fokus Samhällssäkerhet

FOI och arbetet med samhällets säkerhet och trygghet

FOI-R--3684--SE

JUNI 2013

FOI

fokus Samhällssäkerhet

FOI och arbetet med samhällets säkerhet och trygghet

Georg Fischer, Per Larsson, Lotta Ryghammar, Carolina Sandö (red.)

Juni 2013

FOI-R--3684--SE

Titel	fokus Samhällssäkerhet FOI och arbetet med samhällets säkerhet och trygghet
Rapportnr/Report no	FOI-R--3684--SE
Månad/Month	Juni/June
Utgivningsår/Year	2013
Antal sidor/Pages	158 p
ISSN	1650-1942
Projektnr/Project no	I181605
Godkänd av/Approved by	Maria Lignell Jakobsson
Ansvarig avdelning	Försvarsanalys

Förord

Du håller nu i den första utgåvan av *fokus Samhällssäkerhet* som ges ut av Totalförsvarets forskningsinstitut, FOI. Med denna skrift vill jag och mina medarbetare visa upp exempel från den breda verksamhet FOI bedriver inom området samhällets säkerhet och trygghet. Vi hoppas skriften kan bidra till samhällsdebatten och lyfta några av de frågor som vi arbetar med för att stärka samhällets säkerhet och trygghet.

FOI har sina rötter i försvarsforskning för det militära och det civila försvaret där militärt angrepp var det dominerande hotet. Samhällets syn på hot och risker förändrades och vidgades efter det kalla krigets slut och för att möta denna förändring vidgades FOI:s uppgifter. Nu är FOI en kompetens för Sveriges alla krisberedskapsaktörer och vi skapar nytta åt hela samhället genom vår forskning.

Vi vill att du med denna skrift ska få en känsla för de många olika typer av arbeten som bedrivs på FOI och att det är en mängd forskare inom vitt skilda områden som verkar för att göra samhället tryggare och säkrare. En del forskare arbetar på en övergripande nivå genom att till exempel analysera hot och risker, andra är mer specialiserade och utför experiment i syfte att förhindra att människor skadas vid olyckor och katastrofer. Vi hoppas att denna skrift bidrar till den ständigt pågående kunskapsuppbyggnaden och att du kommer få en djupare insikt om några av de utmaningar som samhället står inför!

Avslutningsvis vill jag tacka alla som på olika sätt har bidragit till *fokus Samhällssäkerhet*; författarna, redaktionen som bestått av Georg Fischer, Per Larsson, Lotta Ryghammar och Carolina Sandö (projektledare) samt Heidi Askenlöv som förtjänstfullt bistått med redigering av skriften.

Jan-Olof Lind

Generaldirektör

Totalförsvarets forskningsinstitut

Innehållsförteckning

Inledning

Samhällssäkerhet handlar enligt riksdagens och regeringens målsättningar om att värna befolkningens liv och hälsa, värna samhällets funktionalitet och värna vår förmåga att upprätthålla våra grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter.

Arbetet med samhällssäkerhet sker på en mängd olika nivåer och inom olika sektorer och sakområden i samhället och med olika tidsperspektiv. Det omfattar allt ifrån långsiktig kunskapsuppbyggande forskning till direkta och konkreta åtgärder i vardagslivet. Och det är en viktig verksamhet som berör oss alla; myndigheter, företag och individer, och det berör i högsta grad politiska beslutsfattare och journalister som har att bevaka samhällsutvecklingen och den politiska makten. Ytterst berör samhällssäkerheten givetvis oss alla som samhällsmedborgare, det handlar om liv och hälsa för oss och våra nära och kära.

Säkerhetsarbete innebär att man ständigt skaffar sig kunskap om var säkerheten brister i samhället och vidtar de åtgärder som är nödvändiga för att värna det skyddsvärda. Det handlar om att identifiera vad som är skyddsvärt, vilka hot och sårbarheter som finns, vilka konsekvenser säkerhetsbrister kan leda till och vilka åtgärder som behöver vidtas. Säkerhetsarbete kan också handla om att ta fram metoder och verktyg som hjälper individer och organisationer att bättre förstå vilka risker de är utsatta för och hur de kan hantera sin situation.

Samhällssäkerhet är i många avseenden en färskvara. Eftersom samhället och vår omvärld ständigt förändras så måste säkerhetsarbetet kontinuerligt aktualiseras. Vetenskapliga framsteg, ny teknologi, globalisering, klimatförändringar och omställningar inom många andra områden skapar nya förutsättningar för samhällssäkerheten. Nya hot och sårbarheter uppstår, konsekvenserna av säkerhetsbrister kan ändra karaktär och omfattning och möjligheterna att vidta säkerhetshöjande åtgärder kan både förbättras och försämras. För att få veta vad som behöver göras för att värna det skyddsvärda och skapa trygghet i samhället behövs en dynamisk och framåtblickande kunskapsutveckling.

