
- When assessing and reporting effectiveness are the statements made factual rather than speculative?

Checklista för utvärdering av krishanteringsprocessen

Hämtat från CCMD (2003) s. 13.

Questionnaire on Your Organization's Preparedness

In responding to the following questions, managers can assess broadly their organization's capability to respond to crises and emergencies. The questions are intended to identify the strengths and weaknesses of organizations regarding the activities to put forward in the stages of mitigation, preparedness, response, and recovery:

1. Does your organization have a corporate vision for crisis and emergency management? What is it? Does it address the various phases?
2. Has the proper planning been done regarding who will be involved in each of the phases of crisis and emergency management?
3. List the actual capabilities that your organization has in each area, as well as plans to improve your organization's capabilities.
4. On which phase(s) are the majority of your organization's crisis and emergency management efforts concentrated?
5. On which phase(s) is there a shortage of crisis and emergency management efforts?
6. What kind of attention and rewards do people receive when they contribute to each of the phases?
7. Are there phases for which employees' responsibilities and rewards could be increased or improved?
8. How well does your organization plan for all four phases?
9. What barriers keep people from planning all four phases?
10. How could these barriers be overcome?"

ISSN: 1652-3717
ISBN: 91-85053-20-1

Krisberedskapsmyndigheten

Box 599
101 31 Stockholm

Tel 08-593 710 00
Fax 08-593 710 01

kbm@krisberedskaps
myndigheten.se

www.krisberedskaps
myndigheten.se