ÖVERSTYRELSEN
FÖR CIVIL BEREDSKAP

Årssammanställning av omvärldsanalys

Analysenheten ÖCB
hösten 2001

Innehållsförteckning

1 Omvärldsanalys vid ÖCB

I ÖCB:s instruktion står att myndigheten ska bedriva omvärldsanalys. Det är alltså en uttrycklig beställning från regeringen. Det går också att hävda att ÖCB, liksom många andra organ i vår bransch, för att på bästa sätt lösa sina uppgifter är betjänt av en bra omvärldsanalys. Om vi t ex ska bidra till att minska sårbarheten i den samhällsviktiga infrastrukturen är det en nödvändig förutsättning att följa med i utvecklingen vad avser såväl förändringar i dess utformning och funktionssätt som hur man kan beskriva och förstå hur de förhåller sig till varandra. I båda fallen är det dessutom närmast självklart att ta del av hur man ser på dessa företeelser i andra länder, samt hur man väljer att hantera frågorna i sina respektive system. För att åstadkomma en komplett behandling av hot och risker behöver omvärldsanalysens underlag dessutom innefatta underrättelser. I ett betänkande om underrättelsetjänsten nämns även att ÖCB ska bedriva en omvärldsanalys.[1]

Fundera på det här: Lika länge som det samtidigt har existerat flygplan och hus har det varit möjligt att flyga in i hus. Lika länge som det har funnits elledningar har dessa kunnat gå av. När något väl inträffar får vi mycket konkreta erfarenheter av konsekvenser av det inträffade. Vår omvärldsanalys (och för den delen även forskningen) syftar bland annat till att det ska bli möjligt att överväga konsekvenser och åtgärder innan det otänkbara inträffar -- detta för att (någon ska) kunna förebygga dessa händelser samt för att (någon ska) kunna bilda sig en någorlunda god uppfattning om vad som ska göras om något (oönskat) ändå inträffar. En sådan uppgift innefattar följaktligen också en viss skyldighet att försöka tänka "det otänkbara".

Denna rapport ska ge en bild av det senaste årets, hösten 2000 – hösten 2001, omvärldsanalysarbete vid ÖCB samt beskriva tendenser och förändringar i samhället som har betydelse för den civila krishanteringen.

[1] SOU 1999:37 Underrättelsetjänsten – en översyn. I den beskrivs ÖCB:s samordningsuppgift på följande sätt:. ”I samordningsuppgiften och i rollen av funktionsansvarig myndighet ligger att ha en aktuell och väl grundad uppfattning om utvecklingen i omvärlden. ÖCB ska följa utvecklingstendenser som har betydelse för det svenska civila försvarets villkor och inriktning. Rollen som funktionsansvarig tar även sikte på att ÖCB skall bevaka att det civila totalförsvaret utgår från ett vidgat säkerhetsbegrepp och därmed beaktar s.k. hot och risker i en bred hotskala”

2 Sammanfattning och slutsatser

För att kunna skydda samhället mot olika typer av störningar och angrepp krävs ny kunskap. Den breddade hotbilden, samhällets föränderlighet och den snabba tekniska utvecklingen gör att villkor och förutsättningar för ett ändamålsenligt skydd är annorlunda jämfört med till exempel under det kalla kriget. På många områden förändras villkoren också i samma takt som utvecklingen i övrigt. I denna mening förändrade villkor innebär givetvis bland annat att dagens och morgondagens skydd inte kan genomföras med gårdagens metoder. Ett samordnat agerande är avgörande för framgång, både när det gäller preventiv sårbarhetshantering och operativ krishantering, vilket kräver tvärsektoriell samordning och ett nära samarbete mellan statsmakter och näringslivet.

Forskning, utveckling och analys av samhällets utveckling utgör därför en oundgänglig del i en verksamhet som syftar till skydd av samhället och dess olika funktioner. Hot, risker, sårbarhet eller beroenden måste kunna beskrivas och förstås, liksom de delar av samhället som är eller kan bli utsatta. De nya hoten och svårigheten att avgöra om dessa hot vänder sig mot militär eller civila ökar behovet att samverka mellan militär och civil forskning, särskilt med avseende på hot och skyddsåtgärder.

I den gråzon av hot som uppkommit efter nedtoningen av invasionsrisken är det viktigt att vara uppmärksam på nya faror. Hoten i vår omvärld är föränderliga och kräver förutom en flexibel syn på vad som kan utgöra ett potentiellt hot även en flexibel syn på åtgärder. Det är därför ytterst viktigt att följa och analysera utvecklingen i vår omvärld för att på så sätt vara uppmärksam på såväl nya typer av hot som nya sätt att hantera dem.

Inom forskningen rörande infrastrukturen har ännu inte presenterats någon heltäckande beskrivning och förståelse för att utröna de olika funktionernas inbördes beroende. Det behövs därför ytterligare forskning och det är viktigt att utveckla metoder för att beskriva och analysera ömsesidiga beroenden.

Vad avser elförsörjningens sårbarhet kan den endast lösas genom redundans. Det måste finnas ett nät av kommunikationsvägar där man vid ett avbrott på en förbindelse snabbt kan gå över till en annan som har en alternativ sträckning. Vissa viktiga noder kan förmodligen endast skyddas genom att vara belägna långt ner i bergrum.

Sammankopplingen av IT-system i nätverk ger en angripare möjlighet att med förhållandevis enkla och billiga medel skapa stor skada i ett samhälle. Angrepp på viktiga IT-system måste därför kunna upptäckas tidigt, innan skadan blir omfattade. Idag har ingen myndighet det övergripande ansvaret för IT-säkerhetsfrågorna varken nationellt eller internationellt, vilket kan visa sig bli nödvändigt i framtiden.

Det nätverksbaserade militära försvaret, tidigare benämnt RMA och nu Ny krigföring, som är under utformning kommer av allt att döma att vara beroende av robustheten i den civila infrastrukturen. Detta leder till att samhället måste ställa ännu högre krav än tidigare på både skyddet av infrastrukturen i sig och skyddet av den information som hanteras och förmedlas. Utvecklingen av ett framtida nätverksbaserat informations- och ledningssystem för den civila krishanteringen skulle kunna korrespondera med uppbyggnaden av det nätverksbaserade militära försvaret.

En första scenariobaserad studie i syfte att kartlägga viktiga åtgärdsområden avseende skydd av civilbefolkningen bör initieras under en förhållandevis nära framtid. När det gäller forskningsinsatserna inom NBC-området avseende skydd av civilbefolkningen bör en större del användas för att studera aktörsperspektivet och konsekvenserna av NBC-hotet för den civila krishanteringen.

Det krävs ökade insatser för att stärka samhällets förmåga att hantera komplexa skadesituationer där massförstörelsevapen använts. Både avseende skydd av infrastruktur och skydd av civilbefolkningen är viktiga områden lednings- och informationssystem, kunskaps- och erfarenhetsöverföring, utbildning, övning och investeringar i materiel för kris- och konsekvenshantering. För dessa områden bör dimensionerings- och resursfrågor också beaktas.

Det krävs bra analysmetoder och modeller för att göra det möjligt för samhället att i förväg skydda sig mot samt upptäcka och reagera på påfrestningar. Utveckling och framtagande av nya goda och systematiska analysmodeller och metoder inom risk- och sårbarhetsområdet samt inom krishantering bör prioriteras. Det kräver dock att mer finansiella resurser tillförs.

3 Civil sårbarhets- och krishantering

En uppgift som ankommer på det allmänna är att svara för allmän ordning och säkerhet samt att verka för de enskildas personliga välfärd och trygghet. Till det kommer de enskildas eget ansvar att skydda sig själva. Det fullt ut säkra och trygga är emellertid inte möjligt. Kriminalitet, olyckor och sjukdomar finns och kommer alltid att finnas, även i de mest utvecklade samhällena. Krig eller farsoter har mycket länge utgjort de värsta hoten mot samhället och de enskilda. För att kunna hantera hotet om krig har särskilda resurser byggts upp. Dessa har inom ramen för totalförsvaret kompletterats med en omställning av fredssamhällets resurser för användning i krig.

Samhällets resurser för säkerhet och skydd är i allt väsentligt dimensionerade, organiserade och använda för att hantera de skadehändelser som regelbundet inträffar i samhället eller som är tillräckligt frekventa för att beaktas i resursuppbyggnaden. Exempelvis kan nämnas lägenhetsbränder och våldsbrott men också skadehändelser inom kollektivtrafiken eller industrin.

Utvecklingen i omvärlden och förbättrad kunskap om riskerna för naturhändelser har lett till en ökad medvetenhet om att det finns ett område mellan de mera vardagliga skadehändelserna och fullskaligt krig som måste kunna hanteras på ett rimligt sätt av såväl det allmänna som näringslivet och de enskilda. I kapitel 4 och 7 beskrivs närmare hoten, riskerna och sårbarhetsutvecklingen.

Basen för civil sårbarhets- och krishanteringsförmåga

Civil sårbarhets- och krishantering är baserad på kunskap, förståelse, resurser, organisation och förmåga. Detta är grundförutsättningar för att kunna hantera situationer som ligger utanför samhällets, organisationens eller individens normala dagliga verksamhet. Genom utbildning, träning och övning kan enskilda och organisationer lära sig att agera ändamålsenligt även i situationer som är onormala och innebär exponering för hot, påfrestningar och stress.

Kunskap i vid bemärkelse är grunden för civil sårbarhets- och krishanteringsförmåga. Vi behöver en samordnad och interdisciplinär forskning för att bättre förstå hot och risker, system, skydd och sårbarheter. Nätverk mellan olika kunskapscentra, är ett viktigt medel för att skapa den nödvändiga kunskapen. Hur människor och organisationer bättre kan hantera kriser och en snabbt föränderlig värld är ett annat viktigt kunskapsområde. Metodutveckling för civil sårbarhets- och krishantering är en stor forsknings- och utvecklingsutmaning, som kommer att behöva genomföras fortlöpande i det av föränderlighet präglade nätverkssamhället.

Till kunskapsområdet hör också inhämtning och analys av omvärldsutvecklingen. Utan en aktuell och strategisk analys av samhälle, system och sårbarhet kan inte hot och risker förutses och en tillräcklig förmåga att hantera dem skapas i tid. Information om samhällets tekniska, sociala och organisatoriska utveckling samt resultatet av analyser och genomgångar av sårbarheter, beroenden och interdependenser utgör viktiga underlag för den strategiska analysen. Till området hör också fortlöpande bevakning och analys av utvecklingen i andra länder för att förstå omvärldsutvecklingen och ta del av goda exempel. Internationell och regional samverkan har stor betydelse för att möjliggöra en god civil sårbarhets och krishanteringsförmåga.

Fortlöpande planering och uppföljning genom bland annat sårbarhets- och beroendeanalyser gör det möjligt att medvetandegöra beslutsfattare och vikiga aktörer om hur resurser bör styras för att hantera oacceptabla sårbarheter. Det är också viktigt att genom information och olika utbildnings- och övningsinsatser medvetandegöra och träna viktiga aktörer och allmänheten. En ändamålsenlig ansvarsfördelning och ett bra regelverk är också grundförutsättningar för sårbarhets- och krishantering. En myndighet eller en så kallad *risk management* funktion inom t ex ett företag skall och bör inte frånta andra ansvaret för hanteringen av sina egna risker och sårbarheter, den skall se till att risker och sårbarhet hanteras av de verksamhetsansvariga och att beslut om riskacceptans fattas på rätt nivå.

När oacceptabla sårbarheter eller brister i krishanteringsförmåga har identifierats, värderats och förslag till åtgärder utarbetats måste dessa kunna finansieras. Det som utgör en del av det normala driftsansvaret finansieras normalt inom respektive verksamhet. Det finns sannolikt ett område där ansvaret bör delas mellan flera aktörer, det gäller särskilt hot och sårbarheter som involverar offentligt och privat samarbete och ömsesidiga beroendeförhållanden. Hot mot den nationella säkerheten är ett ansvar för staten och finansieras därför normalt med statliga medel. I bilden nedan åskådliggörs de viktigaste verksamheterna för att skapa en stark grund för en god civil sårbarhets och krishanteringsförmåga.

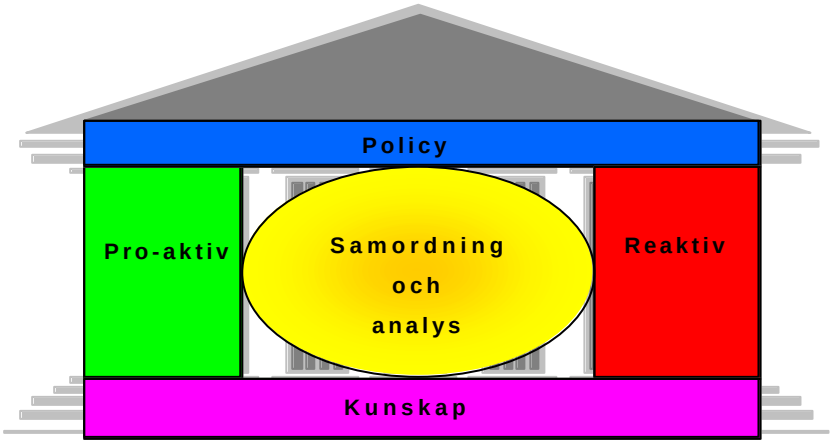
Grundläggande verksamheter för civil sårbarhets- och krishantering				
Kunskaps-utvecklande	Forskning	Utveckling	Studier	Forskarutbildning
Analyserande	Omvärldsanalys	Strategisk analys	FoU beställning	Delgivning
Förmågehöjande	Utbildning	Övning	Träning	Informations-beredskap
Medvetande-görande	Information	Kunskapsspridning	Mediekontakter	
Planerande, samordnande och uppföljande	Planering	Inriktning	Uppföljning	Rapportering
Regelutvecklande	Författningsarbete	Internationella överenskommelser	Folkrätt	
Partnerskaps-byggande	Inomoffentligt samspel	Samarbete med näringsliv och organisationer	Internationellt och bilateralt samarbete	Europeiskt och regionalt samarbete
Särskilda resurser för att hantera hot, risker, sårbarheter, kriser och konsekvenser	Personella	Organisatoriska	Materiella	Finansiella

Den civila sårbarhets- och krishanteringen innehåller tre huvudfaser, den *pro-aktiva*, den *re-aktiva* samt den *post-aktiva.* Ändamål och aktiviteter som ingår i dessa faser anges nedan i tabellen.

