Hot- och riskrapport 2005

KBM:S TEMASERIE | 2005:11

KRISBEREDSKAPS
MYNDIGHETEN

KBM:S TEMASERIE | 2005:11

Hot- och riskrapport 2005

Titel: Hot- och riskrapport 2005
Utgiven av Krisberedskapsmyndigheten (KBM)
Omslagsfoto: Corbis/Darren Modricker
Upplaga: 3 000 ex

ISSN: 1652-2915
ISBN: 91-85053-89-9
KBM:s dnr: 0825/2005
Grafisk form: AB Typoform
Tryck: Edita, Västerås 2005

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

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

KBM:s temaserie 2005:11

Innehåll

Förord

Detta är Krisberedskapsmyndighetens (KBM) andra årliga Hot- och riskrapport. Under det senaste året har händelser både i omvärlden och inom vårt land – som flodvågskatastrofen i Asien och stormen Gudrun – med oönskad tydlighet visat på de förödande konsekvenser som kan uppstå då hot och risker möter de olika sårbarheter som finns i samhället. Dessa erfarenheter visar att krisberedskapen i Sverige står inför stora utmaningar. Mot bakgrund av denna föränderliga och ofta svårtolkade hot- och riskmiljö vill KBM genom denna rapport ge läsaren en övergripande bild av de hot och risker som vårt samhälle kan komma att stå inför.

Ett viktigt led i arbetet för en väl fungerande krisberedskap är att upprätthålla en flexibel inställning till hela spektrumet av potentiella hot och risker. Att kunna hantera det oväntade, fyllt av komplexa osäkerheter, är en förutsättning för framgångsrik krishantering. Detta ställer krav på en förmåga till framåtblickande och öppenhet i bedömningen av hot och risker. Det är därför nödvändigt att inom krishanteringssystemet bedriva omvärldsanalys och kunskapsuppbyggnad utifrån ett helhetsperspektiv.

Vi vänder oss i första hand till alla er som på lokal, regional och central nivå arbetar med uppgifter inom krishanteringssystemet. Målsättningen är att Hot- och riskrapporten ska utgöra ett värdefullt underlag för arbetet med olika strategiska processer, exempelvis risk- och sårbarhetsanalyser, och planeringsprocessen. Vår ambition är också att Hot- och riskrapporten ska vara ett bidrag till det arbete som bedrivs utanför den offentliga samhällssektorn, i näringsliv och frivilligorganisationer.

Staffan Karlsson
Enhetschef
Informationssäkerhets- och analysenheten
Krisberedskapsmyndigheten

Sammanfattande reflektioner och slutsatser

Flexibla hot- och riskbedömningar

I all form av krisberedskapsarbete finns dimensionerna hot och risk. Vilka hot- och riskperspektiv vi utgår ifrån påverkar naturligtvis hur krisberedskapsarbetet bedrivs och prioriteras. Det går inte att bygga ett krishanteringssystem enbart på hot och risker som man i förväg kan identifiera.

I stället måste krishanteringssystemet byggas upp utifrån en generell förmåga att hantera kriser. Det som därför är av central betydelse är att de hot- och riskbedömningar som görs utgår från ett helhetsperspektiv där såväl manifesta som latenta hot och risker bearbetas och analyseras.

Vad som anses som omöjligt eller osannolikt ena dagen kan mycket väl vara bister verklighet dagen därpå. Exempelvis ansågs det fram till den 11 september 2001 som tämligen osannolikt att någon eller några koordinerat skulle kapa ett antal passagerarflygplan och flyga dessa in i stora byggnader. Inte heller ansågs det före 1997 möjligt för fågelinfluensaviruset att spridas direkt mellan fågel och människa.[1] Båda dessa exempel visar tydligt hur olika ”sanningar” mycket fort och med tragiska konsekvenser kan komma på skam.

Svensk krisberedskap har inte råd att i sina hot- och riskbedömningar utgå från alltför snäva perspektiv. När ”förvarningen” eller ”larmet” kommer är det oftast för sent att dimensionera och prioritera om de resurser som bör stå till krishanteringssystemets förfogande. Svensk krisberedskap måste således bygga utifrån en helhetssyn gällande de hot och risker samhället kan tänkas stå inför. Utan denna helhetssyn riskerar beredskapen att byggas utifrån felaktiga antaganden om vilka utmaningar krishanteringssystemets aktörer står inför.

1 Avian influenza: assessing the pandemic threat (WHO)

Svensk krisberedskap – en del av världen

Svensk krisberedskap är en del av den internationella säkerhetsmiljön genom EU-medlemskapet, genom en aktiv utrikes- och säkerhetspolitik, genom den internationaliserade ekonomin o.s.v. Vi måste ta med det internationella perspektivet i vårt arbete med krisberedskapen. Annars riskerar vi att exponeras för hot och risker som faller utanför den ”nationella” förståelseramen. Detta samtidigt som möjligheterna till internationell samverkan påverkas för krishanteringssystemets aktörer, om det saknas praktiska möjligheter till samarbete med andra länders krisberedskapssystem.

Det går inte längre att skilja på den inre och den yttre säkerheten. Smitta, orkaner, långvarigt regn, tekniska fel, organiserad brottslighet och internationell terrorism stoppas inte av nationsgränser. De är till sin natur gränsöverskridande. För att kunna hindra eller hantera dem krävs samarbete inom EU och internationellt. Alla länder, även Sverige, måste kunna ta emot och effektivt hantera hjälp. Det är viktigt att Sverige inte är onödigt sårbart eller saknar förmåga att mobilisera resurser för att hantera konsekvenserna av svåra skadehändelser.

Krishanteringssystemets aktörer måste ta med de internationella dimensionerna i det svenska krisberedskapsarbetet.

Förberedande krisberedskapsarbete

Naturen, tekniska system, terrorister och andra kriminella visar på svagheterna i samhällets motståndskraft och skydd. En del av skyddet mot aktörsrelaterade hot är trovärdighet i motståndskraft, medvetenhet, skydd och konsekvenshantering. Om Sverige framstår som ett land svårt att verka i för organiserad brottslighet och internationell terrorism, där viktiga mål är rimligt väl skyddade, bidrar detta till att minska hotet. Det förebyggande och förberedande krisberedskapsarbetet är avgörande för hur krishanteringssystemets aktörer kan förhindra att kriser uppstår eller hantera nästa kris. Vilken krisen blir vet vi inget om idag, men att den kommer är tämligen säkert.

Inledning

Det är KBM:s uppgift att bidra till att minska samhällets sårbarhet samt utveckla och stärka samhällets krishanteringsförmåga. KBM ska inom sitt område bedriva omvärldsbevakning och genomföra omvärldsanalyser. KBM:s årliga hot- riskrapport är en del av detta arbete.

De hot och risker som beskrivs i denna rapport är såväl sektorsövergripande som gränsöverskridande, vilket ställer krav på en gemensam förståelse hos alla oss som på olika sätt arbetar med samhällets krisberedskap.

Denna årligt återkommande sammanställning har som främsta syfte att förmedla en samlad beskrivning och analys av de hot och risker som krishanteringssystemets aktörer bör ta hänsyn till i arbetet med krisberedskapsåtgärder. Denna rapport bygger till viss del på resultaten från föregående års rapport. Dock är det viktigt att betona att ett av skälen till att producera en årligt återkommande Hot- och riskrapport är att hoten och riskerna är föränderliga. Detta innebär också att de hot och risker som presenterades i 2004 års rapport fortfarande är aktuella och angelägna. Denna rapport ska till viss del ses som komplement till, och utveckling av, föregående års rapport.

Det som presenteras i denna rapport är ett resultat av KBM:s eget arbete. Dock har flera myndigheter och organisationer, med olika roller inom krishanteringssystemet, bidragit med nödvändiga underlag.

De aktörer som KBM vill nå med denna rapport bedöms ha god kännedom om de hot och risker som finns inom den egna sektorn eller det egna geografiska området. Dock finns det ett behov av en överskådlig bild av hot- och riskmiljön för systemet i stort. Denna rapport är alltså riktad till alla som har till uppgift att genomföra krisberedskapsåtgärder på nationell, regional eller lokal nivå, och den ska kunna fungera som stöd i detta arbete. Rapporten kan bl.a. fungera som en av utgångspunkterna för myndigheternas arbete med de årliga risk- och sårbarhetsanalyserna.

Det är viktigt att poängtera att de hot och risker som behandlas i rapporten inte ska ses som de viktigaste

i alla tänkbara sammanhang. Ambitionen är inte heller att utmåla något hot eller någon risk som viktigare än något annat. Det är alltså upp till var och en av aktörerna att avgöra vilka delar som är tillämpbara på den egna verksamheten och utifrån detta prioritera sitt krisberedskapsarbete.

KBM har ett särskilt uppdrag när det gäller informationssäkerhetsarbetet i samhället. I rapporten behandlas informationssäkerhetsfrågorna därför mer utförligt i ett separat kapitel.

Innehållet i denna rapport bör inte enbart betraktas som utgångspunkter för den verksamhet inom krishanteringssystemet som finansieras via anslaget 7:5 Krisberedskap. Också andra typer av åtgärder, vilka respektive aktör har ett eget ansvar för att genomföra, kan utgå från denna hot- och riskrapport.

Hot- och riskanalysens betydelse för krishanteringsförmågan

KBM har uppdraget att främja forskning av god vetenskaplig kvalitet inom områden som är relevanta för svensk krisberedskap. Inom området hot och risker har KBM bl.a. finansierat docent Wilhelm Agrell vid Lunds universitet som har analyserat förvarningsproblematiken och publicerat en lärobok i ämnet. Andra exempel är docent Johan Eriksson vid Södertörns högskola som har forskat kring hur olika tongivande hotbilder skapas och förmedlas. Lektorerna Charles Parker och Eric Stern vid Uppsala universitet har undersökt de många filter som försvårade för signaler om en kommande terrorattack att rätt förstås av relevanta beslutsfattarna i USA i samband med terrorattackerna den 11 september 2001.

Detta avsnitt om hur hot- och riskanalyser kommer till användning, eller inte utnyttjas av dem som behöver dessa, bygger bland annat på resultaten från den forskning som KBM har finansierat. Denna forskningsverksamhet ska vara tillämpbar för det praktiska arbetet inom det svenska krishanteringssystemet.

Att ta fram hot- och riskbedömningar är en komplex och krävande uppgift. En organisation, offentlig eller privat, lägger inte resurser på detta arbete för dess egen skull. Hur kan omvärldsanalyser komma till praktisk användning för att bidra till en förstärkt krishanteringsförmåga?

Hot- och riskbedömningar kan inte göras fristående från krishanteringssystemets övriga verksamhet. Detta diagnosarbete bör användas som ett initialt led i en beredningskedja som leder till beslut och agerande inför svåra situationer som man helst vill undvika genom förebyggande och förberedande arbete. Kunskapsuppbyggnad och kompetensutveckling utgör viktiga framgångsfaktorer för gedigna hot- och riskbedömningar och för deras omsättning till verksamhetsförankrade praktiska åtgärder.

Analytisk flexibilitet

Det mest grundläggande för en god beredskap inför möjliga krissituationer är att upprätthålla förmågan till en flexibel hot- och riskanalys. Genomlysningar av en rad historiska erfarenheter visar att brister i hanteringsförmågan inte primärt har orsakats av att det saknats hotanalys. Det har snarare handlat om att man har fäst alltför stort avseende vid en viss given bild. En rigid fixering vid ett eller några få sannolika hot eller riskmoment inbjuder till obehagliga överraskningar.

Många i ledande ställning bär fortfarande på föreställningar från det kalla krigets hotbild. De senaste åren har vi därtill fångats av det konkreta – och genom TV med egna ögon upplevda – hotet från väpnade terrorister. Andra möjligheter har suddats ut i vår mentala beredskap och i den officiella hot- och riskanalysen. I denna skrift försöker KBM peka på hela det spektrum av hot och risker som måste beaktas i planeringsarbetet. Samhällets säkerhet kan utsättas för påfrestningar av olika typer och från olika håll.

Med ett sådant breddat säkerhetsspektrum måste både sannolikheter och konsekvenser inbegripas i en sammanhållen riskanalys av olika möjliga hot. Vissa angrepp torde få förödande nationella konsekvenser, medan t.ex. en informationsoperation av en terrorgrupp eller ett kriminellt syndikat vore mindre skadeverkande för samhällets säkerhet. Å andra sidan kan dessa typer av angrepp vara mer sannolika, inträffa oftare och därmed ge en kumulativ effekt av stor betydelse för vår nationella säkerhet. Inom vissa områden, som pandemier, måste en mycket god beredskap upprätthållas för att kunna möta ett värstafallsscenario. Vi har begränsad kännedom om spridningseffekterna av olika smittor eller om illasinnade aktörers motiv och förmågor. Frågan infinner sig då hur sannolika dessa dramatiska scenarion är. På vilka områden bör kraftsamlingen ske, och på vilka områden kan man leva med en kalkylerad risk?

I en mening blev händelserna den 11 september 2001 inriktande för fördelning av de knappa resurserna. Det gick åter att planera för ett väpnat hot med relativt hög sannolikhet. Andra hottyper som före denna dramatiska händelse varit tongivande i den svenska diskussionen föll undan. En ny fixpunkt för den säkerhetspolitiska analysen kunde etableras. Konturerna förstärktes av attentaten i Madrid 2004 och London 2005. Denna analytiska insnävning kan innebära ett risktagande för säkerheten inom vårt samhälle då en kris ofta uppstår ur det till synes oväntade, som en blixt från klar himmel. Mordet på Anna Lindh och tsunamikatastrofen visade detta med all oönskad tydlighet. Dessa händelser tydliggjorde alltså behovet av en bred och flexibel hotförståelse

En flexibel hot- och riskanalys för ett nationellt krishanteringssystem behöver även breddas bortom aktörsrelaterade hot där ett ont uppsåt föreligger. Strukturellt betingade risker

behöver sannolikhetsbedömas och deras skadeverkningar beaktas. T.ex. torde ett kollapsat infrastruktursystem i ett närliggande samhälle få stora konsekvenser för vårt land. Denna typ av hot mot vår överlevnad har föranlett betydande investeringar i förberedande insatser inför värstafallsscenarion inom detta fält. Exempelvis fanns det inte i Sverige vid tidpunkten för Tjernobylolyckan någon beredskap för att möta kärnkraftsolyckor i utlandet, medan man hade en god insikt om riskerna kring de egna kärnkraftverken.