FOI bidrar sedan länge, såväl nationellt som internationellt, med kunskapsutveckling till stöd för samhällets säkerhet och trygghet. Det kan gälla:

- att *identifiera* hot och sårbarheter på olika nivåer i samhället,
- att *förebygga* allt från störningar och olyckor i vardagen till storskaliga kriser och katastrofer samt förberedelser för att på bästa sätt kunna hantera dessa om de inträffar,
- att *hantera* allt från störningar och olyckor i vardagen till storskaliga kriser och katastrofer när de väl inträffar,
- att *underlätta* en verksamhets *återgång* till ”vardagen” efter att störningar, olyckor, kriser eller katastrofer inträffat och

- att *inrikta, styra och följa upp* arbetet i det svenska krisberedskapssystemet, inklusive internationellt krisberedskapssamarbete, eller krisberedskaps-arbetet inom en enskild organisation.

Den här skriften fokuserar på hur FOI idag arbetar med att utveckla samhällets säkerhet och trygghet genom långsiktig kunskapsuppbyggnad och genom att direkt stödja olika samhällsaktörer i deras vardagsnära arbete med säkerhets- och trygghetsfrågor. I ett antal artiklar och intervjuer ges ett axplock av aktuella frågor kring samhällssäkerhet som FOI:s ca 850 forskare och analytiker kontinuerligt arbetar med gentemot uppdragsgivare såsom Regeringskansliet och Myndigheten för samhällsskydd och beredskap (MSB).

Artiklarna, som illustrerar den mångfacetterade karaktären i FOI:s verksamhet, behandlar vitt skilda områden som dock alla utgör *en* del av samhällets sammantagna säkerhet och trygghet. De speglar på detta sätt komplexiteten vad gäller samhällssäkerhet som omfattar allt från tekniska detaljer till strategiska frågeställningar. Vidare framkommer FOI:s roll som aktör i processer som gäller såväl enskilda svenska myndigheter som Europeiska unionen (EU). Det finns säkerhetsarbete, som eftersom Sverige och övriga medlemsstater inte själva kan hantera det, måste ske i en europeisk kontext.

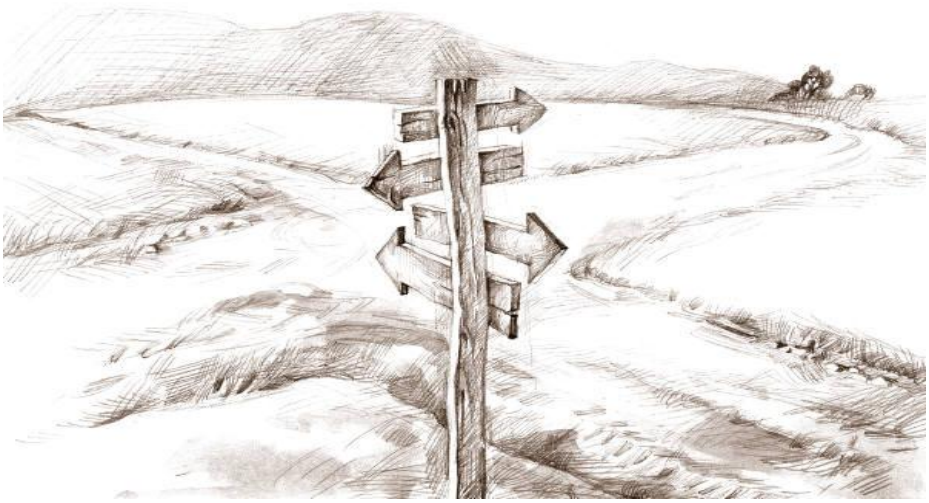
Efter en inramning till skriften med en beskrivning av krisberedskapssystemets utveckling följer ett antal artiklar kring hot och risker; vilka de är, metoder för att identifiera dem, en nationell bedömning och utmaningar för samhällets riskbedömning. Vidare behandlas problem och möjligheter kopplat till informationstekniken; IT-angrepp, informationsmöjligheter och att genom digitala spår upptäcka individer som planerar en massaker i skolmiljö. Tekniken leder oss vidare till system för övervakning och trygghet, system med ambitionen att tillhandahålla inte bara säkerhet, utan också personlig integritet. Farliga ämnen kan beskrivas utifrån en rad olika aspekter. I detta axplock behandlas behovet av bättre krisberedskap, hantering av farligt avfall, biomarkörer för att snabbt identifiera kemisk lungskada och hemmagjorda bomber. En fungerande transportsektor är en nödvändighet i samhället. Hur kan man analysera, upptäcka och åtgärda hot mot den? Idag har vidare samhällets moderna citykärnor mängder av glasade fasader – vackert – men vad händer när de utsätts för tryckvågor till exempel i samband med ett terrordåd? Dock, när det väl händer något – hur reagerar vi människor då? Och – hur kan organisationer förbereda sig på det som komma kan – öva, öva och öva.