Pro-aktivt	**Reaktivt**	**Post-aktivt**
Sårbarhetsreducerande	**Skadehanterande**	**Lärande**
Analyserande och värderande	Indikering	Dokumentering och utredning
Hotanalys	Tvärsektoriell rapportering	Utvärdering
Sårbarhetsanalys	Analys	Analys
Beroendeanalys	Tvärsektoriell operativ varning	Lärande
Interdependensanalys	Information	Implementering
Medvetandegörande		
Informationsdelning	Skadereducering	
Standardisering och certifiering	Aktiva motåtgärder	
Validering	Konsekvenshantering	
Aktiv kontroll	Återställande av funktion	
Rapporterande och hanterande	Återuppbyggnad	
Underlag till regeringen		
Sårbarhetsfinansiering		
Investering och implementering		
Uppföljning och kontroll		

En fortlöpande verksamhet

Civil sårbarhets- och krishantering kommer att vara en verksamhet av betydelse för den nationella säkerheten, nu och framledes. Den starka föränderligheten och utvecklingstakten i samhället är en utmaning som ställer stora krav på samspelet mellan olika aktörer, men också på ett samspel mellan strategisk analys, forskning och utveckling samt planering och genomförande. Förståelse och stöd från policynivån är en förutsättning för framgång inom alla delar av samhället. Samspelet kan illustreras med följande figur.



4 Hotutveckling av betydelse för civil krishantering

Det säkerhetspolitiska läget

Fram till det kalla krigets slut var det i första hand militärallianser eller enskilda stater som kunde hota vårt nationella oberoende och vår territoriella integritet. Krig var synonymt med ett mycket stort antal samtidigt eller över tiden inträffade skadehändelser som ytterst kunde leda till att de legitima statsmakterna förlorade kontrollen över landet. Vårt totalförsvar var det svenska samhället omställt för krig. Denna omställning (mobilisering) krävde förflyttning, omorganisation, utrustning och tid.

Enligt regeringens bedömning ter sig ett invasionsföretag syftande till ockupation av Sverige inte möjligt att genomföra under de närmaste tio åren, förutsatt att vi har en grundläggande försvarsförmåga.[2] Väpnade angrepp, främst genom luften eller genom insatser mot begränsade mål i Sverige, eller andra typer av avsiktliga hot och påtryckningar är dock enligt regeringens bedömning möjliga att genomföra även i nuvarande omvärldsläge.

På det internationella planet har i dag lokala och regionala konflikter som tidigare dämpades av det kalla kriget fått ett större utrymme. Gångna tiders stormaktsinblandning har ofta ersatts av ofta av grannstaters intervention. Detta förhållande riskerar emellertid samtidigt att sänka tröskeln för att regionala konflikter skall, på grund av det ökade samberoendet, ge efterverkningar även på det internationella planet. Ett svenskt deltagande vid internationella, fredsfrämjande insatser vid denna typ av konflikter riskerar att öka landets exponering för grupper eller stater som kan ha för avsikt att hota det svenska samhällets säkerhet.

Under de senaste åren har även de beroendeförhållanden som den fortgående ekonomiska integrationen mellan stater medför kommit allt mer i blickpunkten. Ekonomins globalisering får allt större betydelse för enskilda länder och sätter samtidigt gränser för den nationella handlingsfriheten. De ekonomiska och handelspolitiska frågorna väger samtidigt tyngre i relationerna mellan världens länder och har därmed också fått större säkerhetspolitisk betydelse. Idag kan en aktör genom ekonomiska medel angripa en stat utan att ha kontroll över dess territorium. Parter i konflikter, som kan vara grupper av länder, enskilda sådana eller icke-statliga organisationer eller rörelser, kan vilja påverka omvärlden t.ex. genom att störa försörjningen med strategiska varor och genom sabotage, terror och utpressning.

Nya hot

Aktörer

Framväxten av aktörer som hotar säkerheten i samhället har ökat under de senaste decennierna. Dessa utgör en ny form av hot som benämns asymmetriska, det vill säga att aktörerna inte nödvändigtvis är stater eller grupper av stater, utan grupper som formeras kring en gemensam ståndpunkt. Dessa subnationella grupper kan angripa en stat, men då med andra angreppssätt än de traditionella. Kostnaderna för att skydda sig mot hoten överstiger dessutom i allmänhet

[2] Ds 2001:44, Ny struktur för ökad säkerhet – nätverksförsvar och krishantering, s 49 och Proposition 1998/99:79 Förändrad omvärld –omdanat försvar, s 9 samt Prawitz J, ”Kärnvapenrisker i Europa”, se bilaga

kostnaderna för att verkställa dem. Tröskelsänkande faktorer, såsom de alltmer utvecklade globala kommunikationerna, det komplexa moderna samhället och tillkomst av och tillgång till nya typer av vapen och andra medel för påverkan, gör det möjligt även för små grupper att få stor verkan över stora områden och avstånd.

Vissa av dessa subnationella grupper av aktörer betecknas som terrorister. Själva kan de däremot uppfatta sig som politiska frihetskämpar. Få av dessa grupper är enbart terrororganisationer. Ofta använder sig organisationerna av terrorn som ett verktyg i kampen att nå sina mål. Den trend som den internationella terrorismen följt under 90-talet har främst utmärkts av två, delvis motstridiga tendenser. Å ena sidan har antalet terrordåd minskat under det senaste decenniet jämfört med 80-talet. Samtidigt har dåden, i takt med att den religiöst/sekteristiskt motiverade terrorn ökat, blivit blodigare och ”dödligare”. Således har färre dåd begåtts, men fler människor har dödats och skadats.

Under senare år har riskerna för spridning av massförstörelsevapen och farhågorna för terroristaktioner med sådana vapen uppmärksammats i allt större utsträckning. De fall när en sådan spridning av massförstörelsevapen faktiskt skett eller befaras ha skett är inte längre möjliga att betrakta som enbart lokala eller regionala hot. Skulle massförstörelsevapen komma till användning kan framför allt de politisk-psykologiska konsekvenserna bli närmast oöverskådliga. Ett problem är att de stater som undertecknat konventioner kring minskning av innehav av massförstörelsevapen många gånger inte uppfyllt sina åtaganden. Dessutom har länder som Indien, Pakistan, Israel, Kuba och Nordkorea inte undertecknat konventioner. Arvet från det kalla krigets kapprustning skapar också problem, bland annat då kontrollen över de forna sovjetiska massförstörelsevapnen blivit mer osäker efter Sovjetunionens upplösning.

Teknikutveckling, IT-relaterade hot

I informations- och nätverkssamhället är aktörer och tillgång till tid för omställning inte givna på samma sätt som tidigare. Relativt resurssvaga ickestatliga grupper kan med hjälp av kunskap, kraftfulla verktyg och gränslösa nätverk orsaka allvarliga skador på viktiga infrastruktursystem och totalförsvaret. Internet och den ökade informationstillgången underlättar för antagonistiska aktörer att skaffa sådan information som gör det möjligt att med relativt små medel lamslå stora delar av samhället. Den nya tekniken möjliggör också attacker som syftar till att vilseleda och påverka allmänhet och beslutsfattare genom falsk information.

Angreppen mot IT-systemen kan vara av både fysisk och logisk natur. Med fysiska angrepp avses att någon orsakar en skada genom att t ex slå sönder, spränga eller anlägga en brand i en del av ett IT-system. Logiska angrepp är spridning av datavirus, dataintrång genom t ex analys av lösenord och annan otillbörlig användning av datakod. Intrång eller andra logiska angrepp kan ske av en subnationell grupp utan att den exponerar sig för upptäckt. Det kan ske via informationsnätverk från långa geografiska avstånd och via datorer i flera led. Obehöriga intrång i IT-system används också för spionerі.

En ny arena för angrepp har uppstått genom att sammankoppling och sammansmältning av viktiga funktioner och styrsystem sker i allt snabbare takt i samhället. Internet och andra nätverk för elektroniska informationstjänster ger inte bara tekniskt utvecklade länder och företag nya möjligheter att hantera information och system effektivare. Det ger också helt nya möjligheter för potentiella motståndare. I dag krävs det inte längre miljonarméer eller avancerad militär materiel för att angripa nationalstater.

NBC

NBC-frågorna har på senare år kommit att spela en allt mer framträdande roll i den förvars- och säkerhetspolitiska debatten, såväl i Sverige som internationellt. Det finns en lång rad drivkrafter bakom denna utveckling, bland annat har tillgången på befintliga substanser (agens) och teknologisk kompetens ökat i och med Sovjetunionens fall. Tillgången till information om tillverkning växer på Internet och ett ökat intresse för dessa typer av vapen finns från subnationella grupper/terrorister etc. Frågor rörande s.k. asymmetriska hot, med NBC-dimensioner, måste därför hanteras av totalförsvaret i stort på ett helt nytt sätt i ljuset av dessa omständigheter.

Hittills har utgångspunkten emellertid varit att en annan stat angriper Sverige med NBC-vapen och att det militära försvaret måste utrustas för att möta ett dylikt anfall. Med nya aktörer krävs det att resonemanget blir annorlunda. Subnationella grupper/terrorister har terrorn som mål. Vill dessa grupper slå till där mest skada uppstår, torde civila mål vara av större intresse än militära förband, då dessa har skyddsutrustning. Fokus för NBC-frågorna bör alltså därmed förskjutas från en militär till en civil hantering, samt från skyddsfrågor till att även omfatta aktörs-, access- och preventionsfrågor.[3]

Infrastruktur

Vid ett angrepp mot Sverige, vare sig det rör sig om ett regelrätt krig eller en terrorhandling, finns en överhängande fara för att landets infrastruktur drabbas av attacker av fysisk art. Att lamslå ett land genom att slå ut landets infrastruktur måste ses som en mer kostnadseffektiv åtgärd än att angripa väl försvarade militära mål. Det är därför av stort intresse att Sverige uppnår god kunskap om hur attacker har utförts mot infrastrukturen i länder liknande vårt eget. ÖCB har därför uppdragit åt FOI att studera hur Natos flygkrig mot Jugoslavien 1999 var organiserat och vilka effekter flygbombningen fick på den jugoslaviska infrastrukturen.[4] I förstudien konstateras det att Nato oftast angrep infrastrukturen med precisionsvapen, dels för att uppnå högre träffsäkerhet och dels för att hålla nere förlusterna i människoliv. Effekten av attackerna visade sig utslagsgivande, då t.ex. broar och elverk med lätthet slogs ut, vilket begränsade den jugoslaviska kommunikationen och elförsörjningen.

En långsiktigt verkande faktor som klimatutvecklingen kan komma att få betydelse för säkerhet och beredskap i samhället.[5] I flera globala klimatstudier anges en temperaturhöjning med 2,5 grader under de kommande 50-100 åren som sannolik. Tillsammans med en förväntad ökad årsnederbörd med ca 10-20 procent medför det effekter i alla naturmiljöer och i samhällets olika sektorer. Andra studier redovisar motstridiga resultat, där effekterna inte framstår som lika dramatiska.

Teknisk infrastruktur uppförs och anläggs emellertid ibland utan att tillräcklig hänsyn tas till väderhändelser (extremvindar och extrem nederbörd) som inträffar mycket sällan med nuvarande klimat. Risken för erosion, skred och ras ökar med intensivare hydrologiska förlopp och

[3] En temaskrift om NBC planeras att ges ut av FOI under första kvartalet 2002 på uppdrag av ÖCB. Under 2001 har FOI gett ut rapporten ”Avsiktliga utsläpp av skadliga ämnen. Spridning och samhällskonsekvenser” där skeendet kring tre sinsemellan fundamentalt olika katastrofscenarier analyseras. se bilaga

[4] Det är alltid vanskligt att dra slutsatser från en konflikt för att sedan överföra resultatet på svenska förhållanden. Jugoslavien och Sverige har dock mycket gemensamt när det gäller uppbyggnaden av totalförsvaret och infrastrukturen och det vore olyckligt att inte lära av konflikter i vår omvärld.

[5] SOU 2001:41 Säkerhet i en ny tid

kan hota infrastruktur som vägar, banvallar, broar, byggnader, dammar, avlopps- och vattenförsörjningssystem.