Larmkedjans svaga punkter

Forskning pekar mot att steget ofta är långt från en gedigen hot- och riskanalys till beslut och åtgärder som bygger på denna omvärldsdiagnos. Flera länkar i en komplex beredningsprocess måste säkras för att uppnå en förmåga och en vilja att agera som utgår från en i förväg utarbetad hot- och riskanalys. Ett nödvändigt första steg är den diagnosfas, ofta innefattande en fyllig bild av hot- och riskmiljön, som presenteras i denna skrift. Men frågan kvarstår om och hur denna typ av omvärldsanalys tas om hand och används som utgångspunkt för beslut och agerande. KBM främjar forskning kring dessa frågor som ett led i uppbyggnaden av ny kunskap och kompetens av betydelse för samhällets säkerhet.

I flera väldokumenterade fall av s.k. underrättelsemisslyckanden, som Pearl Harbour 1941, Korea 1950, Yom Kippur 1973, New York och Washington den 11 september 2001 och kanske orkanen Katrina i september 2005, saknades varken relevant hotanalys eller tidiga signaler om en förestående katastrof. Krishanteringssystemet måste alltså kunna orka upprätthålla en flexibilitet inför mångtydigheter, besitta en förmåga att smälta förvånande och udda signaler samt ha kraft att förmedla även ovälkomna budskap vidare upp i beredningskedjan.

Studier av dessa händelser visar att den svaga länken fanns i överföringen av tidiga, svårtolkade, ibland motstridiga indikatorer så att dessa kan fungera som ett underlag för förebyggande, förberedande eller operativa insatser. Det är långt ifrån säkert att en gedigen omvärldsanalys kommer till praktisk användning när den behövs. Om så ska ske, måste detta säkerställas i förväg, innan läget blir akut.

En varning ska inte bara tas emot av en organisation. Den ska även förstås och smältas mentalt av individer och av ett beslutskollektiv. Först då man nått denna länk i kedjan kan en signal omvandlas till en varning som ger anledning till beslut och agerande.

Forskning kring dessa fenomen belyser hur en rad processer fungerar som svårgenomträngliga och förvanskande filter i överföringen av kritisk information till dem som ansvarar för beslut och genomförande. Larmkedjan fungerar inte alltid enligt planen visar flera djupstudier av historiska underrättelsemisslyckanden.

Egenskaper i organisationer skapar en rad väldokumenterade begränsningar för hur omvärldsanalyser tas till vara i beredningsarbetet inför viktiga beslut i trängda lägen. Organisatoriska anomalier fungerar som ett filter för informationsspridning och utformning av underlag för och genomförande av beslut. Uppsättningen relevanta handlingsalternativ styrs ofta mer av de medel organisationen har tillgång till än av situationens egenart.

Ofta bereds och bestäms agerandet i en snäv krets av förtrogna. Organisatoriska rivaliteter, professionella kulturer, regelsystem och rutiner kommer till uttryck i dessa slutna rum. Trycket på att komma överens snabbt, att nå konsensus, undertrycker det lika viktiga behovet av en grundlig och kritisk genomlysning av ett komplext informationsmaterial. Den mest kända patologin inom detta forskningsområde är s.k. groupthink, ett forskningsområde där KBM finansierat studier.

Våra medborgare ska kunna förvänta sig att en omvärldsanalys på saklig grund bidrar till att goda beslut fattas inför olika hot- och risksituationer. Att ta reda på hur man kan uppnå kvalitetsmedvetenhet i beredningsarbetet inför svåra avgöranden kring hot och risker är en viktig uppgift för forskningen med konkret betydelse för den nationella förmågan att hantera kriser.

Nästa steg i beredningskedjan omfattar det avgörande steget från larm till beslut. Det kan finnas många goda skäl för en politiskt ansvarig beslutsfattare att inte ta detta svåra steg. Att agera innebär kostnader och risker av olika slag. Men även ett passivt förhållningssätt kan i efterhand få katastrofala konsekvenser för samhället och för beslutsfattaren personligen. Dagen efter den stora krisen handlar debatten mindre om ansvarsundvikande och mer om ansvarsutkrävande.

I denna fas bedöms inte bara den på omvärldsanalysmaterial baserade analysen av de förhållanden som ska hanteras, utan här tillkommer vanligen också en dimension av vad som är politiskt möjligt. En beslutsfattare vars tillvaro är präglad av osäkerheter och komplexitet kan finna att det minst smärtsamma för stunden är att avvakta. Man kan hoppas att signalen var feltolkad eller att varningen var ännu ett falsklarm, och att beslutskraften och de tillgängliga resurserna bättre ägnas åt mer omedelbara och konkreta problem. Ofta följs en omfattande omvärldsanalys av hot och risker av ett sådant icke-beslut. Det är väsentligt att alla som arbetar med analyser om hot och risker inser att det kan finnas sådana skäl för en till synes passiv handlingslinje.

När motsatsen inträffar och ett aktivt beslut fattas måste detta kommuniceras till berörda aktörer och i förekommande fall till allmänheten. Även här finns en rad svårigheter att hantera. I dagens mediebaserade samhälle räcker det inte med ett resolut agerande inför en hotande situation. Bilden av agerandet måste spegla denna vilja att genomföra motåtgärder för att möta eller hindra kommande hot. Studier om kriskommunikationens

svåra handlag har fått stöd av KBM då denna dimension utgör en väsentlig del av den nationella förmågan till effektiv och legitim krishantering.

Gemensam lägesbild – samlad förmåga

Samverkan tvärs över sektorsgränser eller nationsgränser krävs ofta för att uppnå avsedda resultat inför de hot och risker som lyfts fram i denna rapport. Det finns omfattande forskning om implementeringsproblematiken och om samordningens begränsningar inom nationella strukturer. Nu behövs även djupare kunskaper om det internationella samarbetets problematik. Förutsättningar och begränsningar för samverkan inom ett EU med 25 medlemmar måste belysas genom forskning och studier.

Inom EU växer över tiden fram ett gemensamt synsätt vad det gäller den inre säkerheten i unionen. Detta skapar förutsättningar att bygga vidare på. Även en rad konkreta problem uppstår när en handlingslinje under utveckling ska omsättas till etablerad praktik. Under överskådlig tid kommer sannolikt EU:s gemensamma förmåga att vara otillräcklig i förhållande till gemensamma hot, risker och sårbarheter. Kedjan från hot- och riskbedömningar, över gemensamma beslut och till ett samlat agerande i kritiska lägen kan därför ytterligare komma att försvagas.

I förslaget till EU:s sjunde ramforskningsprogram ska ett av nio prioriterade områden behandla säkerhetsfrågor. Säkerhetsforskningen är avskild från militära kunskapsbehov och är således enbart riktad mot civila frågor. Prioriterade områden inom EU:s säkerhetsforskning är skydd mot terrorism, CIP, gränssäkerhet och upprätthållande av säkerhet vid en krissituation.

I denna rapport utgår KBM från ett svenskt perspektiv. Självklart har vi även ett ansvar för att bidra till den gemensamma krishanteringsförmågan i det EU som vi är en del av. Med ett sådant utökat ansvar måste säkerhetsspektrumet ytterligare vidgas och kedjan från en flexibel hotbildsbedömning till ett resolut agerande smidas ännu fastare.

Hotperspektiv

USA:s Department of Homeland Security (DHS) använder i sin *Interim National Infrastructure Protection Plan* ett ramverk för hot- och riskhantering där en distinktion görs mellan olika typer av hot. DHS bedömning av hot sker snarare utifrån möjliga konsekvenser än utifrån sannolikheten för att de ska realiseras. Med utgångspunkt från detta ramverk har KBM definierat två kategorier av hot: de manifesta och de latenta. KBM anser att användandet av en sådan tolkning av hotbegreppet är fruktbart och kanske till och med nödvändigt, för att nå en generell förståelse för vilka hot som svensk krisberedskap står inför.

Ett manifest hot är något som har klart framträdande tecken på någon

form av bakomliggande företeelse. Det kan vara ett hot eller situationer där det finns underrättelser som pekar på att vissa funktioner i samhället eller vissa mål är hotade, eller på att vissa grupperingar av individer uppvisar olika former av aktivitet. Sannolikhetsbedömningar är centrala för dessa typer av hot, vilka i sin tur dimensionerar mer operativa skyddsåtgärder. Hanteringen av manifesta hot är ofta händelsestyrd eller utgår från mer eller mindre tydliga eller påtagliga indikationer, exempelvis underrättelseinhämtning, larm, anmälan, plötslig upptäckt eller liknande.

Ett latent hot är ett fenomen som inte på samma påtagliga sätt går att observera, men vars existens vi på andra grunder kan sluta oss till. Om ett latent hot realiseras riskerar det att skapa konsekvenser som kan bedömas vara minst lika allvarliga för våra samhällsfunktioner som ett manifest hot. Analysarbetet avseende hot och risker bör följaktligen också kunna utgå från en bedömning av potentiella konsekvenser. Därför måste krishanteringssystemets aktörer utveckla och etablera en generell förmåga att hantera de hot som inte föregåtts av exempelvis underrättelseuppgifter, larm, anmälan eller plötslig upptäckt.

Ett exempel på detta arbetssätt är hur brittiska myndigheter arbetat med dessa två olika hotperspektiv med anledning av terrorattackerna den 7 juli i år. Den brittiska säkerhetstjänsten BSS (MI5) sänkte två veckor före attentatet hotnivån från ”severe general” till ”substantial”. Med andra ord fanns det mindre manifesta hotindikationer och denna sänkning var ett resultat av de hotanalyser som görs inom terrorområdet. Dock fanns det bland de brittiska krisberedskapsaktörerna en utvecklad föreställning om terrorhotet utifrån ett latent hotperspektiv vilket påverkade det förberedande krisberedskapsarbetet hos dessa aktörer. Dimensioneringen av krishanteringsförmågan vilade således på en hotuppfattning som inte byggde på någon förvarning eller larm, utan baserades på en mer generell förståelse av komplexiteten i hot- och riskanalysarbetet.

Det är sådana erfarenheter som gör det viktigt att utveckla våra gemensamma föreställningar om, och bygga upp samhällets förmåga att hantera, också det oväntade. Om samhällets åtgärder för att hantera hot och risker på ett ändamålsenligt sätt ska kunna bygga upp rätt kompetens och förmåga, måste såväl manifesta som latenta hot utgöra en av utgångspunkterna för prioritering och fördelning av resurser i krishanteringssystemet inom ramen för den rådande inriktningen.

Generella utvecklingstendenser

Detta avsnitt syftar till att ge en bild av de trender i den internationella miljön som är av betydelse för svensk säkerhet och krisberedskap. De hot och risker som redovisas i rapporten kan inte ses lösryckta ur sitt sammanhang, utan måste ställas i relation till det samhälle som vi verkar i. Det är således viktigt för krishanteringssystemets aktörer att i sitt arbete ha kunskap om generella globala utvecklingstendenser.

Den tid som vi lever i har getts många namn – t.ex. informationstidsåldern, den postmoderna epoken, den globala byn m.m. Konturerna på utvecklingen av denna ”nya” är ännu för många av oss suddiga och odefinierade. Konsekvenserna utifrån ett hot- och riskperspektiv för samhällslivet framträder emellertid allt tydligare. Dessa konsekvenser visar sig inte enbart i storpolitiska sammanhang utan även till vardags: politiskt, ekonomiskt, kulturellt, socialt och ekologiskt.

Ur ett säkerhetsperspektiv har denna utveckling, där världen bildigt talat hela tiden förändras, åtminstone fyra konsekvenser som redan nu berör Sverige, EU och världen på olika sätt. För det första är våra samhällen och i synnerhet deras infrastrukturer på väg att bli allt mer sårbara. För det andra är gårdagens elitstater – och då i synnerhet de västeuropeiska välfärdsstaterna – på väg att försvagas i förhållande till den omgivande världen. För det tredje får denna utveckling konsekvenser för den globala resursanvändningen med påföljande ekologiska effekter. För det fjärde har den globala politiska miljön förändrats med framväxten av nya spänningsfält och hot. Inom alla dessa fyra områden existerar och utvecklas olika hot mot samhällets säkerhet och beredskap.

Vår säkerhetsmiljö har därmed breddats. Dessa fyra säkerhetsdimensioner är ganska olika varandra, men påverkar samtidigt varandra i större eller mindre grad. Exempelvis skulle en pandemi inte endast utgöra ett direkt hot i form av ett stort antal döda och insjuknade. Den skulle också sannolikt allvarligt påverka den globala ekonomin genom att begränsa eller stoppa flödet av varor och människor. Följderna av sådana sekundära effekter riskerar att bli väl så allvarliga som själva hälsokonsekvenserna.

För femtio år sedan levde nästan halva Sveriges befolkning på landet. Flertalet hade egen brunn, eget dass, egen kökträdgård, egen soptipp och tillgång till ved för att värma sig och tillaga sin mat med. Sverige hade då även en i stort sett nationell ekonomi och ett jordbruk som kunde förse befolkningen med mycket av det som behövdes i matväg. Alla vitala förutsättningar för att överleva – dricksvatten, sanitet, mat, sophantering och värme – var decentraliserade och så enkla och robusta att de i praktiken inte kunde slås ut.

I dag är majoriteten av befolkningen urbaniserad och beroende av en centraliserad teknisk infrastruktur som förser oss med vårt dricksvatten, för bort våra sopor, värmer våra hem och distribuerar vår mat. Den svenska ekonomin är dessutom i hög grad en integrerad del av världsmarknaden.

Som en följd av detta har samhället blivit mycket mer sårbart. Effekterna för samhället av störningar i våra infrastrukturer eller i den globala ekonomin är i dag annorlunda och mer omfattande än tidigare.

En ytterligare säkerhetsdimension är den ekologiska. Den innefattar bl.a. mänsklighetens växande och accelererande inverkan på det globala ekosystemet. Problemen kan delas i två kategorier. För det första utarmar vi vitala resurser, som olja, fisk, brukbar jord och dricksvatten. För det andra påverkar vi det globala ekosystemet med klimatförändringar, ozonhål, alltmer extrema väderleksförhållanden m.m. som följd.

Den politiska säkerhetsdimensionen finns kvar, men är tämligen förändrad. Skillnaden idag från den värld, där nationalstaternas inbördes relationer och konflikter var i fokus, är att de fattigaste delarna av världen numera lever i nära kontakt med de absolut rikaste länderna.

Det stora politiska hotet är inte längre spänningar mellan världens i-länder. Deras djupa ekonomiska integration gör militära konflikter mellan dem mindre sannolika. Konfliktmönstren har förändrats. Ett exempel är den internationella terrorismen med masskadesyfte. En annan destabiliserande omständighet är exempelvis att ungefär 65 procent av världens befolkning lever i de minst utvecklade områdena.

Världen har i flera bemärkelser krympt och världens rika är inte längre avskärmade från de fattiga. Den ”globala byn” har börjat uppstå, men uppvisar stora socioekonomiska skillnader vilket skapar spänningar mellan dess invånare. Ingen enskild aktör eller nation har resurser att ensam lösa de globala problemen. Detta arbete måste ske genom internationell samverkan. Åtgärder inom ett nationellt krishanteringssystem måste därför genomföras med utgångspunkt också i dessa omständigheter, oberoende av om åtgärderna har ett nationellt eller internationellt fokus.