I intervjuerna får vi veta mer om det civila försvaret, EU:s betydelse för svensk krisberedskap, simuleringsstöd för samhällssäkerhet, EU:s handlingsplan för bättre sprängämnessäkerhet och nordisk krisberedskap.

Välkommen att botanisera bland denna skrifts artiklar om samhällets säkerhet och trygghet!

1 Från civilt försvar till kontraktsbaserad samhällssäkerhet

Per Larsson och Lotta Ryghammar



Sverige har sedan 2002 ett nationellt krisberedskapssystem för att förebygga och hantera olika samhälleliga hot och risker. Efter 10 år har ett system tagit form – men hur? Hur har systemet påverkats inifrån och hur har det påverkats utifrån av den allmänna samhällsutvecklingen? Som en reflektion över det svenska krisberedskapssystemets utveckling beskriver den här artikeln i korthet systemets framväxt, utvecklingstendenser samt några strukturella förutsättningar som den fortsatta utvecklingen av samhällets krisberedskap har att beakta. Artikelförfattarna har under en lång tid följt utvecklingen av svensk krisberedskap, inte minst i sitt arbete med att stödja Försvarsdepartmentet i dess uppgift med att inrikta och samordna den nationella krisberedskapen.

Den svenska krisberedskapens utveckling

Kriget – civilt försvar

Enkelt uttryck kan det nu existerande svenska krisberedskapssystemet sägas ha rötterna i dels arbetet med skydd mot vardagliga olyckor, dels i totalförsvarets

beredskap i händelse av ett militärt angrepp mot Sverige under det kalla kriget (1945-1991). För det sistnämnda rörde det sig bland annat om förekomsten av ett civilt försvar med välutvecklade samverkansstrukturer på olika samhällsnivåer (lokal, regional och central) med det militära försvaret, gemensamma civila och militära ledningsplatser på högre samhällsnivåer (regional och central), omfattande statliga beredskapslager (till exempel insatsvaror för industrin), utpekade myndigheter med så kallat funktionsansvar för en specifik samhällssektor och resursstarka försvarsenheter på länsstyrelserna som var högsta civila totalförsvarsmyndighet på länsnivå.

En huvuduppgift för det civila försvaret vid höjd beredskap och krig var att stödja det militära försvaret i dess uppgift att försvara landet. Nationell förvaltningsmyndighet för inriktning och samordning av det civila försvaret var från 1986 och fram till 2002 Överstyrelsen för civil beredskap (ÖCB). Fram till slutet av 1990-talet existerade inte krisberedskap som en från statens sida uttalad samhällsföreteelse och därmed inte heller som ett specifikt politik- och budgetområde i statsbudgeten.

Förmågan att hantera eventuella storskaliga olyckor eller samhälleliga kriser i fredstid förväntades bygga på vardagens resurser och organisation med stöd av det civila försvarets resurser och kompetenser. Detta skedde utan att fullt ut beakta problemet att bruket av det civila försvarets resurser och kompetenser i stor utsträckning, legalt och organisatoriskt, var knutet till höjd beredskap och krig. Under den senare delen av 1990-talet kom därför ÖCB att på olika sätt försöka att ”arbeta runt” olika legala och organisatoriska hinder för att stärka förmågan att hantera fredstida samhälleliga kriser, vilket ansågs i växande grad påkallat mot bakgrund av till exempel Tjernobyl- och Estoniakatastroferna. Samtidigt talade man alltmer i termer av ” fredstida krisberedskap” och allt mindre om ”höjd beredskap och krig”, eftersom slutet på kalla kriget var ett faktum och en militär invasion av Sveriges inte längre bedömdes som sannolik under en överskådlig framtid.