Samhället behöver en god förmåga att ingripa vid akuta händelser för att minska konsekvenserna vid framtida extrema väderhändelser. Särskilt svåra konsekvenser uppstår vid störningar i elförsörjningen eftersom samhällets andra delar är beroende av säker eltillgång. Till viss del kan känsligheten och sårbarheten minskas genom ett strategiskt uppbyggande av ökad säkerhet i elförsörjning och elreservkapacitet. Det är viktigt att kunskapsutvecklingen inom detta område drivs vidare så att det är möjligt att vidta åtgärder för att minska samhällets sårbarhet.

Inriktning av fortsatt arbete

För att kunna skydda samhället mot olika typer av störningar, intrång, angrepp eller förstörelse krävs ny kunskap. Den breddade hotbilden, samhällets föränderlighet och den snabba tekniska utvecklingen gör att villkor och förutsättningar för ett ändamålsenligt skydd är annorlunda jämfört med till exempel under det kalla kriget.

I den gråzon av hot som uppkommit efter nedtoningen av invasionsrisken är det viktigt att uppmärksamma de asymmetriska hoten som framförs av subnationella grupper. Dessa nya aktörer kan använda sig av okonventionella metoder, bland annat av cyberattacker och NBC-krigföring, för att uppnå sina syften. Hoten i vår omvärld är föränderliga och kräver förutom en flexibel syn på vad som kan utgöra ett potentiellt hot även en flexibel syn på åtgärder. Det är därför ytterst viktigt att följa och analysera utvecklingen i vår omvärld för att på så sätt vara uppmärksam inför nya typer av hot.

Forskning, utveckling och analys av samhällets utveckling utgör därför en oundgänglig del i en verksamhet som syftar till skydd av samhället och dess olika funktioner. Hot, risker, sårbarhet eller beroenden måste kunna beskrivas och förstås, liksom de delar av samhället som är eller kan bli utsatta. De nya hoten och svårigheten att avgöra om dessa hot vänder sig mot militär eller civila ökar behovet att samverka mellan forskning för civila respektive militära ändamål, särskilt med avseende på hot och skyddsåtgärder.

5 Skydd av samhällsviktig infrastruktur

Risker, beroenden och hot kan betraktas som komponenter i en sårbarhetsbild, där den totala sårbarheten kan beskrivas som summan av dessa komponenter. Det är bedömningar eller fastställande av en sådan total sårbarhet som bör fungera som underlag för beslut om åtgärder för skydd av den samhällsviktiga infrastrukturen.

Samhällsviktig infrastruktur kan beskrivas på följande sätt. I botten finns ett lager som är gemensamt för alla. Det är själva terrängen som på olika håll uppvisar skilda egenskaper med avseende på höjdskillnader, vegetation, geologi, hydrografi, meteorologi etc. I terrängen har människan ställt ut nästa lager i form av samhällen och byggnader, vägar, järnvägar, broar, tunnlar, flygplatser, hamnar o s v. Till detta kommer ett antal sektorsspecifika lager av vilka det finns i huvudsak tre olika slag; ett som har med sektorns själva funktion att göra – det den är till för (att uträtta), ett för funktionens tekniska aspekter samt ett för kontroll eller övervakning av funktionaliteten i sektorn.

På en aggregerad nivå skulle infrastrukturerna kunna delas in i sex olika sektorer: energi och teknisk försörjning, kommunikation, förvaltning, tjänster, transporter samt skydd.[6] Varje sektor innefattar ett antal specificerade funktioner enligt nedanstående exempel. I denna rapport behandlas främst fyra av de sex funktionerna. Dessa fyra är energi och teknisk försörjning, kommunikation, tjänster och transporter.

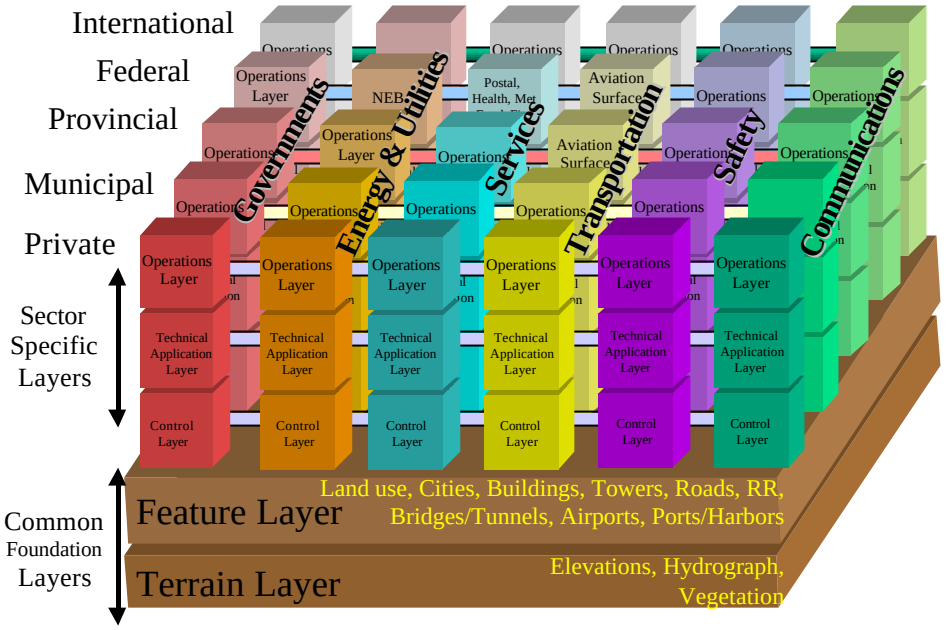
Energi och tekn försörjn	**Kommunikation**	**Förvaltning och ledning**	**Tjänster**	**Transporter**	**Skydd**
- el - vatten - avlopp - olja, petrol. - naturgas	- telekom. - television - radio - kabelnät	- statsförv - kommunal förvaltning - andra myndighetsfunktioner	- hälso- o sjukv - finansiella tj. - post - livsmedel - tull o gränskoll	- flyg - järnväg - landsväg - sjö	- räddningstjänst - kärnkraftssäkerhet - polis - farliga ämnen - ambulans - alarmering - kriminalvård - dammsäkerhet - miljöskydd - eftersök/fjällräddning - administration/byggn

Inom var och en av sektorerna fördelas ansvar mellan en rad olika nivåer. Det finns ett internationellt ansvar som utövas av olika över- eller mellanstatliga organ samt andra sammanslutningar över nationsgränserna. Det nationella ansvaret är i allmänhet statens, och inbegriper ansvar för såväl den egna infrastrukturen som för vissa verksamheter vilka är beroende av funktioner och tjänster som staten tillhandahåller. På regional nivå i Sverige har landsting samt länsstyrelser i egenskap av statens representant ansvar, och kommunerna svarar på den lokala nivån för sina delar av infrastrukturen. Sist, men inte minst, den privata sektorn kontrollerar en stor del av infrastrukturen, vilket också naturligtvis medför ett stort ansvar såväl som intressen som önskas eller bör skyddas.

Skyddet av den samhällsviktiga infrastrukturen är i högsta grad ett samverkansprojekt. Ingen enskild aktör kan sägas äga problemet eller sitta inne med den samlade kunskapen på området. Utbyte och arbete behöver ske över sektorsgränser och i partnerskap mellan offentliga

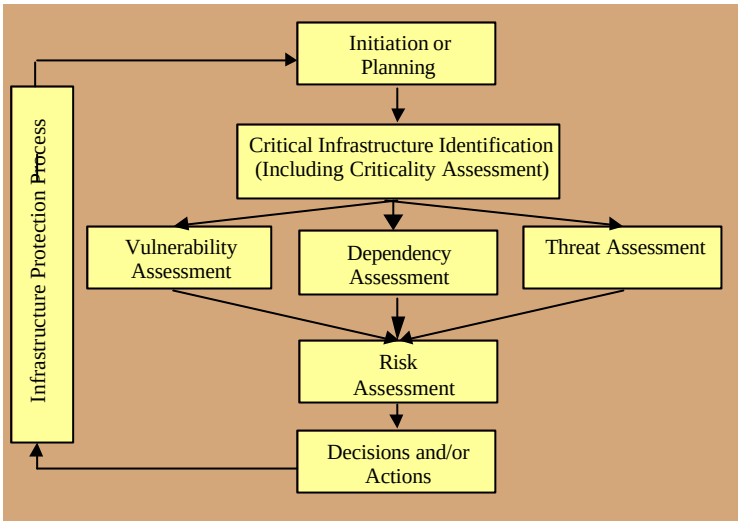
[6] Indelningen i de sex ovan nämnda sektorerna har använts bland annat i Australien, Kanada, Storbritannien och USA.

och privata aktörer. Grunderna för allokering av resurser, liksom de lagar och bestämmelser som omgärdar verksamheten, behöver därmed för närvarande förändras. Skyddet av den samhällsviktiga infrastrukturen bör givetvis utgå från en sådan helhetssyn, som illustreras av bilden nedan.[7]



Själva skyddet av infrastrukturer bör förstås som en *process* snarare än ett antal avgränsade åtgärder. De vidtagna åtgärderna påverkar själva grunden för besluten i nästa varv – hur det ser ut efter att de genomförts. Det gäller i själva verket dessutom oberoende av om de kan betraktas som framgångsrika eller ej. Skyddet kan ha försämrats eller det kan ha skett någon annan utveckling (kanske teknisk) som på ett eller annat sätt förändrar villkoren i termer av sårbarheter, beroenden eller hot. Det är viktigt att betrakta skydd som en dynamisk process, se bild på nästkommande sida.[8]

[7] Kanadensiska *Critical Infrastructure Protection Task Force* har producerat denna bild.
[8] ibid



6

Vad är samhällsviktig infrastruktur?

Det moderna samhället baseras på och är beroende av en väl fungerande infrastruktur. Omfattande störningar och påfrestningar på infrastrukturen kan leda till förlust av viktiga funktioner eller tjänster och i förlängningen att människor skadas. Det finns även infrastrukturer som har en särskild betydelse för andra infrastrukturer, samhällsfunktioner och samhället i övrigt, d.v.s. samhällsviktig infrastruktur. Framför allt är beroendet av teknisk infrastruktur såsom elförsörjning och telekommunikationer stort. Utvecklingen har lett till att många samhällsviktiga infrastrukturer använder sig av andra infrastrukturer, det ömsesidiga beroendet ökar. Ökad kunskap om samhällsviktig infrastruktur efterfrågas allt mer och är ett forskningsområde som ÖCB prioriterar[9].

Utveckling som påverkar samhällets infrastruktur

Utvecklingen i stora delar av världen präglas av föränderlighet då en övergång till informations- och nätverkssamhället sker. Internationella organisationer, stater, organisationer och individer måste nu alla anpassa sig till de nya förutsättningarna. Inom allt fler samhällsviktiga verksamheter används informationsnätverk för vitala lednings- och styrfunktioner. Genom att tillämpa de möjligheter som informations- och nätverkssamhället ger kan även krigskonsten revolutioneras. Det svenska försvaret omformas nu till ett nätverksbaserat system i syfte att uppnå informationsöverlägsenhet gentemot en motståndare. Försvarsmakten har för avsikt att till stor del basera det nya försvarssystemet på civil teknik och civil infrastruktur.

[9] ÖCB finansierar sedan maj 2000 ett ramforskningsprogram vid FOI för säkring av viktig infrastruktur. Dess syfte är att utveckla kunskap och bygga upp kompetens om såväl den fysiska infrastrukturen som de överlagrade informationsstrukturerna, och det inriktas mot grundläggande kunskaper om infrastruktursystem, interna och externa beroendeförhållanden, hotbilder, sårbarheter och konsekvenser av störningar i systemen samt möjliga skyddsåtgärder

Den nya tekniken och de nya möjligheterna ger emellertid också relativt resurssvaga grupper helt nya möjligheter att skada samhällets infrastruktur, vilket gör det än viktigare att vidta skyddsåtgärder. Enligt uppgifter från General Accounting Office (GAO)[10] vid vittnesmål inför representanthuset i USA i juli 2000 har mer än 100 länder utvecklat, eller är i färd med att utveckla, offensiv förmåga för angrepp med hjälp av IT. Många av dessa länder har en låg teknisk utvecklingsnivå, men utnyttjar möjligheten att med relativt små resurser bygga upp sin offensiva kapacitet. Subnationella grupper anpassar sig till nätverkssamhället och utvecklar kapacitet för ”nätkrig”. Det innefattar bland annat organisationsförändringar till mer flexibla ickehierarkiska strukturer och användning av internet som ledningssystem samt för att sprida vilseledande information.

I dag ökar beroendet mellan olika infrastrukturella system och de kan inte längre betraktas som separata enheter. Det har ÖCB belyst i det s.k. Infrastrukturuppdraget.[11] Komplexa beroenden mellan olika infrastrukturer, system och verksamheter i det moderna samhället kan resultera i oväntade och allvarliga problem. Därför är det viktigt att vidta åtgärder för skydd av infrastrukturer och att använda en helhetssyn vid planeringen av åtgärder.

Det ökade beroendet mellan de tekniska systemen har tydliggjorts i rapporten *Den tekniska infrastrukturens sårbarhet, funktion och säkerhet*. I den belyses även utvecklingen inom teknisksystem och hur det påverkar infrastrukturens sårbarhet.[12]

Energi och teknisk försörjning

Inom sektorn energi och teknisk försörjning ingår funktionerna elförsörjning, vatten- och avloppsförsörjning, olja och naturgas. I denna rapport behandlas de två först nämnda funktionerna då de har bedömts ha störst intresse för civil krishantering.