EU och Sverige – en förändrad hotbild?

Här följer nu ett avsnitt som beskriver en tillämpning av den generella utvecklingen inom säkerhetsområdet. Detta avsnitt avspeglar hur den svenska hot- och riskmiljön kan bedömas och värderas utifrån ett EU-perspektiv. Det finns en rad, för svensk krisberedskap, positiva effekter med Sveriges medlemskap i EU. Fokus i detta avsnitt är dock på delar som kan vara angelägna att hantera utifrån ett hot- och riskperspektiv.

Skapandet av EU:s inre marknad, även för tjänster som el och telefoni bidrar till fler sammankopplingar av infrastrukturer och system över nationsgränserna. Ofta är denna sammankoppling ett explicit mål för den verksamhet som bedrivs inom EU. Inom ramen för programmet ”Trans-European Networks” betalas stora belopp ut för att koppla samman den europeiska infrastrukturen på transport-, el- och IT-områdena. Ett avbrott i ett land geografiskt långt ifrån Sverige kan sålunda ge efterverkningar som påverkar det svenska samhället och dess funktionalitet.

Detta är en generell utveckling i världen som inte i grunden orsakas av EU, men denna utveckling kan sägas accelereras av EU. Det faktum att vi är medlemmar i EU skulle även kunna leda till en ökad risk för terrorism om Sverige kopplas samman med den gemensamma utrikes- och säkerhetspolitiken, exempelvis om Sverige deltar i en EU-gemensam fredsframtvingande insats. Det är emellertid svårt att dra gränsen mellan vad som kan vara en risk på grund av EU-medlemskapet specifikt och vad som är en risk rent allmänt i och med den ökade globaliseringen. Vidare kan detta påverka hotbilden för olika utländska intressen i Sverige, liksom större internationella konferenser och engagemang.

Det policydokument som tydligaste anger en uppfattning av de hot som unionen står inför är den så kallade säkerhetsstrategin ”Ett säkert Europa i en säker värld” som beslutades av EU:s stats- och regeringschefer i december 2004. I rapporten lyfts fem hot mot Europas säkerhet fram som särskilt allvarliga: terrorism, där Europa beskrivs både som mål och bas för terrorismen; spridning av massförstörelsevapen, särskilt i kombination med terrorism; regionala

konflikter, exempelvis Kashmir och Mellanöstern; stater i upplösning som Somalia eller Afghanistan; organiserad brottslighet, särskilt i kombination med stater i upplösning och terrorism. Rapporten har en säkerhetspolitisk prägel och de föreslagna åtgärderna handlar om hur unionen ska agera i världen. Strategins effekter vad gäller EU:s politik har också begränsat sig till den gemensamma utrikes- och säkerhetspolitiken.

En annan källa till hur EU ser på hot och risker är rapporterna från det Europeiska Rådets möten. EU:s stats- och regeringschefer träffas normalt tre gånger årligen i det Europeiska Rådet för att lägga upp de stora linjerna för EU:s politik. Under de möten som genomförts under 2004 och 2005 har terrorism varit i fokus och de flesta åtgärder som efterlysts har syftat till att hantera detta hot, exempelvis har ett initiativ för skydd av samhällsviktig infrastruktur tagits. Vid sidan av terrorism har det Europeiska Rådet också diskuterat den organiserade brottsligheten, illegal immigration, användande av droger och organiserad brottslighet som säkerhetsproblem för Europa. Även klimatförändringar har nämnts som ett allvarligt hot på längre sikt. För att hantera dessa hot har bl.a. en handlingsplan antagits, det så kallade Haagprogrammet, som listar en mängd åtgärder som behöver vidtas på det inre säkerhetsområdet.

Strategiska bedömningar av hot och risker för unionen genomförs på regelbunden basis av SITCEN (Situation Centre), vilket är EU:s organ för underrättelsesamarbete. Till en början ägnade sig SITCEN enbart åt externa hot men har på senare tid även börjat få en roll att ta fram underlag om olika hot och risker inom unionen.

Sammantaget kan det sägas att Sveriges medlemskap i EU gör att komplexiteten i den svenska hot-och riskmiljön ökar. Sålunda bör därför EU-dimensionen tas i beaktande i arbetet med krisberedskapsfrågor.

Icke-aktörsrelaterade hot och risker

Detta avsnitt tar upp två huvudsakliga kategorier av icke-aktörsrelaterade hot: extrema natur- och väderhändelser samt smitta. Ett särskilt fokus riktas också mot flodvågskatastrofen i Asien, stormen Gudrun, klimatförändringens effekter på samhällets krisberedskap och fågelinfluensan.

Extrema natur- och väderhändelser

Alla samhällen är sårbara för extrema natur- och väderhändelser. Kring årsskiftet 2004–2005 drabbades det svenska samhället av två extrema natur- och väderhändelser – flodvågskatastrofen i Asien och stormen Gudrun – vilka på skilda sätt medförde mycket allvarliga konsekvenser på liv, egendom och viktiga samhällsfunktioner. Händelserna belyste samtidigt två fenomen som präglar nutiden och har skapat en delvis ny hotbild för samhället: förändringar i resandet med nya mönster och ändrad omfattning som en del av en alltmer sammanflätad och globaliserad värld, samt det utbredda och tilltagande beroendet av olika former av infrastruktur vilka i sig ofta präglas av omfattande och komplexa inbördes beroenden.

Varje år inträffar ett flertal natur- och väderhändelser som orsakar störningar i samhället. I mer sällsynta fall inträffar vad som kan ses som extrema händelser då allvarliga störningar i samhället uppstår. I Sverige är de typer av extrema väderhändelser som normalt sett orsakar mest skada översvämningar och stormar. Historiskt sett har Sverige drabbats av svåra översvämningar med mellan fem och tjugo års intervall. Extrema stormar är något mer ovanliga. Den närmast föregående stormen av karaktär jämförbar med Gudrun inträffade 1969. Andra typer av händelser som i sina mer extrema former kan leda till betydande störningar i samhället är kraftiga regn- och snöfall, is- och saltstormar, skogsbränder, kyla samt ras och skred.

Dessa fenomen kan medföra betydande skador och störningar och kan, i synnerhet vid långvariga förlopp, lamslå väsentliga delar av samhällets verksamhet. Särskilt tydligt blir detta i effekterna på den samhällsviktiga

infrastrukturen: avbrott i elförsörjning samt tele- och IT-kommunikationer, störningar i dricksvattenförsörjning och avloppssystem, förstörda eller oframkomliga vägar och järnvägar. Vid extrema natur- och väderhändelser är denna typ av konsekvenser vanligt förekommande och kan såväl försvåra insatser under den akuta krishanteringsfasen som leda till allvarliga problem med att upprätthålla samhällets funktionalitet i drabbade områden.

Ett exempel på de omfattande konsekvenser för samhället som naturhändelser kan orsaka är orkan Katrina som drabbade USA:s sydkust i augusti i år. Idag saknas en komplett bild av hur långtgående konsekvenserna har blivit och hur väl krishanteringen fungerat. Klart är dock att denna händelse varit förödande för de drabbade områdena vad avser såväl liv, hälsa och egendom, som samhällets politiska, ekonomiska och sociala funktion i övrigt.

Ett särskilt allvarligt scenario i Sverige är extremt höga vattenflöden i de största sjöarna. Kraftiga och långvariga regn kan framkalla nederbördsmängder i tillräcklig omfattning för att göra exempelvis Vänern och Mälaren överfulla. Med nuvarande avtappningsmöjligheter kan sådana situationer bli svåra att hantera med omfattande översvämningar som följd. Denna typ av översvämningar skulle kunna leda till mycket allvarliga konsekvenser i Göta älvdalen samt i Mälardalen och Stockholmsregionen.

En annan typ av händelse som potentiellt kan medföra katastrofala följder är dammbrott vid någon av de större älvarna. I Sverige finns det 185 dammar som enligt Svenska Kraftnät är klassade som högkonsekvensdammar. I huvudsak innebär detta att om ett dammbrott skulle inträffa är sannolikheten för förlust av människoliv eller allvarlig personskada inte försumbar.[2] För närvarande görs bedömningen att dammsäkerheten håller en godtagbar nivå. Dock finns det anledning att arbeta med dessa frågor då konsekvenserna av ett eventuellt dammbrott är så omfattande och att förändringar i klimatet kan ändra förutsättningarna och därmed behovet av krisberedskapsåtgärder.

Omfattande granskningar av Europeiska miljöbyrån visar på en tydlig trend av ökande konsekvenser kopplade till extrema natur- och väderhändelser.[3] I Europa fördubblades antalet allvarliga extrema natur- och väderhändelser under åren 1990–2004 jämfört med föregående period. Under samma period mer än fördubblades den genomsnittliga årliga ekonomiska kostnaden för dessa händelser. Detta kan delvis kopplas till diskussionen om klimatförändring men visar framför

2 Svenska Kraftnät, rapporten ”Dammsäkerhetsutvecklingen i Sverige” 2005-09-23

3 http://www.eea.eu.int Se tex. ”Mapping the impacts of recent natural disasters and technological accidents in Europe”, Environmental issue report no. 35, samt “Impacts of Europe’s changing climate Floods”, EEA report no. 2/2004.

allt på ökande sårbarhet för extrema natur- och väderhändelser. En anledning till den tilltagande samhälleliga sårbarheten är att teknisk infrastruktur spelar en alltmer avgörande roll för att vi ska kunna upprätthålla samhällsviktiga funktioner och tjänster. Få verksamheter i samhället fungerar utan tillgång till el, telekommunikationer och IT. Samtidigt är de samhällsviktiga infrastrukturerna känsliga för tekniska störningar och naturhändelser, vilket ytterligare förstärks av komplexa inbördes beroendeförhållanden. Genom en utveckling mot att system successivt byggs samman till system av system, blir de i vissa fall oöverskådliga, komplexa och tekniskt heterogena. En mindre störning kan fortplanta sig och ge upphov till långvariga störningar som sprids till stora delar av exempelvis transport- och elförsörjningssystemen.

En ökande roll för privata företag inom samhällsviktig infrastruktur sedan ett drygt decennium tillbaka har förändrat förutsättningarna för risk- och krishanteringsförmågan. Beroende på höga effektivitetskrav och tilltagande konkurrens inom flera viktiga infrastrukturområden har nödvändiga reserver och resurser för att hantera omfattande störningar i vissa fall varit otillräckliga. Avregleringen har också lett till att det i många fall saknas en systematiskt uppbyggd helhetsbild av den tekniska infrastrukturen. Sammansättningen av infrastruktursystem är svår att överblicka också på grund av exempelvis komplexa ägarförhållanden och flera led av underleverantörer, med både nationella och internationella aktörer involverade.

Både förekomsten och de potentiella konsekvenserna av extrema natur- och väderhändelser är frågor av betydande vikt för krishanteringssystemet. Extremväder kan – som med all tydlighet visats av flodvågskatastrofen, stormen Gudrun och de olika översvämningarna under senare år – orsaka omfattande skador på liv och egendom samt allvarligt störa eller slå ut viktiga samhällsfunktioner. Risken för extrema vädersituationer ställer krav på förberedande åtgärder och krishanteringsförmåga i samhället.

Extrema natur- och väderhändelser är återkommande fenomen för samhället att hantera. En väl utvecklad förmåga att hantera denna typ av händelser och de störningar som kan uppstå är nödvändig hos de aktörer och de delar av samhället som riskerar att omfattas.

Erfarenheter från tidigare extrema natur- och väderhändelser pekar samfällt mot behovet av förbättrad samordning av krishanteringen. Detta beror dels på nödvändigheten i att koordinera insatser och åtgärder hos ett stort antal inblandade aktörer, dels på behovet av samarbete kring och effektiv fördelning av tillgängliga resurser. Vid exempelvis omfattande översvämningar och extrema stormar uppstår ofta under vissa faser av krishanteringen stora behov av förstärkningsresurser, i form av såväl personella resurser som utrustning.

Klimat i förändring – konsekvenser för samhällets krisberedskap

Mycket tyder på att världen genomgår en global uppvärmning. Det är omöjligt att förutspå exakt i vilken omfattning och hastighet klimatförändringen kommer att utvecklas. Tendensen till ett allt varmare klimat är dock tydlig, likaså att denna utveckling medför risker för avsevärda effekter på natur och samhällsliv. Av särskilt stor betydelse för samhällets krisberedskap är att klimatförändringen kan komma att påverka förekomsten av och styrkan hos extremväder. Sverige riskerar sannolikt att i framtiden drabbas av översvämningar och stormar i högre utsträckning och av värre intensitet än tidigare.

FN:s vetenskapliga klimatpanels (Intergovernmental Panel on Climate Change, IPCC) sammantagna bedömningar av internationell klimatforskning tyder på att temperaturen på jorden är stigande och att denna effekt kommer att tillta under det kommande seklet. Under 1900-talet ökade jordens medeltemperatur med omkring 0,6 °C. Enligt IPCC kan jordens medeltemperatur under det kommande århundradet komma att öka med ytterligare mellan 1,4 och 5,8 °C. Naturvårdsverket och SMHI, som är de huvudsakliga expertmyndigheterna i Sverige, delar denna bedömning. Den främsta anledningen till den stigande globala medeltemperaturen anses vara ökad mängd växthusgaser i atmosfären, vilket i huvudsak beror på användningen av fossila bränslen (kol, olja, naturgas). Detta förstärker den så kallade växthuseffekten och leder till uppvärmning.[4]

Den globala uppvärmningen kan få omfattande följdeffekter för nederbörd, vindar, havsytenivå, klimatzoner och havsströmmar. Genom att klimatförändringen kan påverka ett så brett spektrum av fenomen är konsekvenserna samtidigt svåröverskådliga och potentiellt mycket svåra. Till synes små förändringar i årsmedeltemperaturen kan ge mycket stora återverkningar på övriga delar av klimatet. Redan en förändring på 1 °C anses kunna medföra betydande påverkan.

I ett mycket långt historiskt perspektiv har avsevärda förändringar av jordens klimat förekommit vid ett antal tillfällen. Det som gör dagens klimatförändringar speciella är hastigheten. Enligt Naturvårdsverket går dagens förändringar 10 till 100 gånger fortare än tidigare naturliga förändringar. Exakt hur mycket temperaturen kommer att stiga och hur omfattande följdeffekterna blir går dock inte att fastställa. De scenarion som gjorts av forskare innehåller betydande osäkerheter och den faktiska framtida klimatförändringen kan komma att bli både mindre och större än vad dagens prognoser visar.

Klimatförändringen kan komma att medföra omfattande påverkan på kli-

4 För en mer ingående förklaring se Naturvårdverkets webbplats http://www.naturvardsverket.se/dokument/klimat/index.html

mat och samhälle i Sverige. Forskningssimuleringar gjorda av SMHI[5] visar att kommande temperaturökningar i Sverige antagligen blir högre än den genomsnittliga globala ökningen. Förutom ett allmänt varmare klimat med förändrade årstidscykler och klimatzoner förväntas detta medföra att nederbörden ökar, speciellt i norra och västra Sverige. Ökad nederbörd, intensivare regn och stigande havsytenivåer leder sammantaget till att risken för översvämningar ökar längs kuster, sjöar och vattendrag.

Klimatförändringen för med sig två typer av förändring av sinsemellan skild karaktär. Den första typen av förändring är en pågående successiv stigande årsmedeltemperatur. På sikt kan detta medföra en långtgående påverkan på vitt skilda områden av samhället som exempelvis jord- och skogsbruk, teknisk infrastruktur, energiproduktion, försäkringar och turism.

Den andra typen av förändring rör påverkan på extremväder och är av särskilt stort intresse för samhällets krisberedskap. Dagens kunskap om hur ett varmare klimat inverkar på extremväder är otillräcklig och det går inte att med säkerhet förutspå kommande utveckling. Klart är dock att även vädrets extremvärden påverkas av uppvärmningen och det finns indikationer som talar för att extremväder i form av nederbörd och stormar kan komma att uppstå både oftare och med större intensitet i framtiden. Riskhantering och beredskapsplanering har hittills till största delen baserats på klimatstatistik över historiska data, och därmed alltså på ett underliggande antagande om att klimatet är stabilt. Ett klimat i förändring innebär dock att riskerna för extremväder kan vara under förändring. Tillförlitligheten i att utgå från tidigare väderförhållanden för att möta framtida försvagas därmed avsevärt.

Även om stigande havsytenivå och ett flertal värmerekord i olika delar av världen kan ses som indikationer på klimatförändringen, antas de mer djupgående effekterna till helt övervägande delen ligga en bit in i framtiden. Detta bör dock inte tas som intäkt för att avstå från att vidta åtgärder utifrån ett krisberedskapsperspektiv i nuläget. Händelser som i ett oförändrat klimat i dag kan anses som osannolika, exempelvis perioder av hetta som överstiger +40 °C i Sverige, kan plötsligt bli så pass sannolika att de bör ingå vid bedömningar av risk och sårbarhet. Med andra ord måste de klimatrelaterade frågorna omfattas av en helhetssyn gällande hot- och riskperspektiv.

5 Mer information finns på www.smhi.se (se del om Rossby center)

Erfarenheter från flodvågskatastrofen och stormen Gudrun

Detta avsnitt syftar till att ge exempel på hur arbetet med hot- och riskfrågor kan ses och användas inom krishanteringssystemet utifrån konkreta händelser.

Flodvågskatastrofen i Asien

Morgonen den 26 december 2004 inträffade en kraftig jordbävning strax utanför norra delen av Sumatra i Indonesien. Den flodvåg som framkallades av jordbävningen drabbade inom en tidsrymd av några timmar stora delar av Syd- och Sydostasien med förödande konsekvenser som följd. Den sammantagna dödssiffran uppskattas av FN till mer än 250 000 människor. Den 1 september 2005 hade enligt Rikskriminalpolisen 515 svenska dödsoffer konstaterats och 28 personer var fortfarande anmälda som saknade. Händelsen visar med skrämmande tydlighet vidden av de konsekvenser som en naturkatastrof kan medföra. Flodvågskatastrofen visar också hur det svenska samhället kan drabbas direkt av ett fenomen trots att detta inträffar i en annan världsdel.

Närmast bakomliggande orsak till denna för Sverige förändrade sårbarhet är nya mönster för turism och resande. Allt fler svenskar reser i dag både oftare och till betydligt mer avlägsna resmål jämfört med tidigare. Länder och regioner som förr besöktes av endast ett mindre antal turister är i dag ofta populära destinationer för stora rese- och charterbolag. Sammantaget har utvecklingen medfört att en betydande andel av svenskarna i dag utsätts för en annan, och i vissa avseenden förhöjd, riskbild. Denna innefattar inte endast extrema natur- och väderhändelser, utan också exempelvis smittsamma sjukdomar och terrorism.

Flodvågskatastrofen präglades – som alla katastrofer – av en rad unika omständigheter. En del av dessa yttre omständigheter, som exempelvis geografisk plats, tidpunkt på året samt den kraftiga styrkan i både jordbävningen och den efterföljande flodvågen, bidrog till att förstärka skadeeffekterna. Trots dessa särskilda omständigheter bör flodvågskatastrofen och den efterföljande krishanteringen inte ses som extremt exceptionella. Betraktat ur ett mer generellt perspektiv kan flodvågskatastrofens konsekvenser – sett som typhändelse av karaktären ”stort antal svenskar utomlands i behov av vård och/eller evakuering” – uppstå av ett flertal olika orsaker, förutom extrema natur- och väderhändelser t.ex. terrorattacker, stora olyckor och epidemisk smitta. Större koncentrationer av svenskar, både i form av turister och bofasta, finns dessutom på många platser i världen. Mot denna bakgrund framstår behovet av en god förmåga att hantera liknande framtida händelser som påtagligt.

Flodvågskatastrofen i Asien visar nödvändigheten av att se Sverige som en del av en större omvärld. Att endast ta hänsyn till de risker som är relaterade till det geografiska territoriet

Sverige är otillräckligt. Det svenska samhället är i praktiken avsevärt mer utspritt och vidsträckt än vad landets gränser anger. Vid varje given tidpunkt befinner sig en betydande del av landets medborgare och väsentliga resurser, som företag och andra organisationer, utomlands. Detta är förvisso varken nya eller tidigare okända förhållanden – det var t.ex. ett av huvudbudskapen i KBM:s Hot- och riskrapport 2004. Men återigen måste framhållas att denna trend förstärkts avsevärt sedan ett eller två decennier tillbaka och har i dag ett omfattande och högst konkret genomslag i samhället. En adekvat förståelse av risker och hot av relevans för krishanteringssystemet kräver att hänsyn tas till dessa aspekter i högre utsträckning än tidigare.

Stormen Gudrun

Den 8–9 januari 2005 drabbade stormen ”Gudrun” stora delar av södra Sverige. Stormen ledde till omfattande skador på den samhällsviktiga infrastrukturen i området, förutom de mycket stora skogsskadorna som blev den direkta följden. De indirekta konsekvenserna blev också stora på samhället i de drabbade områdena. Förutom att näringslivet drabbades utsattes den kommunala verksamheten för stora prövningar. Räddningstjänst, socialtjänst, hemtjänst, skola och barnomsorg fick snabbt anpassa sin verksamhet till det svåra läge som rådde. Kommunernas krishantering berörde i många fall stora delar av den kommunala förvaltningen. Fler än tio personer omkom under stormen och vid det efterföljande uppröjningsarbetet.

Stormen ledde till ett omfattande krishanteringsarbete i de drabbade regionerna. Främst drabbades Västra Götalands, Hallands, Skåne, Blekinge, Jönköpings, Kronobergs, Östergötlands och Kalmar län. Värst drabbades Kronobergs län. Krishanteringsarbetet blev både omfattande och utdraget i tiden. I de värst drabbade områdena fick krishanteringsarbetet i början ske under svåra förhållanden utan både elkraft och telekommunikationer. Även framkomligheten på vägar och järnvägar var mycket begränsad de första dagarna.

Stormen innebar att ett stort antal aktörer, både offentliga och privata, fick dra igång ett krishanteringsarbete som krävde stora insatser lokalt och regionalt. Även nationella och internationella resurser fick sättas in när de lokala resurserna inte räckte till. Det handlade främst om resurser för att reparera den tekniska infrastrukturen och att för hantera de oerhört stora mängderna av stormfälld skog så att resurser för reparationer, förnödenheter och annat kunde transporteras till de platser där de största behoven fanns. Prioriteringen av dessa insatser var en mycket stor utmaning för de berörda aktörerna.

Även om skadorna som stormen orsakade blev stora mildrade de rådande omständigheterna konsekvenserna. Det finns flera faktorer som bör vägas in när man drar generella slutsatser om krishanteringen i samband med stormen. Vädret var under de första veckorna efter stormen ovanligt milt.

Kyla och snö hade med största sannolikhet kraftigt förvärrat situationen och därmed också försvårat krishanteringen. För flera myndigheter, organisationer och företag som låg utanför det skadedrabbade området blev omfattningen av stormen tydlig först efter några dagar. Detta bidrog till att strukturerade stödinsatser fördröjdes, vilket blev uppenbart bl.a. när gällde att bistå med reservelverk.

Följande korta sammanfattande slutsatser kan dras om stormens konsekvenser för eldistributionen:

- Omkring 30 000 km elledning skadades. Av dessa kräver omkring nio procent komplett nybyggnation.
- Närmare 1 000 km tillfälligt utlagd kabel ligger på marken. Att åtgärda detta beräknas ta mycket lång tid.
- Det nedgrävda nätet klarade sig oskatt. I övrigt är det ännu svårt att säga vilken luftledningsteknik som är att föredra. Såväl nya som gamla stolpar har knäckts.
- Ledningsgatorna för lokalnäten är som regel inte trädsäkra. Bredare ledningsgator skulle innebära ett ingrepp i landskapsbilden.
- Uppskattningsvis 730 000 elkunder drabbades. Många av dessa drabbades dock enbart under några timmar.
- Nätbolagens beredskap var god, men otillräcklig. De samlade resurserna i landet räckte inte till vare sig personellt eller materiellt. Elsamverkansorganisationen fungerade däremot bra.
- Röjningsarbetet byggde till stor del på frivilliga krafter organiserade utifrån respektive lokalsamhälle. Bristen på röjningsresurser försenade arbetet med att återuppbygga elnätet.
- Brister förelåg beträffande tillgång till och fördelning av reservkraft.
- Telekommunikationssystemet visade sig innehålla allvarliga brister. Beredskapen och återuppbyggnadsarbetet inom teleområdet hade brister.

När det nuvarande elnätet planerades och byggdes var det mycket svårt att föreställa sig omfattningen av det elberoende som präglar samhället ett antal decennier senare. Industrin har exempelvis ett stort behov inte bara av maskiner på verkstadsgolvet utan även av mycket tät kommunikation och av så kallade just-in-time leveranser. Till detta kommer att beroendet av informationssystem och kommunikation via Internet har ökat avsevärt under denna tid och kommer att öka ännu mer i framtiden. Under stormen Gudrun visade det sig att man även drabbades av andra avbrott i olika samhällstjänster. Varken mobiltelesystemet eller lokalradion fungerade tillförlitligt eftersom också dessa drabbades av elavbrott. Detta resulterade i att räddningsinsatser och annan verksamhet uteblev eller fördröjdes.

Återuppbyggnaden efter stormen pågår fortfarande. Detta innebär i sig en riskexponering inför eventuella nya och kanske inte så extrema, väderhändelser. Exempelvis finns det relativt

många provisoriska lösningar inom såväl el- som telekommunikationsområdet som har konsekvenser för krisberedskapen. Dessutom finns det en rad sociala dimensioner av att återuppbyggnadsarbetet inte är färdigt. Förtroende och tillit till olika aktörer i samhället kan långsiktigt skadas om detta arbete inte fungerar.

Pandemisk smitta

Smittsamma sjukdomar och utbrott av epidemier har varit en ständig följeslagare till människan och förekommit under alla tider. Med skiftande intervall har uppkomsten av en ny eller förändrad smittsam sjukdom orsakat pandemier, d.v.s. världsomfattande epidemier. Trots vetenskapliga framsteg, förbättrade behandlingsmetoder och utveckling av vaccin är risken för utbrott av nya epidemier och pandemier fortfarande ett faktum. På olika sätt har samhällets sårbarhet inför omfattande epidemier och pandemier snarare ökat de senaste decennierna.

Utbrott av pandemier finns dokumenterade ända tillbaka till 1500-talet och har sedan dess förekommit i genomsnitt tre gånger per århundrade med intervall på mellan 10 och 50 år. Under 1900-talet inträffade influensapandemier vid tre tillfällen, ”Spanska sjukan” 1918–1919, ”Asiaten” 1957 och ”Hongkong” 1968. Ett återkommande mönster under de tre pandemierna har varit snabb och omfattande smittspridning. Enligt Socialstyrelsen kan vid denna typ av pandemier (av influensavirus) upp till 15–30 procent av befolkningen insjukna under en period av ett fåtal veckor.[6] En sådan hög nivå av smittspridning gör att även utbrott med en förhållandevis låg dödlighet, som pandemierna 1957 och 1968, medför omfattande konsekvenser för samhället.

Det är samtidigt viktigt att inse att förutsättningarna för uppkomst och utveckling av en pandemi är annorlunda i dag jämfört med tidigare. Dagens samhälle är globaliserat i en helt annan utsträckning än vad som var fallet vid de tre pandemierna under 1900-talet. Handel, resande och andra former av kontakter mellan olika länder och regioner har nått nivåer som långt överskrider tidigare decenniers. Utvecklingen av flygtrafiken har dessutom dramatiskt förkortat rese- och transporttiden. Globaliseringen har som oavsiktlig sidoeffekt skapat nya möjligheter för snabb och effektiv smittspridning. Detta visades tydligt under 2002–2003 då SARS, en virussjukdom som orsakar svårartad lunginflammation, spreds med hög hastighet mellan ett flertal länder i Sydostasien och vidare till Nordamerika. Endast efter omfattande ansträngningar, genom bl.a. restriktioner för resande och karantän av sjuka, kunde spridningen efter hand begränsas, dock inte utan att orsaka betydande

6 Socialstyrelsen, ”Influensa – Strategier för prevention och kontroll”

ekonomiska kostnader och utbredd social oro. SARS har en förhållandevis låg smittsamhet, då smitta uppstår endast vid nära kontakt med en insjuknad person. Enligt WHO:s bedömning skulle liknande insatser som de som framgångsrikt begränsade SARS vara otillräckliga för att förhindra utbrott av sjukdomar med högre smittsamhet från att utvecklas till en pandemi. Detta kan exempelvis gälla influensavirus som kan spridas per luft och är smittsamt redan innan sjukdomssymptomen blir märkbara.[7]

För ”Asiaten” och ”Hongkong” tog det månader från lokalt utbrott till global spridning. Genom bl.a. den utbredda flygtrafiken skulle idag motsvarande förlopp kunna gå betydligt snabbare och snarare räknas i veckor eller dagar. Smittspridningens hastighet försvårar sjukvårdens och samhällets möjligheter till effektiva motåtgärder, dels genom att tidsspannet från upptäckt av smittan till dess att den svenska befolkningen drabbas har förkortats, dels genom att stora delar av världen drabbas i princip samtidigt vilket begränsar möjligheten till internationella hjälpinsatser.