Elförsörjning

En fungerande elförsörjning är väsentlig för att levnadsstandarden ska kunna upprätthållas och för att näringsliv samt andra samhällsviktiga verksamheter ska kunna fungera. Ett elavbrott får därför ofta omfattande och kännbara konsekvenser för de flesta delarna av ett samhälle. Elförsörjningen är känslig för sabotage och extrema väderhändelser vilket leder till att samhället drabbas av påfrestningar. Dessa förhållanden belystes i Infrastrukturuppdraget.[13] Huvudteman var den oväntat stora sårbarheten i elförsörjningen och de stora inbördes beroendena mellan el och tele.

Elproduktionen i Sverige sker till stor del i delar av landet där konsumtionen ej sker vilket leder till långa överföringssträckor. Detta, i kombination med ett stadigt ökande elberoende, gör elförsörjningen sårbar. Det har även visat sig att utslagna ställverk eller andra noder tar mycket lång tid att bygga upp medan man, beroende på omfattningen, relativt snabbt kan reparera elnät.

---

[10] Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination (07/26/2000), T-AIMD-00-268
[11] ÖCB-rapport, ”Infrastrukturuppdraget – om sårbarheten i den tekniska infrastrukturen”
[12] Dellgar U, Thedéen T m.fl., ”Den tekniska infrastrukturens sårbarhet, funktion och säkerhet – TIS”, se bilaga
[13] ÖCB-rapport, ”Infrastrukturuppdraget – om sårbarheten i den tekniska infrastrukturen”

Det är viktigt att motverka sårbarheten i elförsörjningen. Ett sätt är att se till att det finns ett nät av kommunikationsvägar, redundans. Uppstår ett avbrott på en förbindelse ska elförsörjningen kopplas om till en förbindelse som har en annan sträckning.

Det ökande elberoendet och komplexiteten i systemen belystes av ÖCB i två OA-notiser som behandlade de elavbrott som drabbade Arlanda under våren och sommaren.[14] Även om skadeeffekterna begränsades till terminalerna och de interna informationssystemen så noterades en sekundär, men nog så alarmerande effekt: ansvariga vid flygplatsen var förbluffade över det inträffade och förmedlade i båda fallen ett budskap av att ”detta skall inte kunna hända”. Just denna överraskningseffekt noterades även vid en liknande men betydligt allvarligare incident vid Gardemoens flygplats i Oslo 1999. Vi vill har därför peka på en måhända oroande trend på ett mer allmänt plan: överraskningarna tenderar att bli allt vanligare i takt med samhällets ökade beroende av teknisk och komplex infrastruktur med flera aktörer och systemägare. ”Svarta lådan-syndromet” förefaller att bli vanligare.

Ett antal studier har gjorts med anknytning till de senaste årens stora elavbrott i utlandet. Elavbrotten 1998 i Auckland och i Kanada (i samband med den s.k. isstormen) samt avbrottet i Buenos Aires 1999 har analyserats i tre studier[15]. De lärdomar som kunnat dras av dessa tre likartade händelser är att omfattande elavbrott ofta får indirekta konsekvenser som man sällan kunnat förutse. Effekterna av elavbrottet påverkar ofta andra infrastrukturer och samhällsfunktioner. I värsta fall kan det leda till ekonomiska och/eller sociala kriser. Ledning och upprätthållande av förtroendet för samhällets förmåga är viktiga faktorer i denna typ av krishantering.

Fler studier om hur effekter av elavbrott kan mildras och hur funktionen elförsörjning kan återställas bedöms som angelägna.

Vatten- och avloppsförsörjning

En grundläggande förutsättning för människans överlevnad är tillgång på vatten av god kvalitet. Hoten mot vattenresurser ökar och blir mer mångskiftande. Det rör sig om allt från olyckor vid lokala verksamheter till global påverkan som försurning, växthuseffekt och spridning av radioaktiva ämnen och andra föroreningar. Det medför ett ökat behov av att identifiera, bedöma och värdera riskerna för att kunna prioritera och utforma skydd och andra förebyggande åtgärder. Den största användningen av infrastrukturområdet vattenförsörjning sker inom jordbruket, industrin, näringslivet, brandbekämpning och hushållen. Vattenförsörjningen till jordbruket och industrin hämtas i många fall utanför det kommunala VA-systemet. I vissa fall är dock industrin och jordbruket beroende av kommunal vattentillförsel och avbrott kan ge förödande konsekvenser.

Avloppssystem är oumbärlig del av infrastrukturen. Om avloppssystem inte fungerar finns det risk för allvarliga störningar, t ex för översvämningar med följdverkningar och miljöfarliga utsläpp. Liksom i övriga infrastrukturer ökar användningen av tekniska system för att optimera vattenförsörjningssystemets funktion, vilket i sin tur gör att nya typer av sårbarheter uppstår genom risk för intrång i dessa system.

[14] ÖCB, ”Omvärldsanalysnotiser 1/2001 och 3/2001” se bilaga
[15] FOI, Molin, S. och Fischer, G., ”Isstormen i Kanada”, FOI, Fischer, G. och Molin, S., ”Elavbrotten i Auckland”, CRISMART, Ullberg, S., ”The Buenos Aires Blackout” se bilaga

Inom området vatten- och avloppsförsörjning har ÖCB finansierat två studier under det senaste året.[16] I dessa har främst riskidentifiering av hot mot vatten- och avloppsförsörjningen redovisats. Det finns en efterfrågan på fler studier inom vattenförsörjningsområdet. En internationell utblick visar bl.a. att inom den amerikanska planeringen av programmet *Critical Infrastructure Protection* anges säkerheten av vattenförsörjningen som ett viktigt delområde. Inom detta område planeras forskning fokuserat på identifikation och detektion av smittbärare och toxiska kemikalier, sårbarhet i styr - och reglersystem, sårbarhetsanalys av vattenförsörjningssystem samt upprättandet av ett expertcentrum inom området. Det kan ge uppslag till nya forskningsprojekt avseende skydd av vattenförsörjningen i Sverige.

Kommunikation

Elektroniska informationstjänster

Teknikutvecklingen inom informations- och nätverkssamhället sker snabbare och snabbare. Ny teknik som baseras på digitala system, Internetprotokoll och nätverk leder till en sammansmältning av tjänster, system och marknader. Det som förut var separata system och avgränsade nätverk växer nu samman till elektroniska informationstjänster. Konvergensutredningen beskriver i sitt betänkande utvecklingen på följande sätt:

> Konvergens (sammansmältning) som fenomen kan beskrivas på olika sätt beroende på vilket perspektiv som diskuteras och hur graden av komplexitet varierar. Grundläggande är de förutsättningar som den tekniska utvecklingen medför för konvergens av infrastrukturer, tjänster och apparater. Till detta kommer de marknadsrörelser som innebär att aktörer inom olika sektorer engagerar sig i en eller flera angränsande sektorer. Utifrån Konvergensutredningens uppdrag är det relevant att beskriva konvergensens effekter i förhållande till nätkonvergens, tjänstekonvergens, apparatkonvergens och marknadskonvergens.[17] Konvergens leder till att sårbarheten i det moderna informationssamhället ökar.

Utvecklingen de närmaste åren

Sverige är idag världsledande när det gäller utbyggnad av nät för överföring av stora mängder information med hög hastighet och till låg kostnad. Befintliga infrastrukturer som vägar, banvallar och kraftledningsnät nyttjas i första hand för dragning av de fiberoptiska näten. Även mobiltelefoni kommer att kunna utnyttjas för s k bredbandsöverföring av information. På lokal nivå byggs mer finmaskiga fiberoptiska eller andra nät. Även här nyttjas i hög grad befintliga strukturer som t ex fjärrvärmenät. Dessutom kan elnätet användas för bredbandig överföring av information. I OA-notis nr 2/2001 redogjorde ÖCB för denna teknik, *Power Line Communication* (PLC), som går ut på att distribuera telekommunikation med bredbandskapacitet via det befintliga elnätet.[18] Tillgång till stora informationsmängder och fast uppkoppling till Internet kommer inte längre att vara förbehållet myndigheter, organisationer och företag. Även enskildas möjlighet att få tillgång till bredband ökar, i princip en möjlighet som ges till samtliga medborgare som så önskar. Det kommer att förändra vårt samhälle och skapa

[16] Chalmers, Rosén, L., ”Riskanalys för att värdera och hantera hot mot vattenresurser” Chalmers, Olofsson, B. m.fl. , ”Riskidentifiering av urbana VA-system” se bilaga

[17] Konvergensutredningen, SOU 1999:55, *Konvergens och förändring*, har bl.a. behandlat konvergensens (d v s tendensen att olika infrastrukturella system - såsom tele, IT, rundradio - tekniskt, tjänste- och aktörsmässigt gör intrång på varandras områden) konsekvenser ur ett rättsligt perspektiv. Det vill säga det tilltagande juridiska problemet att lagstiftningsmässigt hålla isär de tidigare så lätt urskiljbara infrastrukturella systemen och huvudmannaskapen för dessa.

[18] ÖCB, Omvärldsanalysnotis nr 2/2001 se bilaga

möjligheter för enskilda som det ännu är svårt att föreställa sig, såsom tillgång till information, kommunikation och delaktighet i beslutsprocesser.

Utvecklingen går mot att allt fler informationssystem kopplas samman i olika nätverk. Det uppstår komplexa system *av system*. Det kan inte förutsättas att någon samlad kunskap om alla informationstekniska nätverk kommer att finnas. Lokala trådlösa nätverk nyttjas redan inom många företag. Stora och komplexa tekniska system kan också drabbas av störningar på grund av fel hård- och programvara. Relativt små fel kan leda till kaskaderingseffekter där system efter system slås ut eller kommer i så kallad självsvängning.

Idag sker många intrång och andra datarelaterade brott genom handlingar av s.k. *insiders* d.v.s. personer som har tillgång till IT-systemen genom att de är behöriga användare eller personer som finns inom organisationen och på så sätt lättare kan skaffa sig en obehörig tillgång till IT-system. Internet underlättar för s.k. *outsiders* att göra intrång i viktiga IT-system och nätverk. Information om viktiga system kan insamlas via Internet och intrång kan sedan ske via ett sämre skyddat system som i sin tur ger tillgång till andra system och nätverk.

Allt detta förutsätter att säkerhet och skydd införs i de nya nätverken som skyddar individerna från olika typer av databrott och åtkomst av privat information. Ansvaret för att så sker åvilar statsmakterna, operatörer, nätverksägare och den enskilde. Stora krav kommer att ställas på enskildas säkerhetsmedvetenhet. Den stora tillgången till information kommer ställer stora krav på källkritik och kontroll av korrektheten i informationen. Genom intrång hos enskilda kan information som är oåtkomlig hos myndigheter och företag komma att insamlas.

Viktiga åtgärdsområden

Den utbredda användningen av IT-system i nätverksstrukturer och en angripares möjlighet att välja tid, plats och metod gör att proaktiva åtgärder som robusthet och skydd inte räcker. Angrepp på viktiga IT-system måste kunna upptäckas tidigt och den ordinarie driften återställas. Tidigt och samordnat agerande är avgörande för framgång, både när det gäller preventiv sårbarhetshantering och operativ krishantering.

En effektiv kris- och sårbarhetshantering kräver tvärsektoriell samordning och ett nära samarbete med näringslivet. Idag har ingen myndighet det övergripande ansvaret för informationsteknik (IT)-säkerhetsfrågorna. Ett organ för tvärsektoriell samordning är vidare nödvändigt för bilateralt och internationellt samarbete.

Det behövs ny kunskap för att kunna skydda IT-system mot angrepp. Utan betydande forsknings- och utvecklingssatsningar kommer inte effektiva åtgärder för att skapa robusta och säkra IT-system att vara möjliga.

Det nätverksbaserade militära försvaret

Under året har Försvarsmaktens koncept för framtiden, som tidigare kallades RMA (*Revolution in Military Affairs*) och nu benämns som Ny krigföring, analyserats ur ett civilt perspektiv. I en kommande ÖCB-rapport om implikationer för den civila infrastrukturen, beskrivs hur Försvarsmaktens vision för hur det framtida svenska försvaret skall ledas börjar ta form. Det kommer att bygga sin informationshantering och ledning på en i huvudsak civil infrastruktur (i första hand de civila telenäten). Detta medför att säkerheten och tillgängligheten i dessa civila system måste kunna garanteras på ett helt annat sätt än idag.

Skyddet av informationen i nätverket, *Information Assurance* (IA), är av avgörande betydelse för att konceptet skall fungera. Den nya militära försvarsmodellen ger upphov till ett antal frågor rörande civil sårbarhets- och riskhantering.

- Vilken grad av skydd av samhällsviktig infrastruktur är nödvändig för ett nätverksbaserat militärt försvar?
- Vilka skydds-, upptäckts- och försvarssystem behövs inom de militära och civila informationsinfrastrukturerna?
- Hur bör ett civilt ledningssystem vara utformat i framtiden?
- Hur kan resurserna inom det civila lednings- och informationssystemet användas i det militära systemet och omvänt?
- Vilka krav på nationella strukturer för skydd av samhällsviktig infrastruktur behövs när det militära försvaret är nätverksbaserat?

Det är uppenbart att betydande resurser, både civila och militära, kommer att behöva satsas de närmaste åren för att bygga upp ett skydd av samhällsviktiga infrastrukturer och ett nätverksbaserat försvar. Satsningar inom forsknings- och utvecklingsområdet har en nyckelroll för utvecklingen av såväl civil krishantering som militärt försvar.

En särskild fråga är hur ett lednings- och informationssystem för planering, sårbarhets- och krishantering bör vara uppbyggt med hänsyn till de möjligheter som nätverks- och informationssamhället erbjuder. Behovet av effektiv ledning och effektivt resursutnyttjande ställer också krav på möjlighet till gemensamt informationsutnyttjande för civil krishantering och militärt försvar. Mycket talar för att ett civilt system, i likhet med det militära, bör vara nätverksbaserat.

Båda systemen bör syfta till att uppnå informationsöverlägsenhet eller mycket god lägesuppfattning. Detta kan t.ex. ske genom att civila informationsdatabaser kan nyttjas i det militära systemet. Det militära systemets sensorer kan vara lämpliga att använda vid räddningsinsatser, eftersök eller vid asymmetriska angrepp mot svensk civilbefolkning eller viktiga samhällsresurser.

Tjänster

Finansiella tjänster

I takt med att ekonomin internationaliseras och den säkerhetspolitiska utvecklingen sker i en allt snabbare takt har kunskapsbehoven kring samvariationen av dessa fenomen ökat. Vidare har avregleringar och marknadslösningar inom områden som är av vikt för totalförsvarsförmågan i samhället skett successivt under de senaste 20 åren. Som exempel kan nämnas internationaliseringen av stora delar av den försvarsindustriella sektorn och avregleringen av el- och telemarknaden i Sverige.

Med detta som grund finansierar ÖCB ett flerårigt forskningsprogram inom området Ekonomi och Säkerhet. Programmet har pågått sedan december 1999 och omfattar forskare vid UI, Stockholms universitet och FOI. Uppdraget är att ur ett flerdimensionellt perspektiv analysera

relationen mellan just ekonomi och säkerhet och ur detta arbete har det under 2001 genererats flera intressanta rapporter[19].

Betalningsförmedling/utbetalningssystem har, inte bara av ÖCB, identifierats som varandes synnerligen kritiska delar av vårt samhälle. Fallerar dessa funktioner får detta långtgående och svåröverskådliga konsekvenser för samhället. ÖCB initierar därför under 2002 ett projekt lett av FOI om de statsfinansiella konsekvenserna av störningar i dessa system; hur påverkas egentligen samhällets olika aktiviteter och vad kostar dessa störningar?

Transporter

Transportsektorn kännetecknas i dag av effektiva tekniska system, avreglerade marknader, internationalisering, specialisering och stordrift. Transportarbetet har under flera år ökat med i genomsnitt ett par procent per år och prognoserna för de kommande tio åren talar för att denna ökningstakt fortsätter. Utvecklingen i transportsektorn och dess omvärld har såväl positiva som negativa konsekvenser för sektorns sårbarhet och för beredskapsarbetet.

Den tekniska utvecklingen bidrar till att komplexiteten och beroendeförhållanden mellan olika system ökar. Exempelvis är transportsektorn i behov av en kontinuerlig försörjning av drivmedel, reservdelar och elkraft för att fungera. Drivmedelsförsörjning, tågdrift, trafikledning samt godshantering i hamnar och lager är bara några exempel på transportsystemens elberoende. Beroendet av fungerande elförsörjning samt intakta IT-system gör transportsektorn mycket sårbar.

De övergripande infrastruktursystemen som samhället i större eller mindre grad är beroende av har, som tidigare nämnts, i sin tur blivit alltmer beroende av varandra. För att kunna identifiera sårbarheterna i systemen är det viktigt att identifiera transportsektorns beroendeförhållanden främst avseende el, tele och IT.

Befolkningsutvecklingen går mot en allt större koncentration till några få städer, vilket kräver en omfattande varudistribution och ökade trafikmängder i dessa städer. Storstäderna innehåller dessutom vissa mycket viktiga nav i transportsystemet och om dessa slås ut kommer återverkningarna att bli omfattande för hela landet. Av den anledningen blir det allt viktigare framöver att arbeta med risk- och sårbarhetsanalyser för dessa nav. Särskilt intressant är Arlandaområdet, Öresundsregionen och Göteborgs hamn.

Förutsättningarna för beredskapsarbetet kommer att förändras genom att det internationella inslaget i transportsektorn ökar. Därigenom blir det svårare att disponera transportresurser i händelse av en allvarlig säkerhetspolitisk kris. Det faktum att andelen internationella transportföretag som trafikerar Sverige har ökat gör att åtgärder för att säkra nödvändiga transporter bör ses över. Dessa kan vända sig direkt till berörda företag, till exempel genom möjligheten att skriva in klausuler i samband med trafikeringsavtal. Det kan också vara aktuellt att lyfta upp vissa beredskaps- och krishanteringsfrågor i internationella sammanhang.

Avreglering, konkurrensutsättning och privatisering är faktorer som antagligen kommer att få större betydelse i framtiden. Detta påverkar beredskapsverksamheten i hög grad genom att

[19] Utrikespolitiska institutet, Andersson, J. ”Hotbilder, ekonomi och säkerhet” Stockholms universitet och Westfalk, S. ”Läkemedel, EU och den nationella säkerheten” se bilaga

hänsynstagande till beredskapsaspekter, som tidigare var myndighetsuppgifter, nu i många fall måste läggas fast i avtal med privata eller offentligägda bolag. Avregleringen m.m. leder också till ett ökat konkurrenstryck med minskade marginaler inom transportföretagen som följd. Beredskapsverksamheten måste anpassa sig efter dessa ändrade förutsättningar och nya arbetssätt utvecklas för att skapa robusthet i infrastrukturen samt krishanteringsförmåga hos berörda aktörer.

En summering av tendenserna de senaste decennierna ger en bild av alltmer avancerade system och inbördes beroenden inom transportsektorn. Det finns flera sårbara punkter som kan leda till stora störningar. Transportsystemets ökade integrering med samhällets övriga system medför dessutom att allvarliga störningar i transportsystemet får större konsekvenser för samhället i framtiden.[20]

Exempel på angrepp mot samhällets infrastruktur

I några studier har exempel på hur samhällets infrastruktur kan drabbas vid olika typer av angrepp belysts. Exemplen har hämtats från terrorattacken mot USA och Natos flygkrig mot Jugoslavien. Det visar sig att om en infrastruktur slås ut påverkar det omedelbart även andra funktioner.

I samband med terrorattacken i USA genomförde FOI en snabbanalys av dessa händelser.[21] I ett av avsnitten har angreppens påverkan på flera av infrastrukturområdena behandlats och där berörs även konsekvenser för samhällets säkerhet. Vid terrorattacken i New York slogs stora delar av det mobila nätet ut, då två basstationer för mobiltelefoni fanns placerade på ett av de två WTC-tornen. Som en följd av detta använde New York-borna framförallt e-post för att kommunicera med anhöriga. I nyhetsbrevet Delete görs en genomgång av vilka effekter som terrorattackerna hade på infrastrukturen med särskild fokus på informationsinfrastrukturen.[22] Efter attackerna var stundtals e-post det enda kommunikationsalternativet. Det innebar att en stor del av informationsflödet från myndigheter och nyhetsbolag sköttes med hjälp av internet. Trots att vissa nyhetstjänster, t.ex. CNN.com och ABC News.com var ur funktion på grund av överbelastning fungerade internettrafiken förvånansvärt bra.

Användning av teknik för ledning och kommunikation vid kriser diskuteras i flera länder. En lösning som föreslagits är att utveckla de civila kommersiella systemen för mobiltelefoni för att ge dessa en ökad robusthet.

Speciellt under det akuta skedet av en kris är transportkapacitet en kritisk resurs. Behovet av speciella resurser samt det faktum att samhälles ordinarie flöden och transportvägar kan vara utslagna eller störda, ställer speciella krav på transportinfrastrukturen. Också i New York uppstod ett omfattande transportbehov.

---

[20] ÖCB, Enheten för transportsamordning ”Utvecklingen inom transportsektorn och konsekvenser för sårbarhet och transportberedskap” 2001-09-13 samt ”Uppdrag angående framtida inriktning för beredskapsverksamheten inom transportsektorn” dnr 6-1064/2000

[21] FOI , Avdelningen för Försvarsanalys ”Snabbstudie av terrorattacken mot WTC/Pentagon 11 september 2001 och dess konsekvenser”

[22] Försvarshögskolan, Delete 2001/10. Det är ett månatligt nyhetsbrev som ges ut av Informationskrigskansliet (IKK) vid Operativa institutionen, , på uppdrag av ÖCB. Nyhetsbrevet är en sammanställning av den omvärldsbevakning som sker vid IKK beträffande civil beredskap och skydd av kritisk infrastruktur gentemot informationsoperationer.

Skyddet av teknisk infrastruktur har till övervägande del varit inriktat på att skapa beredskap mot angrepp av olika slag. Exempelvis är de amerikanska programmen inom *Critical Infrastructure Protection* (CIP) främst inriktade mot att skapa en beredskap mot angrepp som innebär utslagning eller störning av driftsfunktionen. Terroristerna var vid terrorattackerna tvärtom beroende av att de tekniska infrastukturerna fungerade. Speciellt uppenbart är detta när det gäller utnyttjandet av inhemska amerikanska flygplan som ”missiler”. Troligen kommer fokus för skyddet av den tekniska infrastrukturen att utvidgas till att i högre grad omfatta skydd mot att terrorgrupper utnyttjar infrastrukturen för sina syften.[23]

FOI har i en förstudie analyserat konsekvenserna av Natos flygkrig för Jugoslaviens infrastruktur.[24] Några intressanta iakttagelser som man kan göra av luftkriget mot Jugoslavien är att infrastukturen är mycket sårbar för punktinsatser. Det behövdes bara en flygbomb för att slå ut en bro eller ett ställverk och det tar i båda fallen upp till ett år att bygga upp dessa igen. Utslagna kraftledningar kan däremot byggas upp relativt fort, undantaget i Jugoslavien var där de var dragna i flodövergångar. Jugoslaverna lyckades ibland även hitta provisoriska lösningar på hur man kunde komma förbi delvis utslagna ställverk. Då detta inte gick var den vanligaste åtgärden att låta distribuera den el som fanns tillgänglig inom separata delsystem s.k. ödrift. Vid ett angrepp mot Sverige, vare sig det rör sig om ett regelrätt krig eller en terrorhandling, så finns en överhängande fara för att landets infrastruktur drabbas av liknande attacker av fysisk art.

Vad Sverige kan lära sig av Jugoslaviens situation är behovet av redundans i elsystemet. Om delar av elnätet slås ut så måste det finnas möjlighet att kunna föra över distributionen på andra nät. Att förebygga att ställverk och liknande noder slås ut kan endast göras om man bygger in dem i djupa bergrum och/eller har ett starkt luftförsvar. Lösningar som dock är mycket kostnadskrävande.

Även annan infrastuktur drabbades av Natos flygbombningar, bl.a. broar. Militära mobila broar är sannolikt den enda lösningen mot detta. Anfall mot den jugoslaviska informationsspridningens infrastruktur fick dock begränsad verkan. Den serbiska televisionen kunde exempelvis återuppta sändningarna bara några timmar efter anfallen, troligen p.g.a. att reservsändningsplatser redan fanns förberedda. Att ha flera små fasta eller mobila enheter för telekommunikation är antagligen det effektivaste sätter att förebygga att telekommunikationen slås ut.

Inriktning av fortsatt arbete

Det är viktigt att samhällets infrastruktur skyddas. Sårbarheten ökar då samhällets funktioner har blivit mer komplexa. Väsentliga värden står på spel inför de nya påfrestningar som möter samhället. De olika infrastrukturerna blir mer och mer beroende av varandra, främst av elförsörjning och telekommunikationer. Inom flera av infrastrukturernas funktioner såsom finansiella tjänster, transporter, vatten- och avloppsförsörjning ökar användningen av allt mer avancerade system. Det ökade beroendet leder till att samhället blir än mer sårbart. Slås en av infrastrukturerna ut påverkar det omedelbart andra samhällsfunktioner.

[23] FOI , Avdelningen för Försvarsanalys ”Snabbstudie av terrorattacken mot WTC/Pentagon 11 september 2001 och dess konsekvenser”
[24] FOI, Wulff, P., ”Jugoslavienkriget 1999. Antagonism med humanitära restriktioner.” se bilaga

Inom forskningen rörande den samhällsviktiga infrastrukturen har ännu inte presenterats någon heltäckande beskrivning och förståelse för att utröna de olika funktionernas inbördes beroende. Det behövs därför ytterligare forskning och det är viktigt att utveckla metoder för att beskriva och analysera ömsesidiga beroenden.

Sammankopplingen av IT-system i nätverk ger en angripare möjlighet att med förhållandevis enkla och billiga medel åstadkomma stor skada i ett samhälle. Angrepp på viktiga IT-system måste därför kunna upptäckas tidigt, innan skadan blir omfattade. Idag har ingen myndighet det övergripande ansvaret för IT-säkerhetsfrågorna varken nationellt eller internationellt, vilket kan visa sig bli nödvändigt i framtiden.

Det nätverksbaserade militära försvaret, tidigare benämnt RMA och nu Ny krigföring, som är under utformning kommer av allt att döma att vara beroende av robustheten i den civila infrastrukturen. Detta leder till att samhället måste ställa ännu högre krav än tidigare på både skyddet av infrastrukturen i sig och skyddet av den information som förmedlas. Utvecklingen av ett framtida nätverksbaserat informations- och ledningssystem för den civila krishanteringen skulle kunna korrespondera med uppbyggnaden av det nätverksbaserade militära försvaret.