Den alltmer sammanflätade världen har gjort steget från lokalt utbrott av en smittsam sjukdom till pandemi avsevärt mindre. Samtidigt balanseras dessa ökade risker till viss del av att utvecklingen även lett till ökade möjligheter att upptäcka sjukdomar tidigt och att förvarna om utbrott. I en värld där information förmedlas snabbare än någonsin och där få, om några, områden är helt isolerade är det avsevärt mindre risk att en epidemi uppstår oupptäckt.

Influensa och andra smittsamma sjukdomar

Många experter lyfter fram influensavirus som en av de största riskerna för att en pandemi ska uppstå. Anledningen till detta är bl.a. virusets höga smittsamhet och dess förmåga att återkomma i nya skepnader.

Mer begränsade utbrott av influensa uppstår så gott som varje år. Detta beror på gradvisa förändringar i virusets egenskaper vilket medför att många saknar eller har begränsad immunitet mot smittan. Riktigt farligt blir influensaviruset dock då det sker en plötslig och genomgripande förändring i virusets genetiska uppbyggnad. Detta kan ske exempelvis om influensavirus från en människa blandas med influensavirus från fågel eller gris. Inför en sådan ny variant av influensa saknar stora delar av befolkningen helt immunitet. Risken för omfattande smittspridning och pandemi är därför mycket hög. Exakt vilka följder en pandemi medför går inte att säga på förhand utan beror på ett flertal faktorer som t.ex. virusets dödlighet, smittsamhet, smittvägar och i vilket land utbrottet uppstår.

7 WHO, ”Avian influenza: assessing the pandemic threat”

Det finns samtidigt en risk med att alltför ensidigt fokusera på influensapandemier. Många andra smittsamma sjukdomar kan ha förmågan att utlösa utbrott med potential att utvecklas till pandemier eller på annat sätt orsaka allvarliga störningar på samhällets funktion. Utbrottet av SARS orsakades exempelvis av ett tidigare okänt coronavirus. Hiv/aids har i vissa regioner smittat en så hög andel av befolkningen att det vuxit till ett strukturellt hot mot samhällets utveckling. Ett annat problemområde är den ökande förekomsten av multiresistenta bakterier vilket på sikt kan framkalla betydande svårigheter för sjukvården. Gamla folksjukdomar som malaria och tbc skördar miljontals liv varje år. Fortfarande drabbas främst utvecklingsländer men smittspridningen har under senare år ökat i Sverige och Europa. Ett exempel på denna trend är utbrottet av tbc i Bromma i Stockholm som uppmärksammades i slutet av sommaren 2005. Den förhållandevis låga smittsamheten hos tbc gör den till ett problem snarare för sektorerna smittskydd och sjukvård snarare än för krishanteringssystemet i sin helhet. Samtidigt visar händelserna i Bromma hur även ett relativt begränsat utbrott kan orsaka stor social oro samt tryck från allmänhet och media mot ansvariga aktörer.

Djursjukdomar

Stora utbrott av smittsamma djursjukdomar kan orsaka allvarliga störningar i samhället och leda till mycket omfattande ekonomiska skador. Aktuella exempel som tydligt visar detta är det pågående utbrottet av fågelinfluensa (se nedan) och det utbrott av mul- och klövsjuka som drabbade Storbritannien 2001. I båda dessa fall har följderna nått långt utanför de direkt drabbade uppfödarna och djuren och slagit hårt mot hela samhällen. För att hantera smittoutbrottet och dess konsekvenser är det ofta nödvändigt med långtgående åtgärder – som avspärrningar, karantän, nödslakt och handelsrestriktioner – vilka kan behöva genomföras både i en omfattande utsträckning och under en utdragen tidsperiod.

Djursjukdomar kan också utgöra ett hot mot människors hälsa. Rabies, salmonella och West Nile Fever är exempel på sjukdomar som kan smitta människor via djur. Många smittsamma sjukdomar som människor drabbas av har ursprungligen utvecklats ur djursjukdomar. SARS och hiv är exempel på sjukdomar som tidigare funnits hos djur men efter gradvisa förändringar eller plötsliga mutationer överförts till människor. De tre influensapandemierna under 1900-talet anses ha haft sitt ursprung i en blandning av mänskliga influensavirus och influensavirus från grisar och fåglar. Genom

uppblandningen förändras viruset och kan spridas då befolkning saknar immunitet mot dessa nya typer. De två senaste pandemierna uppstod i Asien, vilket anses bero på det mycket stora antalet människor som lever i nära kontakt med grisar och fåglar.[8] Genom att följa utvecklingen av sjukdomar hos djur kan man på ett tidigare stadium upptäcka risker som på sikt kan leda till nya hot mot människors hälsa.

Förutsättningarna för spridning av djursjukdomar har, på liknade sätt som för humansjukdomar, påverkats av trenden mot ett alltmer gränsöverskridande samhälle. Omfattande internationell handel med djur och livsmedel ökar riskerna för smittspridning. Detta gäller särskilt då gränsskydd och kontroll och provtagning minskat under senare år. Som en följd av detta har även smuggling och annan illegal införsel av djurarter ökat vilket ytterligare bidrar till riskerna för spridning av nya djursjukdomar till Sverige.[9] Ett oroväckande exempel kommer från Belgien där flygplatspersonal i oktober 2004 avslöjade ett försök att illegalt införa två örnar från Thailand; båda fåglarna visade sig efter provtagning vara smittade med fågelinfluensa av H5N1-typ.[10]

Fågelinfluensa

Ett i högsta grad aktuellt exempel som belyser riskerna med både influensavirus och djursjukdomar är utbrottet av fågelinfluensa (H5N1) i Sydostasien. Utbrottet som först inleddes i Hong Kong 1997 bedöms av många expertorgan utgöra en betydande risk för pandemi.

Fågelinfluensa är inte ett nytt fenomen utan identifierades enligt WHO redan 1959 och har sedan dess i olika varianter drabbat höns- och fågeluppfödning i ett tjugotal utbrott. Dessa utbrott var dock betydligt mer begränsade än det som nu pågår i Sydostasien. Efter att utbrottet först upptäcktes i Hong Kong 1997, och då begränsades genom omfattande nödslakt av fåglar, upptäcktes det åter i slutet av 2003 och spreds snabbt vidare över stora delar av Sydost- och Östasien. Enligt WHO hade vid slutet av september 2005 omkring 115 människor smittats av fågelinfluensa, och av dessa hade drygt 60 avlidit. Samtidigt har mer än 100 miljoner fåglar dött eller nödslaktats. Utbrottet är det hittills geografiskt största och tidsmässigt utdragna som inträffat.[11]

Vid tidigare epidemier av fågelinfluensa har fall då smittan överförts till människor varit extremt ovanliga. Fram till 1997, då det första dokumenterade fallet av direkt smitta mellan fågel och människa inträffade i Hongkong, ansågs detta vara omöjligt. Trots att ett

8 Socialstyrelsen, Influensa – Strategier för prevention och kontroll

9 Smittskydd, nr 3/2005

10 WHO, ”Avian influenza: assessing the pandemic threat”

11 http://www.smittskyddsinstitutet.se/SMItemplates/Article____5504.aspx

i jämförelse med tidigare utbrott stort antal människor insjuknat är risken att smittas av fågelinfluensa oerhört liten. Smittan överförs främst genom nära kontakt med sjuka fåglar eller deras avföring. I ett mycket litet antal fall kan även spridning från människa till människa ha inträffat. Antalet personer som hittills smittats ska också ses i relation till de miljontals människor i Asien som dagligen hanterar fåglar.

Det stora hotet mot människors hälsa är inte fågelinfluensan som den ser ut i dag utan risken att viruset ska förändras och få förmåga till effektiv spridning mellan människor. Enligt Socialstyrelsen och Smittskyddsinstitutet är risken för en sådan utveckling svårbedömd. Eftersom fågelinfluensan fram till nu smittat endast ett relativt litet antal personer, verkar viruset ha svårt att anpassa sig till människor. Om lika gynnsamma förutsättningar består framöver går dock inte att säga. Risken för förändringar i viruset ökar i takt med att fler människor och djurslag blir smittade. Särskilt oroande är om personer som smittas av fågelinfluensa samtidigt bär på vanlig influensa, då detta kan leda till att fågelviruset tar över egenskaper från det mänskliga viruset och ytterligare öka risken för att H5N1 kan spridas effektivt mellan människor.

En av anledningarna till att utbrottet av fågelinfluensa betraktas som så oroväckande är den höga dödlighet som H5N1-viruset uppvisat. Drygt tre fjärdedelar av alla patienter som fått diagnosen fågelinfluensa har avlidit. Siffrorna bör dock betraktas med viss försiktighet, då många fler personer sannolikt har smittats och insjuknat med lindrigare symptom och därmed undgått diagnos.[12] Under sommaren och hösten 2005 har fågelinfluensan spridit sig till Europa. Bekräftade fall har upptäckts i Ryssland, Turkiet och Rumänien. Vilken utbredning en eventuell spridning av viruset har bland flyttfåglar och vilka följdverkningar detta kan ge för fortsatt smittspridning går ännu inte att fastställa men denna utveckling är av mycket stor vikt att följa.[13]

Konsekvenser vid ett utbrott

WHO har under 2004 och 2005 uppmanat medlemsländerna att höja sin beredskap för pandemier mot bakgrund av fågelinfluensans spridning. Oavsett om det nu pågående utbrottet av fågelinfluensa ger upphov till en influensapandemi eller ej, kvarstår pandemirisken. All tidigare erfarenhet pekar mot att en pandemi av influensa eller någon annan smittsam sjukdom kommer att inträffa inom en kortare eller längre tidsperiod.

Socialstyrelsen och Smittskyddsinstitutet bedömer att det svenska smittskyddet har en godtagbar förmåga att hantera begränsade smittoutbrott. Samma bedömning gör Jordbruksver-

12 Ibid.

13 Smittskydd nr 3/2005

ket och Statens veterinärmedicinska anstalt vad gäller djursjukdomar. Myndigheterna framhåller dock att vid mer storskaliga epidemier eller vid en pandemi kommer de tillgängliga resurserna inom smittskyddet, som laboratorie- och provtagningskapacitet samt vårdplatser vid infektionskliniker, sannolikt att visa sig otillräckliga. Redan de årligen återkommande normala influensaepidemierna får effekter på hälso- och sjukvården. Främst sker detta genom att antalet vårdsökande blir fler, vilket kan medföra betydande utmaningar då det akuta behovet av slutenvårdsplatser ofta överstiger tillgången redan under en ganska normal säsong. Vid en större epidemi eller pandemi menar Socialstyrelsen att det är helt orealistiskt att räkna med tillräcklig kapacitet vid landets infektionskliniker.[14]

Exakt vilka följder en omfattande epidemi eller pandemi får går inte att avgöra på förhand utan beror bl.a. på mönster och omfattning av smittspridningen samt sjukdomens dödlighet. De initiala effekterna kommer huvudsakligen att slå mot hälso- och sjukvårdssektorn, vars resurser snabbt hamnar under extrem ansträngning. Samtidigt är det viktigt att inse att konsekvenserna inom kort kan komma att bli mycket omfattande för samhället som helhet. Enligt Socialstyrelsens bedömning kan totalt sett uppemot en tredjedel av befolkningen insjukna. Detta är dock den genomsnittliga andelen; inom en del områden och på vissa arbetsplatser kan nivån av smittade vara avsevärt högre.

Många insjuknade, särskilt barn och äldre, kommer dessutom att behöva vård från anhöriga. Detta leder till att sannolikheten är hög för att det ska uppstå omfattande problem beroende på personalbrist. Inom många verksamheter är sårbarheten för personalbortfall stor på grund av höga effektivitetskrav och ekonomiska neddragningar. Även upprätthållandet av samhällsviktig verksamhet som polis, räddningstjänst, transportsystem, energidistribution och vård och omsorg, kan komma att begränsas.

Till dessa direkta effekter måste läggas samhällsekonomiska konsekvenser och den påverkan på den internationella handeln som sannolikt följer på ett pandemiutbrott. Företag och handel är i hög utsträckning beroende av ett ständigt flöde av kommunikation och transporter. Utbrottet av SARS visar tydligt hur resande och transporter mellan, och i viss mån inom, länder kraftigt begränsas under en pandemi. Detta är en följd dels av åtgärder för att begränsa smittspridningen, som reserestriktioner och olika former av karantän, dels av ett frivilligt avstående från resande beroende på rädsla för smittan. Trots att utbrottet av SARS kunde begränsas och efter hand hanterades överlag framgångsrikt blev de ekonomiska följdverkningarna och andra

14 Socialstyrelsen, Influensa – Strategier för prevention och kontroll

störningar i de drabbade länderna omfattande. Erfarenheterna från SARS ger i denna bemärkelse en förvarning de mycket långtgående konsekvenser som en mer utbredd epidemi eller pandemi kan orsaka.

God tillgång till och en fungerande distribution av vaccin och antivirala läkemedel skulle sannolikt kunna begränsa konsekvenserna av en pandemi avsevärt. Enligt Socialstyrelsen kommer dock tillgången på vaccin under de inledande skedena av en pandemi att vara begränsad. Detta beror dels på att det rör sig om en ny typ av virus och produktionen av vaccin inte kan inledas förrän virusstammen är identifierad och karakteriserad, dels på att vaccintillverkarnas förmåga att på kort tid producera stora mängder av ett nytt influensavaccin är begränsad. Slutsatsen är att samhället inte kan förvänta sig att pandemier och stora smittutbrott kan avvärjas genom massvaccinationer. Särskilt utsatta är länder som, liksom Sverige, saknar egen produktion av influensavaccin.

I en sammantagen riskbedömning av pandemi och omfattande epidemier framstår två faktorer som väsentliga ur ett krisberedskapsperspektiv. För det första måste ett pandemiutbrott i ett längre tidsperspektiv betraktas som omöjligt att undvika. För det andra är de möjligheter vi har att undgå konsekvenserna av en pandemi begränsade trots förbättringar av vaccin och andra läkemedel. Utgångsläget för planering måste vara att ett stort antal människor insjuknar vid en pandemi. Detta kommer att leda till omfattande effekter på samhället som helhet och kan komma att orsaka allvarliga störningar i samhällsviktig verksamhet. Ur resonemanget kring dessa två faktorer kan i sin tur två slutsatser dras: Eftersom pandemier bör ses som kontinuerligt återkommande, måste samhället ha en godtagbar förmåga att hantera konsekvenserna av dessa. Konsekvenserna av en omfattande epidemi eller pandemi drabbar hela samhället och ställer därmed krav på alla delar av krishanteringssystemet.

Aktörsrelaterade hot och risker

Detta avsnitt behandlar ett par exempel på aktörsrelaterade hot och risker att ta hänsyn till i krisberedskapsarbetet. De beskrivna fenomenen är tämligen olika till sin natur men som avsnittet visar har de olika konsekvenser för samhällets krisberedskap.