6 Skydd av civilbefolkningen

I en värld av ökat regionalt och internationellt samarbete och samberoende får den traditionella nationalstaten en mindre framträdande roll. Det är en paradox att i tider när medborgarnas behov av det skydd som nationalstaten kan ge dem är stor, leder utvecklingen mot ett globalt informations- och nätverkssamhälle där nationalstaten får allt mindre möjligheter att kontrollera och påverka utvecklingen. Ett sätt att ge medborgarna det nödvändiga skyddet är att aktivt delta i bilateralt, regionalt och internationellt samarbete.

Våra föreställningar om hur och varför civilbefolkningen skall skyddas är nära förknippade med våra föreställningar om hur krig har och kommer att gestalta sig. Särskilda organisationer och resurser har byggts upp inom det område som kallas befolkningsskydd. Till detta kommer det vardagliga samhällets skydd i form av polis, räddningstjänst, ambulans- och akutsjukvård. Risken för och erfarenheter från hantering av smittsamma och dödliga sjukdomar samt katastrofer och terrorism har också inneburit en viss resursuppbyggnad och framför allt övning och kunskapsuppbyggnad.

Den svenska modellen för säkerhet och försvar bygger i huvudsak på att de sektoriserade fredstida strukturerna inordnas i ett väl samordnat totalförsvarssystem. Resurserna inom totalförsvaret är till stora delar fortfarande anpassade för ett storskaligt territoriellt krig med möjlig användning av NBC-vapen från motståndarsidan. Civilbefolkningen, kulturhistoriskt viktiga föremål, anläggningar som innehåller farliga krafter har ett särskilt folkrättsligt skydd. Detta beaktas också i den svenska totalförsvarsplaneringen. Verksamheten i fred bygger således i hög grad på myndigheternas självständiga ansvar att sköta sina uppgifter och samverka med andra myndigheter.

Nytt skyddstänkande

Under det kalla kriget var det möjligt att sortera ansvar och befogenheter efter faktorer som krigsfara, krig, höjd beredskap m.m. Som tidigare beskrivits i kapitel 4 har hotbilden förändrats. De nya hoten riktas i många fall mot civilbefolkningen, byggnader och anläggningar som har ett särskilt folkrättsligt skydd. Den breddade hotbilden, samhällets föränderlighet, nya aktörer och den snabba tekniska utvecklingen gör att villkor och förutsättningar för ett ändamålsenligt skydd är annorlunda jämfört med tidigare. För att förstå och analysera hotutvecklingen med inriktning mot aktörsperspektivet fordras ökade insatser. Samverkan mellan forskning och underrättelsetjänst har här stor betydelse.

När det gäller utformningen av skyddet för civilbefolkningen bör också hotet från långräckviddiga missiler och styrda precisionsvapen uppmärksammas. I en studie, gjord av FOI på uppdrag av ÖCB om Jugoslaviens civila försvarssituation under bombkriget 1999, visas att en angripare som vill undvika civila offer med stor framgång kan använda sig av precisionsbomber i en kombination med att angripa vid tidpunkter då befolkningen inte befinner sig i närhet av målet.[25] Det svenska luftförsvarets effektivitet ger motståndaren mindre möjligheter att bekämpa mål med precisionsvapen vilket skulle kunna leda till att angriparen får mindre precision med större civila offer som följd.

[25] FOI, Wulff, P., ”Jugoslavienkriget 1999. Antagonism med humanitära restriktioner.” se bilaga

Med den nya hotbilden som utgångspunkt bör uppbyggnaden av befolkningsskyddet breddas från att främst gälla höjd beredskap till att även omfatta skydd vid svåra påfrestningar och kriser. Skyddet av civilbefolkningen i Sverige bör grunda sig på en risk- och sårbarhetsanalys som beaktar hot, risker, befolkningskoncentrationer, viktiga samhällsfunktioner, livsnödvändiga infrastrukturer och särskilt utsatta objekt. Verksamheter av betydelse för den nationella säkerheten bör särskilt uppmärksammas.

Det är rimligt att se åtgärder för att skydda civilbefolkningen i tre faser, nämligen:

- Skydda, förebygga
- Upptäcka
- Reagera

En annan viktig fråga är olika system för upptäckt, indikering, av främmande ämnen i luft eller vatten. Utan tillräckligt effektiva indikeringssystem kan inte civilbefolkningen varnas och skyddas. Tillgång till personlig skyddsutrustning har här stor betydelse. I anslutning till utsatta platser eller verksamheter kan utrustningen behöva vara mer tillgänglig än idag. Personal som har att hantera konsekvenserna av NBC incidenter bör har adekvat skyddsutrustning och vara samövade.

Ytterligare ett område där skyddet av civilbefolkningen är intressant är det faktum allt fler blir uppkopplade mot Internet med bredband eller andra former av fast uppkoppling, där användaren är ständigt ansluten till Internet. I takt med att beroendet av ostörd tillgång till information och informationsnätverk ökar, ökar även behovet av att skydda informationen mot att ändras, förstöras, exploateras eller att kommunikationen på annat sätt avbryts.

Åtgärder för att skydda civilbefolkningen måste också bygga på förmåga till egenskydd. För det ändamålet fordras väl avvägda insatser för information, utbildning och övning i syfte att höja civilbefolkningens förmåga och riskmedvetenhet. Insatser mot och hanteringen av konsekvenser av svåra påfrestningar måste kunna ske samordnat och med ett så stort utnyttjande av samhällets samlade resurser och kunskap som möjligt.

En bredare inriktning på skyddet av civilbefolkningen ger även mervärde på angränsande områden. En bra förståelse för och förmåga att hantera de nya hoten såsom terrorism med massförstörelsevapen ger goda förutsättningar att kunna bidra till skyddet av civilbefolkningen i andra länder och vid internationella fredsbevarande eller fredsframtvingande operationer. Även anpassningsförmågan mot väpnat angrepp och beredskapen mot olyckor med farligt gods och utbrott av smitta stärks.

Inriktning av fortsatt arbete

En första scenariobaserad studie i syfte att kartlägga viktiga åtgärdsområden avseende skydd av civilbefolkningen bör initieras inom senast något år. När det gäller forskningsinsatserna inom NBC-området avseende skydd av civilbefolkningen bör en relativt större del användas för att studera aktörsperspektivet och konsekvenserna för civil krishantering av NBC-hotet.

Det krävs ökade insatser för att stärka samhällets förmåga att hantera komplexa skadesituationer där massförstörelsevapen använts. Både avseende skydd av infrastruktur och skydd av civilbefolkningen är viktiga områden lednings- och informationssystem, kunskaps- och erfa-

renhetsöverföring, utbildning, övning och investeringar i materiel för kris- och konsekvens-hantering. För dessa områden bör dimensionerings- och resursfrågor också beaktas.

7 Hantering av hot, risker, sårbarhet och kriser

I dag står samhället inför en annorlunda hot- och risksituation än tidigare. Krigshotet förefaller alltmer avlägset, men nya hot och risker uppträder i dess ställe. Dessa är svåra att förutse och att bedöma samtidigt som de orsakar svåra påfrestningar på samhället. De kan dessutom uppkomma snabbt. För att kunna hantera de nya hoten i samhället gäller det att vara beredd på det oförutsedda.

Det krävs goda och systematiska analysmetoder och modeller för att göra det möjligt för samhället att skydda sig mot samt upptäcka och reagera på påfrestningar. Efterfrågan på analyser ökar vilket gör det än viktigare att utveckla nya metoder och modeller som kan belysa de svåra och krävande situationer som samhället ställs inför.

Analyser inom risk- och sårbarhetsområdet används till att belysa de två momenten, sårbarhetsreduktion och upptäckt. Krishanteringsanalyser är viktiga då de visar på samhällets förmåga att reagera på och hantera påfrestningar.

Risk- och sårbarhetsanalys

I risk- och sårbarhetsanalys definieras risk vanligen som sannolikheten att något oönskat inträffar samt konsekvenserna av detta. Sårbarheten är det samlade resultatet av risker och ett samhälles, en kommuns, ett företags eller en organisations förmåga att hantera och överleva inre och yttre påfrestningar. Sårbarhet kan förstås som en funktion av hot, risk, känslighet och skydd samt förmåga:

- Sårbarheten ökar om hotet eller känsligheten ökar,
- Sårbarheten ökar om skyddet blir mindre effektivt eller förmågan att hantera hotet eller risken minskar
- Sårbarheten ökar om kris- och konsekvenshanteringsförmågan minskar

Helhetssyn och ett metodiskt och systematiskt arbetssätt är grundförutsättningar för en framgångsrik hantering av hot, risker och sårbarheter. Det är ett arbete som bedrivs före, under och efter en kris.

Sårbarhetsanalyser används ofta som beslutsunderlag för en nation eller en kommun när de avgör vilka åtgärder som ska vidtas för att hantera risker och dess konsekvenser. En metod som används vid sårbarhetsbedömning är Geografiskt Informationssystem (GIS) som visar den geografiska spridningen av risker. Risker återfinns naturligtvis även inom olika funktioner i samhället och en metod som belyser den funktionella riskspridningen efterfrågas allt mer.

Inom området risk- och sårbarhetsanalys har ÖCB under det senaste året finansierat ett antal forskningsprojekt samt deltagit i uppbyggnaden av ett internationellt kunskapsnätverk. Forskningsprojekt med inriktning risk- och sårbarhetsanalys har under det senaste året bedrivits vid Lunds universitet och Chalmers. I Västra Götalands län genomför ett antal kommuner risk-

analys med stöd från ÖCB. ÖCB har också inlett ett samarbete med den federala tekniska högskolan i Zürich om en elektronisk plattform för dialog och samverkan inom riskanalysområdet.

Forskningsprojekt vid Lunds universitet

För att kunna bedöma ett samhälles sårbarhet är det viktigt att genomföra risk- och sårbarhetsanalyser på nationell och lokal nivå. Risker behöver ofta hanteras lokalt, i Sverige på kommunal nivå. Det är därför angeläget för kommuner att kunna bedöma risker samt få insikt om hur de kan bemästras. Forskargruppen LUCRAM (Lunds universitets centrum för riskanalys och risk management) har behandlat risker och sårbarheter på lokal nivå. Här redogörs för tre av deras forskningsprojekt.

I ett av dem presenterar LUCRAM ett alternativt angreppssätt på riskanalys.[26] I projektet föreslås att flera objekt bedöms sammantaget och då sociala, ekologiska, tekniska och ekonomiska aspekter integreras i bedömningen ges en bättre uppfattning av risksituationen. I ett annat projekt behandlas sårbarhetsanalys och kommunal sårbarhetsrevision. Resultaten presenteras i en rapport, i vilken det redovisas ett antal metoder för att bedöma och jämföra kommunal sårbarhet.[27] En diskussion förs även om möjligheterna att utveckla en modell av riktat stöd till kommunerna för deras sårbarhetsarbete. Rapporten har varit ett av många underlag till utredningen Säkerhet i en ny tid.[28]

I samband med uppbyggnaden av forskningsområdet Sårbarhetshantering, kommunal sårbarhetsrevision och statlig fördelningsmodell anordnade ÖCB och LUCRAM ett möte för att få till stånd en samlad diskussion kring sårbarhetsfrågor.[29] Vid mötet presenterades först ett antal metoder avseende riskanalys och därefter diskuterades för- och nackdelar med dem.

Forskningsprojektet Sårbarhetshantering, kommunal sårbarhetsrevision och statlig fördelningsmodell inleddes under våren 2001.[30] Projektet är ett betydelsefullt och viktigt moment i utvecklingen av risk- och sårbarhetsanalyser. Det ska resultera i en modell för att mäta sårbarhet i kommuner samt ge förslag till ny planeringsmodell avseende fördelning av medel från centralt håll. När det gäller sårbarhetshantering kommer man i projektet att utveckla och pröva en dator- och internetbaserad metod för kommunal sårbarhetsrevision. På kommunal nivå ska den utgöra grunden för kommunala åtgärdsplaner. På central myndighetsnivå ska den ge en samlad bild av sårbarheten på kommunal, regional och nationell nivå och underlätta framtagandet av centrala åtgärdsplaner.

Vid framtagandet av en statlig fördelningsmodell måste hänsyn tas till skilda riskbilder samt de riskkällor av regionalt och nationellt intresse som finns inom en kommun. En kommun eller en region kan hysa riskkällor som inte bara har lokal påverkan utan har regional och nationell betydelse. Den viktigaste frågan vid konstruerandet av modellen blir hur kommuner och regioner med olika sårbarhetsbilder på bästa sätt ska stimuleras och stödjas.

---

[26] Lunds universitet, Magnusson, S.E. m.fl. ”Integrerad regional riskbedömning och riskhantering” se bilaga
[27] Lunds universitet, Nilsson, J. m.fl. ”Sårbarhetsanalys och kommunal sårbarhetsrevision” se bilaga
[28] SOU 2001:41 ”Säkerhet i en ny tid”
[29] Lunds universitet och ÖCB, workshop ”Tvärsektoriell risk- och sårbarhetshantering på lokal och nationell nivå” se bilaga
[30] Lunds universitet, Nilsson, J. m.fl.. m.fl. ” Sårbarhetshantering, kommunal sårbarhetsrevision och statlig fördelningsmodell” se bilaga

Övriga forskningsprojekt

Västra Götalandsprojektet har bedrivits i kommunerna i Västra Götaland om robusthet och risker. Ett grundläggande syfte vid arbetet har varit att bygga riskbedömningar på ett brett och tvärsektoriellt underlagsmaterial som arbetas fram vid en riskinventering.

I två forskarrapporter från Chalmers har, som nämnts tidigare, risker inom vattenförsörjningsområdet behandlats. Den första är en riskanalys av hot mot vattenresurser.[31] I den ges en översikt över metoder som kan användas vid värdering av hot, både kvalitativa riskklassificeringsmetoder och kvantitativa riskanalyser presenteras. I den andra redovisas en genomgång av de riskhändelser som kan uppstå i svenska VA-system[32]. Studien ska ses som ett samlat försök att identifiera riskhändelser på likartat sätt inom hela VA-verksamheten. Kommuner ska sedan kunna använda den i sitt riskanalysarbete.

Internationellt samarbete

Under det senaste året har ÖCB inlett ett samarbete med Zürichs tekniska högskola om en elektronisk plattform för dialog och samarbete inom riskanalysområdet. Projektet koordineras och utvecklas av *Center for Security Studies and Conflict Research.*

CRN är en dialogplattform för metoder, arbetssätt, verktyg och fallstudier för nationellt riskprofilarbete. Den stöds av den schweiziska regeringen som en del av landets deltagande i Partnerskap för fred (PfF). CRN ska vidare göra det möjligt för partnerstaterna inom PFF och det Euroatlantiska partnerskapsrådet att jämföra sina insatser och utbyta erfarenheter inom riskhanteringsområdet på nationell och lokal nivå. CRN bedöms bli ett mycket användbart verktyg för forskare och praktiker inom risk- och krishanteringsområdet samt bidra till att sprida och utbyta forskningsresultat. Den är därför av intresse för civil krishantering i Sverige.[33]

ÖCB och ledningen för CRN har tillsammans genomfört två workshops. Den första behandlade Riskanalys i Europa och genomfördes i Uppsala i april 2001. Temat för den andra var Säkring av kritisk infrastruktur och hölls i Zürich i november 2001.

Krishantering

Samhället blir allt mer komplext och därmed mer sårbart. Det leder till att fler kriser uppstår där betydande värden står på spel, begränsad tid står till förfogande och omständigheterna präglas av betydande osäkerhet. Det är viktigt att samhället kan hantera dessa akuta situationer. Krishantering visar på samhällets förmåga att reagera på och hantera svåra fredstida påfrestningar.

Med krishantering avses alla de åtgärder som under eller efter en allvarlig kris vidtas för att motverka de skadeeffekter som krisen åstadkommer. Det är svårt att vid en kris avgöra vilka insatser som bör anses vara krishantering och vad som bör anses vara normalt återställningsarbete efter en olycka eller skada. En förutsättning för att det ska kunna definieras som krishantering är att arbetet startar omedelbart efter det att krisens akuta skede är över och att det

[31] Chalmers, Rosén, L., ”Riskanalys för att värdera och hantera hot mot vattenresurser” se bilaga
[32] Chalmers, Olofsson, B. m.fl. , ”Riskidentifiering av urbana VA-system” se bilaga
[33] Mer information kring samarbetet finns på http://www.isn.ethz.ch/crn/index.cfm

är tydligt kopplat till krisens konsekvenser. Åtgärderna bör vara relativt omfattande och avvika påtagligt från det normala arbetet i berörda organisationer och verksamheter.

Det är viktigt att inse att en kris inte kan hanteras isolerat på en samhällsnivå, såsom den lokala, regionala, nationella eller internationella. Det är de ömsesidiga kopplingarna mellan dessa nivåer som är centrala både för uppkomsten av risker och kriser och för deras framgångsrika hantering. Nationell krishantering måste därför sättas in i ett internationellt perspektiv.

Svåra kriser kan leda till att det blir uppenbart för de politiskt ansvariga att framtida insatser i liknande hotande situationer kan förbättras genom att öka tillgängliga resurser för planering, informationsinhämtning och analys inom krishanteringsområdet. Det ligger i statsmakternas intresse att bidra till en ökad krishanteringskompetens då akuta och svårhanterade kriser kan få direkta konsekvenser för Sveriges säkerhet.

De tidigare refererade rapporterna om elavbrott beskriver även vad som har fungerat bra och mindre bra vid krishantering. Vid elavbrottet i Buenos Aires fungerande inte beslutsprocessen hos de ansvariga organen och kommunikationen med allmänheten fallerade.[34] För flera av aktörerna vid elavbrotten i Kanada 1998 kan huvuddelen av svagheterna i krishanteringen hänföras till en bristfällig planeringsprocess.[35] Elkrisen i Auckland gav en god illustration av hur beroende ett modernt samhälle är av en fungerande infrastruktur och hur pass beroende man är av en infrastrukturoperatörs krishantering. I Auckland gavs ett exempel på hur ett infrastrukturföretag i en krissituation kan få en utökad roll i krishanteringen, som går utöver rollen att endast hantera påfrestningar i de egna systemen.[36]

Kriserfarenhet kan leda till ökad skicklighet att hantera framtida krissituationer. I en studie, Agera och lära i kriser, har olika aktörers erfarenheter av kriser illustrerats. Genom bl.a. intervjuer har hur beslutsfattare och andra aktörer uppfattar och agerar inför risk-, hot- och krissituationer.[37]

Inriktning av fortsatt arbete

Samhället står idag inför en annorlunda risk- och hotsituation än tidigare då krigs- och invasionshotet dominerade. De nya riskerna är svåra att förutse och bedöma samtidigt som de kan orsaka svåra påfrestningar på samhället. Utvecklas riskerna och påfrestningarna till akuta och svårhanterade kriser, kan det få direkta konsekvenser för den civila krishanteringsförmågan. Därför ligger det i statsmakternas intresse att bidra till en ökad krishanteringskompetens. Risk- och sårbarhetsanalyser som kan ge ett bra underslag till beslutsfattare efterfrågas allt mer.

Det krävs bra analysmetoder och modeller för att göra det möjligt för samhället att skydda sig mot samt upptäcka och reagera på påfrestningar. Utveckling och framtagande av nya goda och systematiska analysmodeller och metoder inom risk- och sårbarhetsområdet samt inom krishantering bör prioriteras. Det kräver dock att mer finansiella resurser tillförs.

[34] CRISMART, Ullberg, S., ”The Buenos Aires Blackout” se bilaga
[35] FOI, Molin, S. och Fischer, G., ”Isstormen i Kanada” se bilaga
[36] FOI, Fischer, G. och Molin, S., ”Elavbrotten i Auckland” se bilaga
[37] Försvarshögskolan, Enander, A. och Johansson, A., ”Agera i och lära av kriser” se bilaga

Bilaga

Notiser från Analysenheten

Notis 2001/1: Elavbrottet på Arlanda - reservkraften fungerade (2001-04-11)

Ett större elavbrott inträffade kl 0745 måndagen den 9 april 2001. Avbrottet varade i ca 40 minuter men hotade aldrig de vitala funktionerna för flygsäkerheten kring flygplatsen. Däremot blev samtliga terminalbyggnader mörklagda inklusive datorerna vid incheckningen och hänvisningsmonitorerna. Även vissa delar av telefonväxeln samt bagagetransporterna och högtalarutropen slogs ut. Flygledartornet och ledljusen i terminalerna fungerade dock genom att reservkraften användes.

Orsaken till avbrottet var att matningen av elkraft skulle läggas om tillfälligt p.g.a de pågående byggnadsarbetena vid Arlanda. Detta misslyckades och vid försök till återuppkoppling till Vattenfalls kabel uppstod ytterligare problem. Från ansvarigt håll menar man att det var ett misstag att göra denna omkoppling under högtrafik. Reservsystemen vid Arlanda är dubblerade så att reservkraft skall säkra de vitala funktionerna för flygsäkerheten. Det innefattar främst flygledartornet med dess system för övervakning av luftrummet och kommunikation med flygplanen.

Notis 2001/2: Pågående prov med bredband via elnätet (PLC) (2001-05-31)

Sedan ett par år pågår försöksverksamhet med telekommunikation via elnätet. Elnätskommunikation, eller PLC (*Powerline Communication*), har förutsättningar att bli ett kraftfullt medium för bredbandsaccess. Det är framför allt energiföretagens gemensamma forsknings- och utvecklingsorgan, Elforsk AB, som sedan september 2000 drivit utvecklingen i ett projekt i samverkan med ett 40-tal svenska energiföretag samt det franska EdF.

Tekniken för PLC har utvecklats snabbt och de största nätföretagen står snart i begrepp att saluföra konceptet med Internet-anslutning via det befintliga elnätet på den öppna marknaden. Optimismen är stor om att man på allvar skall kunna konkurrera med de ordinarie leverantörerna inom telekomsektorn. Fördelarna med PLC är att elnätet används som accessnät. Elnätet är redan etablerat och mer utbyggt än såväl det gamla telenätet med kopparkabel som de nya fiberoptiska nät som f n installeras eller planeras (eluttag finns oftast i varje rum).

Notis 2001/3: Nytt elavbrott på Arlanda – reservkraften fungerade på nytt (2001-08-23)

För andra gången på mindre än ett halvår inträffade ett stort elavbrott på Arlanda flygplats. Avbrottet, som inträffade den 21 augusti klockan 18.55 och varade i drygt två timmar, hotade dock aldrig de vitala funktionerna för flygsäkerheten kring flygplatsen eftersom reservkraften för flygtrafiken fungerade. Konsekvenserna av elavbrottet var att samtliga terminalbyggnader blev mörklagda inklusive datorerna vid incheckningen och hänvisningsmonitorerna. Även högtalarutropen och vissa bagagetransporterna slogs ut. Ledljus fanns dock att tillgå. Orsaken till avbrottet var att ett äldre ställverk kortslöts. Brister i systemet gjorde att problemet fortplantade sig i nätet och slog ut den ordinarie strömtillförseln för hela flygplatsen. Tekniker kunde efter två timmar återstarta strömtillförseln men det tog ytterligare en timme innan de var säkra på var problemet låg och kunde börja vidta åtgärder.

Urval av forskningsrapporter och studier som har finansierats av ÖCB

Avsiktliga utsläpp av skadliga ämnen. Spridning och samhällskonsekvenser
(Jan Burman m.fl., Avdelningen för NBC-skydd, FOA)

Skeendet kring tre sinsemellan fundamentalt olika katastrofscenarier analyseras. I två av fallen är den verksamma substansen av det slag som normalt kopplas samman med B- och C-krigföring. I det tredje fallet handlar det om ett kemiskt ämne som alla dagar på året finns i stora mängder i tankbilar på de svenska vägarna.

I det första fallet handlar det om utsläpp av mjältbrandsbakterier (antrax) - utomhus och under sommartid - i en mellanstor stad i norra Sverige. I andra fallet är scenariot att en ensam förövare krossar en flaska med nervgasen sarin i en tunnelbanestation. Det tredje scenariot utspelas i en utomhusarena i en svensk storstad. Respektive scenario bygger på noggranna studier av yttre och inre miljöer och inte minst på den tekniska utformningen av t.ex. trapphallar, rulltrappor och vänthallsmiljöer. Också ett stort antal intervjuer med företrädare för räddningstjänst, lokalförvaltning och sjukvårdsorganisation i respektive ort har genomförts. De scenarier som valts bedömer vi vara fullt rimliga mot bakgrund av den kunskap som internationellt finns rörande hotbilder, teknisk kapacitet etc. Denna sannolikhet kan motiveras av de nya hotbilder som är en realitet då icke-statliga aktörer också kan komma i besittning av och faktiskt också bruka bakteriologiska och kemiska vapen, eller substanser som kan användas som vapen.

Temaskrift om NBC

ÖCB planerar tillsammans med FOI/Umeå en bok/skrift som ska komma ut under 2002, med ett brett spektrum av myndigheter som tänkt målgrupp. Syftet är att ringa in detta vida begrepp som många uppfattar som alltför komplext och mångdimensionellt för att kunna förstå fullt ut. Skriften ska behandla olika infallsvinklar som exempelvis aktörer, handel med och tillgång till olika agens och tekniker, organisationsfrågor samt tekniska frågor rörande indikering, skydd och sanering. Vidare är det planerat att några säkerhetspolitiska kännare/debattörer ska ge sin bild av området.

Skriften är tänkt att hålla en populärvetenskaplig ton som både ska förklara och nyansera, men även ställa en rad frågor som den tänkte läsaren ska ta till sig och fundera vidare kring.

Den tekniska infrastrukturens sårbarhet, funktion och säkerhet – TIS. Metodstudie med exemplet värmeförsörjning och dess stödsystem
(Uno Dellgar Tyréns, Torbjörn Thedéen, KTH, m.fl.)

Syftet med projektet har varit flerfaldigt med tyngdpunkt på följande:
- beskriva hur utvecklingen inom tekniksystem kan komma att påverka systemens funktionsförmåga och sårbarhet i förhållande till framtida hot, påfrestningar och krav.
- tydliggöra samband och beroenden mellan de tekniska systemen som har betydelse för deras sårbarhet, funktion och säkerhet.
- studera metoder för att beskriva och analysera sårbarhet, funktion och säkerhet som är anpassade för olika besluts- och planeringssituationer.

Rapporten fokuserar på studier av metoder som sedan tillämpats på värmesystem och tillhörande stödsystem. Arbetet har bedrivits genom en kombination av teoretisk metodutveckling och praktiska metodstudier i utvalda kommuner och energiföretag.