Terrorism

Terrorhotet har under de senaste åren varit det dominerade aktörsrelaterade hotet, händelser som 11/9 2001 i New York, Balibombningarna 2002 och i oktober i år, attentaten i Sharm-el-Sheik i juli, Madrid den 11 mars 2004, de nästan dagliga attentaten i Irak osv. Listan kan göras mycket lång. Alla dessa händelser har gjort att terrorhotet har varit påtagligt närvarande för det stora flertalet av oss. Utvecklingen inom terrorområdet, vilken har såväl internationella som nationella dimensioner, följs och förberedande och hanterande åtgärder planeras för att möta denna typ av hot. Att följa den internationella utvecklingen är ett sätt att skapa förutsättningar för att bygga fungerande krisberedskap inom detta komplexa och föränderliga område.

Vi vet med vilka medel terrorgrupper hittills genomfört attacker, och vilka konsekvenser det inneburit. Det finns emellertid skäl att utveckla vår kunskap om vilka ytterligare medel och konsekvenser som man måste ta hänsyn till i arbetet med samhällets säkerhet och beredskap.

London den 7 juli 2005

Den 7 juli i år kom den storskaliga självmordsterrorismen till Europa. På förmiddagen genomförde fyra brittiska medborgare en samordnad attack mot Londons kollektivtrafiknät. Hur krishanteringsarbetet bedrivits i samband med dessa händelser väcker en rad intressanta frågor om den svenska krisberedskapen.

Sedan den 11 september 2001 har många länder riktat insatserna inom kontraterrorarbetet mot underrättelseinhämtning och -analys. Trots att mycket stora resurser satsats på denna verksamhet världen över kunde alltså inte Londonattentaten förhindras. Den

brittiska säkerhetstjänsten BSS (MI5) sänkte till och med sin bedömning av hotnivån avseende internationell terrorism från ”servere general”, som är den näst högsta nivån, till den lägre nivån, ”substantial”, veckorna före attentatet då det inte fanns några manifesta indikationer på något förestående attentat. Detta visar hur oerhört svårt det är att förutse och därmed förhindra denna typ av händelser och att en stark fokusering på och resursallokering till underättelseinhämtning inte är tillräcklig. Självklart behövs starka underättelsefunktioner, dock kräver denna typ av terrorhot att arbetet bedrivs med olika medel och metoder och kanske framför allt utifrån fler perspektiv än det rent brottsbekämpande. Denna typ av terrorism behöver analyseras och förstås utifrån en helhetssyn på både fenomenet och samhället i stort. Politiska, sociala, teologiska och ekonomiska dimensioner, utifrån ett brett samhällsperspektiv, måste komplettera de rent brottbekämpande perspektiven.

Skälen till att de mer traditionella brottsbekämpande insatserna (underrättelseinhämtning, gränsskydd m.m.) inte var tillräckliga vid Londonhändelserna är flera. Ett skäl var att attentatsmännen var brittiska medborgare och redan fanns i landet, ett annat var den typ av mål som attentatsmännen valde. De preventivt riktade insatserna som exempelvis gränsskydd och skalskydd var alltså inte tillräckliga för att förhindra attentaten. Vidare är det moderna öppna samhället, i sig självt, sårbart för denna typ av attentat. Med andra ord är det mycket svårt att undvika eller förebygga illdåd av detta slag.

Att dessa brottsförberedande preventiva åtgärder därmed visat sig otillräckliga för att förhindra denna typ av brott, ställer krav på andra funktioner i samhället. Det rör sig om såväl sociala och politiska åtgärder som förmågan att hantera konsekvenserna för samhället om ett attentat inträffar. Detta gäller exempelvis räddningstjänst, brottsutredande funktioner och sjukvårdens förmåga att ta hand om skadade. Men det gäller också förmågan att upprätthålla förtroendet för samhället. Exempel på detta är den snabba och effektiva polisutredning som följde på Londonattentaten som hade stora förtroendeskapande effekter.

De brittiska myndigheterna kan ur ett krisberedskapsperspektiv sägas ha uppvisat en väl fungerande beredskap för att hantera denna typ av händelse, både när det gäller dimensioneringen och när det gäller samordningen av operativa krishanteringsresurser som räddningstjänst, sjukvård och polisiär verksamhet. Förutom dessa rent undsättande och vårdande funktioner har de brittiska myndigheterna varit framgångsrika i sitt arbete att hantera den efterföljande brottsutredningen. Att snabbt komma fram med resultat inom detta område har en stark signaleffekt på samhällets förtroende för samhällets olika funktioner.

De olika aktörer som arbetar med antiterror- och krisberedskapsfrågor i Storbritannien hade redan före attentatet identifierat terrorhotet och bedömt

risken för ett attentat just i London som stora.[15] Trots avsaknaden av manifesta underrättelser om specifika aktörer eller mål möjliggjordes en ändamålsenlig resursallokering till samhällets olika funktioner som har roller i det brittiska krishanteringssystemet. Skälet till detta är att före attentaten behandlade myndigheterna terrorproblematiken ur ett generellt hot- och riskperspektiv som omfattade både de manifesta och latenta dimensionerna.

Händelserna den 7 juli visar på att verktygen som fanns utifrån ett manifest hotperspektiv inte räckte till för att förhindra att attentaten genomfördes. Dock hade hot- och riskanalyserna som genomförts, vilka även omfattade de latenta hoten, visat att risken fanns för att ett attentat med sådana stora konsekvenser kunde inträffa. De krishanterande aktörerna hade både beredskapen och resurserna för att mildra de samhälleliga konsekvenserna av en storskalig terrorattack utan att det fanns manifesta förvarningssignaler.

Att på detta sätt i det förberedande krisberedskapsarbetet analysera terrorhotet utifrån både ett manifest och ett latent hotperspektiv innebar att en fungerande krishanteringsapparat fanns till hands trots att det inte fanns specifika indikationer avseende aktörer eller mål. För svenskt vidkommande visar detta på ett behov av flexibla och helhetsorienterade hot- och riskbedömningar där händelser med låg sannolikhet men med stora konsekvenser tas hänsyn till. Utan en sådan ansats riskerar samhället att stå särdeles illa rustat inför denna typ av hot.

Den svenska hotmiljön

Säkerhetspolisen (Säpo) har till uppgift att leda och bedriva polisverksamhet för att förebygga och beivra brott mot rikets säkerhet. Säkerhetspolisen ska även leda och bedriva polisverksamhet när det gäller terrorismbekämpning.

Säpos uppdrag och arbetet med dessa frågor kan beskrivas som inriktat mer mot de manifesta typerna av hot. Säpos bedömningar vilar på en bred underrättelseinhämtning och -analys. Säpos bedömning är att sannolikheten för terrorattentat direkt riktade mot Sverige för närvarande är låg, däremot finns en risk att utländska intressen i Sverige kan drabbas. Säpo betonar också att förändringar i omvärlden snabbt kan förändra hotbilden för Sverige och utländska intressen i Sverige.

Just att händelser i och utanför Sverige snabbt kan påverka hotbilden, är en av de saker som skiljer terrorhotet från exempelvis den hotbild som fanns under det kalla kriget. Under det kalla kriget uppfattades hotet som konstant, känt och därmed planeringsbart. Terrorhotet är annorlunda på flera sätt, men den kanske största skillnaden är de komplicerade delmängder av potentiella förvarningssignaler som finns

15 ”The London bombings and the broader strategic context”, Dr. Magnus Ranstorp, 2005-07-20. Artikel publicerad hos The Elcano Royal Institute

och att till synes små händelser i vår omvärld mycket snabbt kan förändra förutsättningarna.

Det förberedande arbetet inom området samhällets säkerhet och beredskap bör således utgå från ett generellt och bredare hotperspektiv. I analysen av den svenska hotmiljön bör man också beakta de hot och risker av mer latent karaktär kopplade till terrorområdet. Syftet med detta ska vara att nå en bred och generell krisberedskap i samhället.

Följande punkter utgör exempel på sådana omständigheter som visar hur man kan ta hänsyn till latenta hot i krisberedskapsarbetet:

- Sverige har en aktiv utrikespolitik. Precis som de flesta länder agerar Sverige i den internationella miljön, bl.a. genom fredsfrämjande operationer och som medlem i EU. Händelser i omvärlden kan därför mycket snabbt förändra hotbilden för Sverige och därmed för den svenska krisberedskapen. Att hotbilden är så föränderlig ställer stora krav på ett flexibelt förhållningssätt i genomförande av förberedande insatser. De konsekvenser som kan antas uppstå från dagens hot kan mycket väl vara helt annorlunda i morgon, då förutsättningarna för hotanalysen mycket fort kan ändras.
- Islamistiskt orienterade aktörer som har terrorism på sin politiska agenda, finns idag i Sverige. Begreppet islamism innefattar både sunnitisk och shiitisk politisk extremism med skilda etniska och nationella tillhörigheter och det senaste decenniet har inneburit en internationalisering av grupper, organisationer och strukturer som omfattas av detta tankegods. Ett samlingsbegrepp för detta fenomen kan beskrivas som jihadterrorism. Viktigt att notera är att detta är politiska idéer som inte på något vis får förväxlas med islam som religion.

  Enligt Säpo finns det idag en rad individer och grupper som är verksamma i Sverige. Dessa bedriver i första hand religiös och politisk verksamhet. Att dessa grupper finns i Sverige kan innebära att finansierings- och logistikinsatser kan bedrivas, vilka kan vara mycket svårupptäckta. Erfarenheterna från attackerna i London i juli 2005 visar just att när dessa personer lever och verkar i samhället är det mycket svårt att förhindra att dessa genomför systemhotande verksamhet, genom exempelvis logistiska uppgifter.
- Det finns en social och politisk jordmån för dessa politiskt extrema idéer i Sverige. De internationella erfarenheterna från såväl forskning som myndighetshåll visar att radikaliseringen av främst unga, andra generationens muslimer kanske är den stora utmaningen för antiterrorarbetet i våra samhällen. De bakomliggande drivkrafterna för radikaliseringen kan vara flera och mångfacetterade. Det finns exempel på hur upplevt socialt och ekonomiskt utanförskap, kombinerat med

svårigheter att finna gemenskap med såväl det ”nya” som det ”gamla” landet, kan leda till en radikalisering både gällande de politiska och de religiösa dimensionerna i livet. Dessa tendenser finns även här. Sverige är inte immunt mot denna typ av politiska rörelser. Exempelvis finns såväl ekonomisk som social segregation, i synnerhet i och kring storstadsregionerna. Att förstå de olika drivkrafterna bakom politisk/islamistisk radikalisering är en viktig utgångspunkt för arbetet med samhällets säkerhet och beredskap. Kunskap om vad de fenomen som bidrar till att politiska idéer som kan leda till terrorhandlingar, är nödvändig för att aktörer med ansvar för samhällets samlade krisberedskap ska kunna lösa sina uppgifter.

- Det finns utifrån ett krishanteringsperspektiv vissa brister i det svenska samhällets beredskap inför händelser liknande Londonattentaten. Dessa sårbarheter kan således i sig utgöra ett hot som bör tas i beaktande när hot- och riskbedömningar görs inom terrorområdet[16].

Det som ovan beskrivs leder till slutsatsen att terrorhotet är komplext. För att kunna förstå och hantera hoten och riskerna inom detta område måste samhällets olika aktörer samverka, och aktörer med olika uppgifter måste på ett mer funktionellt sätt arbeta med olika metoder och från olika utgångspunkter. Att enbart förlita sig på en sannolikhetsbaserad hot- och riskanalys på terrorområdet kan leda till situationer där samhället står mycket illa rustat inför konsekvenserna av en terrorattack.

Å andra sidan kan en alltför ytlig och vårdslös bedömning av hoten och riskerna leda till att resurser förslösas och andra hot- och riskområden blir eftersatta. Denna balans är svår, men nödvändig att hålla för varje aktör i krishanteringssystemet.

Andra aktörsrelaterade hot

Med detta delavsnitt vill vi beskriva den bredd som finns när det gäller aktörsrelaterade hot. Utöver terrorism finns andra hot som på sikt kan vara utmaningar mot samhällets grundläggande värden och som är tämligen vanligt förekommande. Här nedan följer två exempel på sådana hot.

Organiserad brottslighet

Såväl internationella som nationella erfarenheter visar att den organiserade brottsligheten mer och mer framstår som ett säkerhetshotande fenomen. Exempelvis är organiserad brottslighet ett av huvudområdena i EU:s säkerhetsstrategi. Ett av de främsta skälen

16 För mer information, se KBM:s omvärldsexempel 2005.

till detta är de allvarliga konsekvenser den organiserade brottsligheten har på rättstaten och dess funktioner.

Även i Sverige har detta fenomen på senare tid fått konsekvenser som är både bredare och djupare än tidigare. Organiserad brottslighet har börjat ses som något som får följder utöver de rent brottsliga konsekvenserna, till att omfatta även sådana konsekvenser där samhällets grundläggande värden hotas. Exempelvis pågår en diskussion om huruvida Säpo ska vidga sina uppgifter till att även omfatta den organiserade brottsligheten. Skälen bakom detta förslag är att organiserad brottslighet, på samma sätt som exempelvis terrorism och olaglig underrättelseinhämtning, medför konsekvenser för våra gemensamma värden och därmed blir en fråga för nationens säkerhet och beredskap.

För svensk krisberedskaps vidkommande är organiserad brottslighet främst en angelägenhet för polis och rättsväsen. Dock finns det skäl att utifrån ett generellt krisberedskapsperspektiv följa utvecklingen. De konsekvenser som den organiserade brottsligheten för med sig, avseende exempelvis tilliten till rättsstaten, är en angelägenhet för samhället i stort. För att bygga en bred och generell krisberedskap bör dessa fenomen vara medtagna i de övergripande hot- och riskbedömningarna.

Hot mot förtroendevalda

Den 22 maj 2005 utsatte en enskild person eller en grupp kommunalrådet i Malmö för ett attentat. Någon eller några avfyrarde ett vapen mot dennes bostad. Detta var inte första gången som detta kommunalråd utsattes för liknande hot. Trots upprepade våldshandlingar och hot om våld fortsätter kommunalrådet sitt förtroendeuppdrag. Om denne i stället skulle ta beslutet att hoppa av sitt uppdrag, till följd av att hoten blir en alltför stor belastning på honom personligen, vad kan då sägas om exempelvis konsekvenserna för demokratin?

Det öppna och demokratiska samhället bygger på att våra folkvalda kan utföra sina uppdrag i enlighet med de spelregler som demokratin stipulerar. Men vad händer egentligen om dessa politiskt engagerade människor på grund av våld eller hot om våld mot dem själva eller deras närstående tappar viljan att inneha politiska förtroendeuppdrag? Våld eller hot om våld mot förtroendevalda har därmed en ytterst allvarlig påverkan på samhällets grundläggande värden. Detta innebär att svensk krisberedskapsförmåga kan komma att påverkas negativt och att krishanteringssystemets aktörer därför bör ha både en kunskap om vilka konsekvenserna detta svåra, latenta fenomen kan leda till och hur det förberedande arbetet bör hanteras.