Studien belyser offentliga insatser och internationella initiativ för det offentliga åtagandet inom den tekniska infrastrukturen för robusta system. Vissa förslag ges på hur utvecklingen kan främjas i riktning mot ett mindre sårbart samhälle.

Isstormen i Kanada
(Georg Fischer och Staffan Molin, FOI)

En rapport från FOI där elsystemkollapsen i Kanada 1998 och dess konsekvenser studerats. Studien har fokuserats på att belysa effekterna för infrastrukturen, främst elförsörjning och telekommunikationer samt hur man där hanterade krisen. Även effekterna och katastrofhanteringen inom andra samhällsområden har studerats.

Elsystemkollapsen, som var en följd av den värsta isstormen i modern kanadensisk historia, hade effekter på många vardagliga och ekonomiska aktiviteter. Nödvändiga dagliga rutiner försvårades eller blev omöjliga att genomföra och situationen blev livshotande för människor och djur. Mycket omfattande insatser krävdes från hela samhället för att hantera situationen.

Några av de viktigare iakttagelserna som gjorts i studien är att:
- Den successiva och osannolika eskaleringen av krisen fördröjde krishanteringen.
- Det var viktigt att snabbt få en bild av effekterna av isstormen och uppkomna problem.
- Såväl nationella resurser som stöd från andra länder krävdes för att hantera situationen.
- Försvarsmaktens snabba och omfattande resursinsats liksom frivilliga och ideella insatser från privatpersoner, frivilligorganisationer och näringsliv var av stor betydelse. Samordningen av insatserna var dock mycket viktigt.
- Förberedd krishantering, gott ledarskap, personliga nätverk och effektiva kommunikationer var väsentliga.

Elavbrotten i Auckland
(Staffan Molin och Georg Fischer, FOI)

En rapport från FOI, där man på ÖCB:s uppdrag har genomfört en studie av de elavbrott som drabbade Auckland, Nya Zeeland, under 1998. Från den 22 januari till 20 februari havererade fyra av de fem kablar som försörjer Aucklands centrala affärsdistrikt, *Auckland Central Business District* (CBD). Via den kvarvarande kabeln kunde en begränsad mängd elkraft inmatas till området. Centrala teman i FOA:s studie är hur störningarna inom elförsörjningen hanterades och hur Auckland CBD drabbades av bortfallet av elkraft. Det krävdes såväl nationella resurser som stöd från andra länder för att säkra och återuppbygga systemet.

Några av de allmänna effekterna av elavbrotten var en ökad brandrisk och försämrad stadsmiljö till följd av vissa av de krisåtgärder som vidtogs. Under de veckor som elavbrotten varade evakuerades drygt 50 procent av affärsfastigheterna vid något tillfälle. Nästan 80 procent av företagen i det drabbade området flyttade åtminstone delar av sin personal. Vardagslivet försvårades allmänt och de flesta boende flyttade från sina bostäder under elkrisen.

The Buenos Airos Blackout – Corporate and Public Crisis Management in Argentina 1999
(Susanne Ullberg, CRISMART – Centrum för Krishanteringsstudier vid FHS)

Rapporten *The Buenos Aires Blackout* analyserar strömavbrottet och krisen som uppstod i dess kölvatten ur ett kognitivt-institutionellt perspektiv, i vilket beslutfattande och kommunikation är centrala processer. Aspekter som probleminramning, informationshantering, politisering av kriser och symboliskt agerande analyseras inom ramen för Buenos Aires och Argentinas kulturella och politiska kontext. Centralt för analysen är privatiseringsprocesser av den offentliga sektorn, vilka har varit högst aktuella reformer för den argentinska staten det senaste decenniet. Som sådan är rapporten också intressant ur ett svenskt perspektiv, då avregleringen av elmarknaden genomförts också i Sverige och viktiga frågor om krishantering i sfären mellan det privata och det offentliga, mellan marknad och stat, blir aktuella.

Riskanalys för att värdera och hantera hot mot vattenresurser
(Lars Rosén, Geologiska institutionen, Chalmers)

Rapporten inleds med en översiktlig beskrivning av riskhanteringsprocessen. Därefter presenteras två olika angreppssätt för att värdera hot - kvalitativa riskklassificeringsmetoder och kvantitativa riskanalyser. Genomgången av angreppssätt och metoder har i rapporten begränsats till sådana som kan tillämpas för att värdera hot mot vattenresurser med avseende på beredskap och krislägen. Författaren förordar ingen speciell metod utan anger att prioriteringen mellan metoderna måste göras utifrån det aktuella hotet. Han poängterar att de insatser som görs vid beredskap och krislägen tar samhälleliga resurser i anspråk och att det måste finnas metoder för att bedöma i vilken omfattning dessa insatser är motiverade. Riskanalys och riskhantering är ett strukturerat verktyg att värdera hoten både kvalitativt och kvantitativt. Det ger även en möjlighet att hantera dessa så att en högsta möjliga säkerhet uppnås utifrån tillgängliga resurser. Rapporten ger en bra översikt över riskmetoder som kan användas vid värdering av hot mot vattenresurser.

Riskidentifiering av urbana VA-system
(Birgitta Olofsson, Henrik Tideström och Johan Willert, Urban Water, Chalmers)

I denna rapport presenteras en genomgång av de riskhändelser som kan uppstå i urbana svenska VA-system. Dessa har normalt sett god driftsäkerhet men ibland händer det som inte får hända. Rapportens syfte är att identifiera och belysa riskhändelser inom vattenförsörjning, spillvatten- och dagvattensystem. Det är 75 olika riskhändelser som behandlas. För vart och ett av dem beskrivs frekvensen i ett avsnitt, i ett annat konsekvenserna samt i ett tredje orsakerna till riskhändelsen. Beskrivningarna koncentreras till identifiering av händelsen som utgör risken samt hur ofta den inträffar, konsekvenserna däremot har behandlats mer översiktligt. Författarna poängterar att för att säkerställa VA-systemens funktion måste kommunerna fortsätta sitt riskanalysarbete för befintliga VA-system och riskidentifiering vid införande av nya systemlösningar. De säger att studien ska ses som ett samlat försök att identifiera riskhändelser på likartat sätt inom hela VA-verksamheten och att kommuner kan använda den i sitt riskanalysarbete. Rapporten ger en bra beskrivning av riskhändelsers frekvenser och orsaker.

Hotbilder, ekonomi och säkerhet
(Jan Joel Andersson, Utrikespolitiska institutet)

Denna rapport ger ett ramverk till hur den ekonomiska utvecklingen och den säkerhetspolitiska utvecklingen påverkar varandra samt hur fenomen som internationalisering/regionalisering inverkar på dessa inbördes beroende system.

Läkemedel, EU och den nationella säkerheten
(Sara Westfalk, SCORE, Stockholms universitet)

I takt med att de säkerhetspolitiska kartorna ritas om, genom kalla krigets slut och Sveriges inträde i EU, har den svenska synen på försörjningssäkerhet förändrats. Hur har detta påverkat läkemedelssektorn, hur ser försörjningspolitiken ut idag och finns dessa frågor på EU:s agenda?

Jugoslavienkriget 1999. Antagonism med humanitär restriktioner
(Petter Wulff, FOI)

Denna förstudien behandlar verkningarna på det civila samhället under Natos flygkrig mot Jugoslavien. Studiens tyngdpunkt ligger på skador på landets infrastruktur och dödsoffer bland civilbefolkningen.

Natos flyginsatser riktade sig till relativt stor del mot knutpunkter i den civila tekniska infrastrukturen. Elsystemet, tex noder för ett flertal ledningar i överföringssystemet samt stora elproduktionsanläggningar, utsattes till en början huvudsakligen för temporärt funktionshindrande insatser för att sedan slås ut helt. Efterhand som allt fler viktiga stationer i överföringssystemet drabbades av skador eller helt slogs ut övergick jugoslaverna till drift av separata delsystem med hjälp av lokal produktion, s.k. ö-drift.

Broar som anfölls raserades mer eller mindre fullständigt. Anfall mot den jugoslaviska informationsspridningens infrastruktur fick dock begränsad verkan. Den serbiska televisionen kunde exempelvis återuppta sändningarna bara några timmar efter anfallen, troligen pga att reservsändningsplatser redan fanns förberedda.

Nato hade allmänt deklarerat att man skulle hålla nere förlusterna i människoliv till ett minimum. Detta lyckades man i huvudsak med vilket förklarar de relativt få förlusterna av civila människoliv.

Integrerad Regional Riskbedömning och Riskhantering
(av Sven Erik Magnusson och Jerry Nilsson, Per-Olof Hallin LUCRAM, Lunds universitet och Bo Lenntorp, Institutionen för kulturgeografi, Stockholms universitet)

I denna rapport behandlas riskanalyser. I ett flertal fall fokuseras dessa på ett enskilt objekt i taget och riskbilden redovisas utifrån detta. Syftet med LUCRAM-projektet är att presentera ett alternativt angreppssätt där flera objekt bedöms sammantaget i riskanalysen. Genom att utgå från en rumslig avgränsning och integrera sociala, ekologiska, tekniska och ekonomiska aspekter i bedömningen kan man få en bättre uppfattning av en befintlig risksituation och få ett förbättrat beslutsunderlag.

Sårbarhetsanalys och kommunal sårbarhetsrevision
(Jerry Nilsson, Sven Erik Magnusson, Per-Olof Hallin, LUCRAM, Lunds universitet och Bo Lenntorp, Institutionen för kulturgeografi, Stockholms universitet)

En fördjupning av risk- och sårbarhetsanalyser ger LUCRAM i denna rapport. Först ges en internationell översikt över hur andra länder har hanterat säkerhetsfrågor (fokus på svåra påfrestningar). Norge, USA, Schweiz och Nya Zeeland ingår i översikten. Rapporten visar att i dessa länder betonas vikten av insatser på lokal nivå och vikten av att hantera risker pro-aktivt för att reducera samhällets sårbarhet.

Därefter presenteras ett antal metoder för att analysera, bedöma, presentera och jämföra kommunal sårbarhet. För att kunna föreslå lämpliga metoder/modeller är det nödvändigt att först försöka ta reda på hur arbetet med risker, sårbarhet och säkerhet fungerar och fortlöper i kommunerna i dag. Därför görs ett försök att identifiera några grundläggande drag i en mindre fallstudie, omfattande Helsingborg, Trelleborg och Perstorp. Slutligen förs en diskussion i rapporten om möjligheterna att utveckla en modell för fördelningen av riktat stöd till kommunerna för deras arbete med att reducera sårbarheten.

Sårbarhetshantering, kommunal sårbarhetsrevision och statlig fördelningsmodell
(LUCRAM, Lunds universitet)

Projektet startade våren 2001 och i den ska en metod för sårbarhetshantering, Robusta kommuner, utvecklas. Inom ramen för projektet ska även ett förslag till ny planeringsmodell för att fördela medel från centralt håll tas fram.

Agera i och lära av kriser. En förstudie om olika aktörers erfarenheter
(Ann Enander, Ann Johansson, Ledarskapsinstitutionen, Försvarshögskolan)

Utvecklingen inom det svenska totalförsvaret medför att ökade och mer komplexa krav ställs på olika aktörer att hantera ett brett spektrum av tänkbara påfrestningar. En förstudie har genomförts för att belysa hur beslutsfattare och andra aktörer uppfattar och agerar inför risk-, hot- och krissituationer. Studien syftar till att ge underlag för fortsatta studier och utveckling av stöd och omfattar tre delmoment. Det första är en explorativ intervjustudie med ett mindre urval totalförsvarsaktörer med skilda erfarenheter av beredskapsproblematik och av hantering av risk- och hotsituationer. I studiens andra moment har intervjuundersökningen kompletterats med analys av vissa data från en tidigare av FOA genomförd enkätstudie om kommunala aktörers syn på och erfarenheter av krisledning. Som tredje moment belyses den från intervjuerna framtagna modellen utifrån forskningslitteratur.

I en avslutande diskussion identifieras sex aktörsrelevanta problemområden för fortsatta studier och stöd: riskmedvetenhet och omvärldstolkning; hantering av olika roller utifrån vardagens respektive krisens krav; hantering av bilden av krisen; lärande utifrån inträffade händelser; utveckling av aktörers förmåga samt ledarskap vid svåra påfrestningar.

Kärnvapenrisker i Europa
(Jan Prawitz, Utrikespolitiska Institutet)

Fyra av de fem etablerade kärnvapenmakterna är närvarande på den europeiska kontinenten. Fortsatt nedrustning och minskning av kärnvapnens traditionella roll i Europa är den mest sannolika prognosen. På kort sikt kommer kärnvapnen knappast att spela någon militär roll.

En risk för att undernationella grupper kan komma över kärnvapen finns fortlöpande. Ett scenario för detta fall beskrivs. Politiskt kommer kärnvapenmakterna att hålla på sina kärnvapen för att manifestera fortsatt särställning. Att nya kärnvapenmakter uppstår i Europa är inte tänkbart. På medellång sikt finns en risk att Ryssland på nytt kan satsa på taktiska kärnvapen för att kompensera för ett konventionellt underläge. Att NATO på nytt skulle satsa på kärnvapen i Europa är en risk tänkbar först på lång sikt.

Skulle Sverige i en framtid bli medlem av NATO kommer inga kärnvapen att stationeras i Sverige i fredstid ("norsk lösning"). Ett angeläget svenskt nästa nedrustningsinitiativ är ett juridiskt bindande avtal om begränsning, helst eliminering av taktiska kärnvapen.