Hot mot folkvalda i kommuner är något som diskuteras som ett framväxande fenomen på flera håll i samhället. Justitiedepartementet, Brottsförebyggande rådet (BRÅ) och Sveriges kommuner och landsting (SKL) är några av de aktörer som identifierat hot mot

förtroendevalda som ett problem. Bl.a. genomförde TEMO en undersökning[17] på uppdrag av SKL som visade att fler än hälften av alla tillfrågande ansåg att hot mot politiker är ett stort samhällsproblem. Vidare ansåg de flesta att detta fenomen har sin bakgrund i ”ett allmänt hårdare klimat i samhället”. Hur det än är med bakgrundsfaktorerna är detta ett problem som såväl myndighets-sverige som allmänheten anser vara ett problem som över tid kan utvecklas till att bli något som utmanar samhällets krishanteringsförmåga. Detta genom exempelvis att ledningsstrukturer ur ett kompetssäkringsperspektiv kan försvagas och därmed möjligheten till kraftfullt och ändamålsenligt agerande vid en kris, vilket i sin tur kan leda till förtroendeglapp mellan den politiska ledningen på den lokala nivån och medborgarna.

Detta fenomen kan och bör således inte hanteras utifrån ett strikt polisiärt perspektiv; det förberedande arbetet är här viktigt. Att enbart agera reaktivt, efter ett dåd, medför att skadan redan är skedd utifrån ett värde- eller krisberedskapsperspektiv. Det reaktiva, polisiära arbetet som respektive polismyndighet hanterar utifrån sitt uppdrag, bör alltså kompletteras med en rad andra insatser gällande exempelvis relationerna till såväl lokala som regionala media, olika former av utbildningsinsatser i skolor m.m. Men kanske framför allt bör krishanteringssystemets aktörer behandla detta fenomen i ett större perspektiv, nämligen ett perspektiv som tar hänsyn till hotet i sin helhet, där de grundläggande värdena för samhället i stort är en del av det som hotas och som gör att dessa frågor behandlas som en del av den svenska krisberedskapen.

17 ”Allmänheten om politiker, hot och mediernas roll”, TEMO juni 2005

Hot mot infrastrukturen – CIP

De hot och risker som behandlas i denna rapport, såväl manifesta som latenta, riktar sig mot sådana samhällsfunktioner som behöver upprätthållas för att det ska vara möjligt att värna våra grundläggande värden. I detta sammanhang har den kritiska, eller samhällsviktiga, infrastrukturen en betydelsefull roll. Den kan betraktas som nödvändig för såväl upprätthållandet av den vardagliga funktionaliteten som för möjligheten att hantera och avhjälpa kriser.

Med begreppet infrastrukturer avses de underliggande strukturer som behövs för att ett samhälle ska fungera. De är nödvändiga för det dagliga livet och befolkningens livsbetingelser. Exempel på infrastrukturer är elnät, vägar, vattenledningar osv.

Vad som betraktas som kritisk infrastruktur och hur den indelas beror på sammanhanget. Någon allmänt erkänd definition eller indelning finns inte. Infrastrukturer är viktiga för ett samhälle men utgör inte allt som gör att ett samhälle fungerar. Exempelvis är befolkningen inte en infrastruktur, och terrängen eller territorialvattnet kan rimligtvis inte heller räknas dit. Dock anses vissa vattendrag och kanaler i många länder som en del av transportinfrastrukturen. De flesta tillverkningsindustrier och tjänsteproducerande företag är beroende av fungerande infrastrukturer men kan knappast räknas som en del av infrastrukturen.

Det finns många definitioner på vad kritisk eller samhällsviktig infrastruktur omfattar. I exempelvis USA används följande definition:[18]

> "...systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"

Betoningen ligger följaktligen på de system och tillgångar som är av bety-

18 PATRIOT Act of 2001(P.L. 107-56), (Sec. 1016e)

delse för samhällets säkerhet och beredskap. Här följer några exempel, ur ett svensk perspektiv, på för samhället viktiga verksamheter som är beroende av de system och anläggningar som utgör infrastrukturen:

- Telekommunikationer
- Datakommunikation
- Elförsörjning
- Försörjning av bränsle och drivmedel
- Vattenförsörjning, avlopp och fjärrvärme
- Transporter och distribution
- Polis, räddningstjänst, sjukvård och alarmering
- Finansiella tjänster
- Viktiga myndighetstjänster som exempelvis förvaltning och ledning

Hot mot infrastrukturen

Kritisk eller samhällsviktig infrastruktur är utsatt för väderhändelser (extremvindar och extrem nederbörd). Risken för erosion, skred och ras ökar med intensivare nederbörd och 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 en säker eltillgång.

Relativt resurssvaga ickestatliga grupper kan med hjälp av kunskap, olika former av okonventionellt agerande och med stöd av gränsöverskridande logistiska och ideologiska nätverk orsaka allvarliga skador på viktiga infrastruktursystem. 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.

Terrorattentaten i exempelvis Madrid 2004 och i London 2005 har på ett påtagligt sätt åskådliggjort infrastrukturens sårbarhet. Vid terrorattacken mot World Trade Center 11/9 2001 slogs stora delar av mobiltelefonnätet ut, då två basstationer för mobiltelefoni fanns placerade på ett av de två WTC-tornen, dessutom slogs elförsörjningen på nedre Manhattan ut.

Terrorism, naturhändelser, stora olyckor eller mänskligt felhandlande är de absolut vanligaste orsakerna till olika störningar i infrastrukturerna. Exempelvis har riklig nederbörd i flera fall inneburit att mark, vattendrag och sjöar blivit så mättande att dammar och kraftverk hotats. Ett annat exempel är de senaste årens störningar i det europeiska elförsörjningssystemet berott på att det inte är dimensionerat för de stormstyrkor som nu förekommer relativt frekvent i Europa.

Det är viktigt att betona att det som betraktas som kritisk infrastruktur är flexibelt och därmed kan förändras över tid. Uppfattningen om hur hot- och risklandskapet ser ut påverkar vad som

räknas till kritisk eller samhällsviktig infrastruktur. Ett exempel på detta är att efter terrorangreppen den 11 september 2001 expanderade antalet infrastrukturområden i USA kraftigt, vilket var en följd av att infrastrukturbegreppet gavs en vidare innebörd.

Att skydda den kritiska infrastrukturen handlar om att prioritera. Konsekvensen blir då att den som försöker skydda allt, mest troligt skyddar ingenting. Med andra ord måste arbetet med CIP-frågorna bottna i en uppdaterad bild av hot- och riskmiljön. Att försöka skydda allt är således inte möjligt utan en sådan ambition motverkar i stället möjligheterna att skydda det som är det viktigaste.

Vidare har det ökande beroendet av dels de tjänster som är beroende av de tekniska infrastrukturerna, dels de tekniska infrastrukturernas inbördes beroenden (interdependens), gjort vårt samhälle mer sårbart. Exempelvis kan tekniska kollapser, mänskliga felhandlingar, sabotage eller extrema väderförhållanden leda till svåra och långvariga störningar som fortplantar sig i mycket stora delar av exempelvis transport- och elförsörjningssystemen.

Den viktigaste slutsatsen är att de som ska skydda vårt samhälle mot allvarliga kriser eller kunna agera vid allvarliga kriser blir mer och mer beroende av fungerande samhällsviktiga infrastrukturer. Infrastrukturerna, tjänsterna och marknaderna konvergerar. Samhällets säkerhet och krisberedskap bygger mer och mer på fungerande infrastrukturer och oömma system här och nu. Men det kanske för närvarande största problemet rörande sårbarheten i dessa system är den bristande medvetenheten om de hot, såväl manifesta som latenta, som systemen är utsatta för, samt vilka konsekvenser eventuella angrepp kan få.

Informationssäkerhets-relaterade hot och risker

KBM har ett särskilt uppdrag inom samhällets informationssäkerhet. Detta uppdrag omfattar ett sektorsansvar som bitvis är annorlunda än KBM:s andra uppdrag. Det nationella informationssäkerhetsarbetet bör dock till följd av sin komplexitet betraktas och hanteras som ett separat kompetensområde där olika hot, risker, sårbarheter och skyddsfrågor beskrivs.

Oavsiktliga hot i form av olyckor, extremt väder, tekniska fel och felaktig hantering bedöms för närvarande utgöra den största källan till avbrott och andra störningar i våra informationssystem. För att allvarliga störningar ska uppstå fordras ofta att flera funktioner, system eller fysiska anläggningar drabbas samtidigt. Eftersom oavsiktliga hot till sin natur ofta är slumpmässiga och därför sällan realiseras samtidigt eller samordnat, är de relativt lätta att skydda sig emot.

Det är ur skyddshänseende viktigt att påpeka att många säkerhetsåtgärder, såsom förberedande verksamhet, redundanta system och ledningsförmåga i krislägen, skyddar mot såväl antagonistiska som icke-antagonistiska hot. Generellt är individers säkerhetsmedvetande och agerande en viktigare säkerhetsmekanism än tekniska skyddsåtgärder.

Spridningen av skadlig kod som exempelvis virus, maskar och trojaner bedöms utgöra en allt större risk av flera anledningar. För det första tenderar den skadliga koden generellt att spridas snabbare och bli mer avancerad och aggressiv till sin karaktär. För det andra blir allt fler verksamheter beroende av Internet samtidigt som allt fler tekniska system och infrastrukturer bygger på IP-teknik (Internetprotokoll), t.ex. IP-telefoni, och därmed riskerar att bli exponerade för skadlig kod. Detta visar sig genom att fysiska verksamheter påverkas i högre utsträckning än tidigare vid spridning av skadlig kod. Ett färskt exempel är en incident i USA i augusti i år då en virus-attack slog ut ett av den amerikanska tullens och gränskontrollens IT-system, vilket förorsakade omfattande köbildningar och förseningar i flygtrafiken i flera amerikanska storstäder.

En risk som särskilt har uppmärksammats på senare tid i detta samman-

hang är styr- och reglersystem, eller så kallade SCADA-system (Supervisory Control and Data Acquisition), som utgör en viktig förutsättning för funktionaliteten i samhällsviktig infrastruktur. Dessa system har tidigare varit åtskilda från andra nätverk men tenderar nu allt oftare att kopplas samman och dessutom använda sig av Internet som bärare av informationen. Detta gör att SCADA-systemen exponeras för de hot som Internet för med sig, såsom skadlig kod och riktade angrepp.

I resultaten från en svensk undersökning av svenska myndigheter och statliga bolag framgår det att det endast är ett fåtal myndigheter och statliga bolag som helt har undgått att bli drabbade av skadlig kod. Emellertid är det hittills främst de administrativa stödsystemen och inte kärnverksamheterna som har drabbats. Skadorna har därför främst drabbat den egna organisationen och de externa konsekvenserna är av mer indirekt karaktär.

Trots att det sker en ständig utveckling av ny skadlig kod och modifiering av redan känd skadlig kod har den tidigare ökningen av omfattande virus- och maskspridningar mattats av under det senaste året. Däremot är den skadliga koden i dag ofta mer avancerad och specificerad för särskilda syften och användningsområden.

En form av skadlig kod som ökar i omfattning är så kallad spionprogramvara (spyware) som utan slutanvändarens vetskap placeras i dennes dator. Det finns uppgifter om att upp till 80 procent av alla datorer är infekterade av spionprogramvara och att varje dator i genomsnitt är infekterad av 25 olika typer av spionprogram. Flera säkerhetsorganisationer räknar även in relativt harmlösa cookies som spionprogram, varför statistik av detta slag ska betraktas med en viss försiktighet. Det råder dock inga tvivel om att spionprogram utgör en ökande risk.

I dag är den största delen av spionprogrammen riktade mot privatpersoner och syftar bl.a. till att stjäla bank- och kontokortsinformation. Det föreligger dock potentiella risker även för organisationer och för samhället, eftersom spionprogram även kan användas för att utöva företagsspionerі och underrättelseoperationer. I dag bedömer två tredjedelar av de IT-ansvariga inom svensk förvaltning att spionprogram utgör ett större hot än virusattacker.

Spridningen av skadlig kod sker fortfarande i hög utsträckning genom e-post och från dator till dator. En generell trend är dock att webbsidor i allt högre utsträckning används för spridning. Enligt ett säkerhetsföretag görs bedömningen att det i dag finns omkring 300 000 webbsidor på Internet som sprider spionprogramvara, vilket är fyra gånger så många som i början av året. Ett vanligt hjälpmedel för spridning av skadlig kod är så kallade botnets.

Bot (förkortning för robot) är en form av skadlig kod som installeras i en dator, oftast utan att ägaren märker det, vilken möjliggör för någon annan att fjärrstyra datorn. Den stora faran

utgörs av att de infekterade datorerna, som kan finnas på olika ställen i världen, bildar nätverk som kan fjärrstyras synkroniserat för olika mål och syften. Dessa nätverk av bots kallas botnets. Den samlade datorkraft som ett botnet kan generera kan antingen fokuseras och riktas mot ett specifikt utvalt mål, eller användas för att på kort tid uppnå en mycket stor spridningseffekt på Internet. Den spridningseffekt som botnets kan generera används bl.a. för phishing, spridning av spam, avlyssning av trafik, spridning av skadlig kod som exempelvis spionprogram eller nya bots samt massinformationsstöld. Exempel på riktade attacker är så kallade DDoS-attacker (Distributed Denial of Service), se mer i nästa avsnitt om riktade attacker.

I likhet med andra typer av skadlig kod sprids bots genom bl.a. e-post och webbsidor och utnyttjar oftast kända sårbarheter i Windows operativsystem. Vanligtvis är det slutanvändares datorer med bredbandsuppkoppling och bristande säkerhet som infekteras av bots. Styrningen av och kommunikationen i botnets sker vanligtvis genom Internet Relay Chat (IRC). Ett botnet kan innehålla hundratusentals bots och ju fler bots desto större datorkraft kan genereras. Det finns dock indikationer på att mindre botnets börjar användas i större omfattning. Orsakerna är sannolikt att de är svårare att upptäcka än stora botnets.

Det ska nämnas att botnets i sig inte möjliggör nya typer av hot utan är ett verktyg som gör att attacker får större effekt än tidigare. Den totala omfattningen av botnets och deras konsekvenser är inte kända men det råder stor enighet bland experter om att botnets utgör ett allvarligt och ökande problem, såväl internationellt som i Sverige. Detta understryks av att flera länders brottsbekämpande myndigheter, exempelvis i USA och Storbritannien, har gett botnetbekämpningen mycket hög prioritet.

Spam eller så kallad skräppost, som är ett vanligt användningsområde för botnets, innebär att det sker ett massutskick av oönskad e-post, ofta med kommersiellt budskap och utan mottagarens samtycke. Spam har under flera år ökat lavinartat och medför sammantaget stora kostnader för samhället i form av spamhantering och nätverkskapacitet som tas i anspråk. På senare tid har dock ökningen av spam mattats av och andelen e-postmeddelanden som utgörs av spam har minskat från 85 procent till 63 procent under 2005. Majoriteten av all spam sprids genom botnets.

Till skillnad från spam fortsätter fenomenet phishing mot finansiella institutioner och deras kunder att öka mycket kraftigt. Det senaste större försöket var riktat emot Nordea i början av oktober i år.

Phishing är en metod som går ut på att lura mottagaren att lämna ifrån sig konfidentiell finansiell information genom att antingen svara på ett falskt e-postmeddelande eller besöka en falsk webbsida. Under sommaren har antalet phishing-attacker ökat med 16 procent

per månad. Svenska organisationer som har drabbats är bl.a. Eurocard (i november 2004) och Handelsbanken (i juli 2005). Begreppet phishing inbegriper dock ett bredare användningsområde än enbart attacker mot finansiella institutioner. Ett annat exempel på phishing är ett antal e-postmeddelanden som spreds strax efter orkanen Katrina i södra USA. Meddelandena innehöll länkar som uppgavs leda till information om katastrofen eller insamlingar till offren, men som i själva verket spred skadlig kod.

Botnets används också för att sprida olika typer av avlyssningsprogram för informationsstöld. Det finns emellertid få uppgifter om omfattningen av detta fenomen, bl.a. på grund av att den typen av attacker ofta sker i det fördolda. De mest uppmärksammade användningsområdena är identitetsstöld, något som betecknas som mycket omfattande i USA. Andra användningsområden för botnets som nämns i öppna källor är övervakning av datortrafik och lagring av barnpornografi och annat olagligt material.

Riktade angrepp avser angrepp som är riktade mot ett specifikt och utvalt mål, t.ex. en enskild organisation eller en enskild dator. Till skillnad från spridning av skadlig kod ökar de riktade attackerna i omfattning. Ofta rör sig riktade attacker om företagsspionerі och underrättelseoperationer. Ett exempel är ett omfattande fall av företagsspionerі i Israel som för närvarande utreds och hittills har lett till ett tjugotal arresteringar. Attackerna har genomförts av privata utredningsbolag som har arbetat för ett flertal ledande företag i Israel. Spionprogrammen har installerats på de drabbade företagens datorer genom trojaner som har skickats via e-post. En annan metod som användes var att sprida trojanerna genom disketter som skickades till företagen med information om anbud och affärsförslag.

Även om en organisations tekniska IT-säkerhet är god kan riktade angrepp genomföras genom så kallad social engineering, vilket innebär att människor, snarare än datorer, manipuleras och luras till att lämna ifrån sig känslig information. Exempelvis kan phishing utnyttjas för att lura in personal på förfalskade eller så kallade spoofade webbsidor i syfte att lämna känslig information, t.ex. lösenord.

En annan form av riktad attack som till stor del utförs med hjälp av botnets är DDoS-attacker (Distributed Denial of Service) som överbelastar ett nätverk med information. Omfattningen av DDoS-attacker mot svenska organisationer är inte känd men en undersökning i Storbritannien visar att hela 14 procent av det brittiska näringslivet drabbades av DDoS-attacker under 2004. DDoS-attacker medför inte sällan att hela eller delar av den drabbade organisationens verksamhet blockeras från Internet. De ekonomiska förlusterna för företag som är beroende av onlineverksamhet kan bli katastrofala och det har förekommit att företag har gått i konkurs till följd av DDoS-attacker. För organisationer som levererar eller handhar samhällsviktig

verksamhet, t.ex. SCADA-system, via Internet är de externa riskerna kring DDoS-attacker påtagliga.

Ett allt vanligare fenomen är att DDoS-attacker sker i kombination med utpressning. Under 2004 utsattes 50 brittiska företag för den typen av attack. Ett exempel är det brittiska betalningsföretaget Nochex som i augusti 2004 fick ett e-postmeddelande med följande text:

> ”If you want save your business, you should pay 10.000$ bank wire to our bank account. When we receive money, we stop attack immediately. If we will not receive money, we will attack your business 1 month, and destroy your router and DNS? think about how much money you lose while your servers are down.”

Tio minuter senare genomfördes en DDoS-attack mot företagets Internetserver med 155 Mbit/sekund. Företaget normala inkommande trafik låg på omkring 7–8 Mbit/sekund och Nochex webbserver slogs ut direkt.

Inte sällan ligger även politiska ställningstaganden eller åtminstone politiska förtecken bakom DDoS-attacker. Så var fallet när holländska myndigheter drabbades av omfattande DDoS-attacker under 2004, vilket beskrevs i förra årets hot- och riskrapport. Det är också mycket vanligt att hackare i länder som är involverade i internationella konflikter utsätter motståndarlandets myndigheter och företag för DDoS-attacker. Fenomenet har bl.a. uppmärksammats vid konflikterna Israel–Palestina, Indien–Pakistan och USA–Kina.

Det finns även exempel på att DDoS-attacker används i näringslivet för att slå ut konkurrenter. I Massachusetts i USA är VD:n för bolaget Orbit Communication Corp (återförsäljare av satellit-TV) misstänkt för att ha hyrt flera botnets som användes för att sänka tre konkurrenter på Internet. Attackerna resulterade i att de konkurrerande företagen låg nere under långa tidsperioder, vilket förorsakade ekonomiska förluster på två miljoner dollar för de drabbade företagen och deras Internetleverantörer.

En uppmärksammad DDoS-attack i Sverige skedde i slutet av 2004 mot Datainspektionen. Sammanlagt var hundratusentals datorer involverade i attacken. De flesta av de attackerande datorerna var ADSL-anslutna hemdatorer i Östeuropa och Asien. Endast ett fåtal svenska datorer var involverade. Förutom det stora antalet attackerande datorer karaktäriserades denna attack av att angriparen ständigt bytte angreppssätt i takt med att man vidtog skyddsåtgärder. Flera tjänster låg nere till följd av attacken men Datainspektionens onlineverksamhet blev inte helt blockerad. Orsaken till denna attack är okänd men den är att betrakta som allvarlig då den drabbade en statlig myndighets kärnverksamhet under lång tid. Attacken visar på de sårbarheter i samhället som kan komma att uppstå i samband med utbyggnaden av 24-timmarsmyndigheten.

En generell trend är att aktörsbilden bakom vardagliga attacker håller på att förändras och bli mer professionaliserad och kriminaliserad. För några år sedan bestod majoriteten av attackerna av okynneshackning som genomfördes av så kallade ”script kiddies”. I dag bedöms majoriteten av attackerna vara mer målinriktade och genomförs i specifika syften, inte minst på grund av att kriminella individer och organisationer i allt högre utsträckning begår brott via Internet.

En annan trend är att olika aktörer samverkar i högre utsträckning och att det är olika aktörer som utvecklar, modifierar respektive använder skadlig kod. Mycket pekar på att det förekommer en marknad för skadlig kod, vilket gör att enskilda aktörer inte själva behöver ha den tekniska förmågan att utveckla kod för att utföra attacker. Detta gör att hoten ut ett aktörsperspektiv är mycket komplexa och snabbt föränderliga. Handel med skadlig kod har särskilt uppmärksammats när det gäller botnets. Det finns uppgifter om att man får betala mellan 500 och 1 500 dollar att för att få en DDoS-attack genomförd genom botnets eller att man för 100 dollar kan hyra ett botnet för att sprida spam eller utföra phishingattacker. Riskerna med denna utveckling är inte bara kopplade till att fler aktörer får tillgång till attackverktyg, utan även till att det börjar ställas högre krav på funktionalitet och att mer avancerade verktyg för att bl.a. minska möjligheterna att detektera och spåra attacker kommer ut på marknaden.

Vissa stater och statsunderstödda organisationer bedöms fortfarande utgöra den mest avancerade aktörskategorin, både teknisk och operativt. Detta är ett resultat av att många stater utvecklar förmågan att bedriva militära informationsoperationer (IO); en förmåga som även kan tillämpas för civila ändamål. Staters överlägsna förmåga har också att göra med tillgången till stödresurser, exempelvis underrättelsetjänst och stora möjligheter att värva insiders. Insiders utgör generellt ett stort hot mot enskilda organisationer, oavsett om de verkar för egen räkning eller är rekryterade av en utomstående aktör. Då insiders ofta har behörighet till information är det svårt att vidta förberedande tekniska säkerhetsåtgärder mot insiders.

Det största hotet när det gäller statsaktörer utgörs i fredstid av underrättelseoperationer. Områden som är av särskilt intresse är spetskompetensen – bl.a. forskning och utveckling inom telekommunikation, medicin- och försvarsindustri – och det politiska fältet med Sveriges politiska agerande och ställningstagande i internationella frågor. Det förekommer att andra stater utifrån eller med stöd av värvade insiders bedriver underrättelseoperationer genom dataintrång, men då denna verksamhet sker i det fördolda är det svårt att få en bild av den totala omfattningen.

En annan risk som den enskilda organisationen bör beakta har att göra med vilken information som ligger öppet på den externa webbsidan.

Det blir exempelvis allt vanligare att det läggs ut kontaktinformation om de anställda. Denna service bör vägas mot ökade möjligheter för antagonistiska aktörer att värva insiders och bedriva social engineering. Innehållet på webbsidor kan också användas i olika typer av underrättelseoperationer. En uppmärksammad empirisk studie från Försvarshögskolan påvisar hur lätt det är för exempelvis terroristorganisationer att inhämta underrättelser genom öppna källor på Internet i syfte att planera för konventionella fysiska attacker[19]. Studien visar att det är möjligt att få relativt detaljerad information kring ett antal kritiska infrastrukturer i Stockholm, information om vad målen består av och var de fysiskt är belägna, sårbarheter, bevakning samt om nyckelpersoner.

19 ”CNI – en metod för terroristernas underrättelsetjänst?” Krohné, C-uppsats Försvarshögskolan 2005

Bilaga 1.
Förslag till fördjupad läsning

Kampen om hotbilden, Johan Eriksson – Santérus Förlag 2004
Globalised Islam, Olivier Roy – Hurst & Company 2004
Förvarning och samhällshot, Wilhelm Agrell – Studentlitteratur 2005
Beredskap mot skadlig kod – KBM:s temaserie 2005
KBM:s lägesbedömning av samhällets informationssäkerhet 2005 (pdf)
International CIIP Handbook 2004 – CRN/ETH Zurich
Säkerhetspolisens öppna verksamhetsberättelse 2003 (pdf)
Ett säkert Europa I en bättre värld – EU:s säkerhetsstrategi 2004 (pdf)
Interim National Infrastructure Protection Plan – Department of Homeland Security (pdf)

KBM:S TEMASERIE

2005:11 Hot- och riskrapport 2005

2005:10 Medborgare om våldsdåd
Reaktioner efter mordet på Anna Lindh och andra dåd

2005:9 Samverkan i organisation eller nätverk?
Fallen elektroniska affärer och elberedskap

2005:8 Mind the gap!
Hur bygger vi broar mellan stat och näringsliv i arbetet med krisberedskap?

2005:7 Samverkan mellan offentlig sektor och näringslivet vid krishantering
En studie av kriser i Sverige 1993–2003

2005:6 Hot på agendan
En analys av nyhetsförmedling om risker och kriser

2005:5 Förtroendekriser
Kommunikationsstrategier före, under och efter

2005:4 Efter flodvågskatastrofen
Svenska folkets åsikter om och förtroende för myndigheter, medier och politiker

2005:3 Propagandakriget i backspegeln
En studie i påverkansförsök och svenska nyhetsmedier

2005:2 Allmänheten medverkar vid övningar
Erfarenheter från Övning Havsörn

2005:1 Beredskap mot skadlig kod
En kartläggning av IT- och informationssäkerheten inom större myndigheter och statliga bolag i Sverige med fördjupad analys av skadlig kod

2004:6 Hot- och riskrapport 2004
Gränsöverskridande sårbarheter

2004:5 "We're a peaceful nation"
Krigsretorik efter 11 september

2004:4 Ministermordet
En studie om myndigheternas kommunikation vid attentatet mot Anna Lindh

2004:3 Säkerhet och beredskap i Europeiska unionen

2004:2 Stereotyper i vardagen
Bilder av "de främmande"

2004:1 Krisjournalistik eller journalistik i kris?
En forskningsöversikt om medier, risker och kriser

SPECIAL FEATURE

2004:5 "We're a peaceful nation"
War Rhetoric after September 11

Hot- och riskrapport 2005

Detta är Krisberedskapsmyndighetens (KBM) andra årliga Hot- och riskrapport. Rapporten vänder sig i första hand till er som på lokal, regional och central nivå arbetar med uppgifter inom krishanteringssystemet. Målsättningen är att Hot- och riskrapporten ska utgöra ett värdefullt underlag för arbetet med olika strategiska processer, exempelvis risk och sårbarhetsanalyser, och planeringsprocessen. Ambitionen är också att rapporten ska vara ett bidrag till det arbete som bedrivs utanför den offentliga samhällssektorn, i näringsliv och frivilligorganisationer.

Under 2004 har händelser både i omvärlden och inom Sverige – som flodvågskatastrofen i Asien och stormen Gudrun – visat på vilka förödande konsekvenser som uppstår då hot och risker möter de olika sårbarheter som finns i vårt samhälle. Dessa tragiska erfarenheter visar tydligt att svensk krisberedskap fortsatt står inför stora utmaningar.

Mot bakgrund av den föränderliga och svårtolkade hot- och riskmiljön vill KBM ge läsaren en övergripande bild av de hot och risker vårt samhälle står inför. En viktig beståndsdel i arbetet för en fungerande och effektiv krisberedskap är en flexibel inställning till hela hot- och riskmiljön. Att kunna hantera det oväntade är en förutsättning för en lyckosam krishantering. Detta ställer samtidigt krav på förmåga till framåtblickande och öppenhet i bedömningen av hot- och risker. En framgångsrik hot- och riskbedömning utgår från ett helhetsperspektiv. Alltför snäva analysperspektiv kan få negativa konsekvenser.

Exempelvis går det därför inte längre att skilja på den inre och yttre säkerheten, svensk krisberedskap är numera en del av den internationella säkerhetsmiljön. Smitta, orkaner, översvämningar, tekniska fel, organiserad brottslighet och internationell terrorism stoppas inte av nationsgränser.

Krisberedskapsmyndigheten

Box 599
101 31 Stockholm

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

kbm@krisberedskaps
myndigheten.se

www.krisberedskaps
myndigheten.se

ISSN 1652-2915
ISBN 91-85053-89-9