Vid mitten av 1990-talet hade den av regeringen tillsatta *Hot- och riskutredningen* i sitt slutbetänkande *Ett säkrare samhälle* också redovisat en bredare hotbild än den traditionella militära hotbilden mot landet. Enligt utredningen stod Sverige inför ett brett spektrum av risker vid sidan av de rent militära såsom massflykt, terrorism, sabotage, internationell kriminalitet, miljökatastrofer och kärnenergiolyckor. Mot bakgrunden ovan pågick under 1990-talet också en diffus process som ledde till att det tidigare arbetet med civilt försvar avstannade för att mer eller mindre helt upphöra i samband med att ÖCB lades ned i december 2001 och det militära försvaret ominriktades från ett invasionsförsvar till ett insatsförsvar. I praktiken innebar det att beredskapslagren tömdes, funktioner som civilbefälhavare och funktionsansvariga myndigheter avskaffas med mera. En civilförsvarsepok avslutades och en krisberedskapsepok påbörjades.

Scanpix: Maria Stéen

Den fredstida krisen – krisberedskap

Den av regeringen tillsatta *Sårbarhets- och säkerhetsutredningen* presenterade 2001 en utredning som tydligt betonade vikten av ett vidgat säkerhetsbegrepp som inkluderade svåra påfrestningar på samhället i fredstid, det vill säga olika former av fredstida kriser. Sårbarhets- och säkerhetsutredningens förslag behandlades i regeringens proposition *Samhällets säkerhet och beredskap* (prop. 2001/2002:158). Som ett resultat av propositionen ersattes Överstyrelsen för civil beredskap (ÖCB) vid årsskiftet 2001-2002 av Krisberedskapsmyndigheten (KBM). Den nya myndighetens roll och befogenheter begränsades i huvudsak till att inrikta, samordna och stödja krisberedskapsarbetet i samhället.

Framförallt medförde dock propositionen att grunderna till dagens nationella krisberedskapssystem etablerades via en rad legala, organisatoriska, ledningsmässiga samt finansiella strukturer och principer. Dessa strukturer och principer har sedan 2002 fram till dags datum policymässigt utvecklats och justerats i varierande utsträckning. Idag kan krisberedskapssystemet policymässigt sägas vara fastlagt och uppbyggt kring ett antal mål, strukturer och principer. Dessa finns emellertid inte samlade och tydligt uttryckta i någon officiell ”krisberedskapsdoktrin”, ett särskilt dokument, utan är spridda över tid i olika styrdokument såsom propositioner, skrivelser, utbildningsmaterial med mera. De mest grundläggande av dessa mål, strukturer och principer kan dock sägas vara följande:

För det första, målen med krisberedskapen vilar ytterst på målen med samhällets säkerhet. De är ”att värna befolkningens liv och hälsa, värna samhällets funktionalitet och värna vår förmåga att upprätthålla våra grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter” (prop. 2008/09:140, bet. 2008/09: FöU10, rskr. 2008/09:292). Utifrån dessa har de specifika målen för samhällets krisberedskap formulerats som att ”minska risken för och konsekvenserna av allvarliga störningar, kriser och olyckor. Skulle en sådan händelse inträffa bör kvinnors, mäns och barns liv, personliga säkerhet och hälsa tryggas samt skador på egendom eller i miljö begränsas. Arbetet med samhällets krisberedskap bör även bidra till att minska lidande och skadeverkningar av allvarliga olyckor och katastrofer i andra länder genom bland annat bistånd och andra insatser” (budgetprop. 2012/13:1). Målen med samhällets krisberedskap handlar således både om att värna oss själva i Sverige och att i en anda av solidaritet bistå människor i andra länder vid kriser och katastrofer. Målen fokuserar vidare på allvarliga händelser högt upp på hotskalan. Genom separata lagstiftningar i form av Lag (2003:778) om skydd mot olyckor respektive Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap särskiljs legalt också arbetet med vardagliga och mer frekventa störningar i samhället från arbetet med särskilt allvarliga störningar i samhället.

För det andra, samhällets krisberedskap villar på *ansvarsprincipen*, *närhetsprincipen*, *likhetsprincipen* och *solidaritetsprincipen* (att bistå kris- och katastrofdrabbade länder i vår omvärld), ett geografiskt områdesansvar fördelat på nationell, regional och lokal nivå samt ett sektorsansvar fördelat på ett antal myndigheter med särskilt utpekat krisberedskapsansvar. Med det geografiska områdesanvaret och sektorsansvaret avses hela samhällslivet täckas in ansvarsmässigt ur ett krisberedskapsperspektiv. Med utgångspunkt i ansvarsprincipen och det geografiska områdesansvaret, utgörs samhällets krisberedskap inte av en särskild organisation utan av en verksamhet som omspänner hela samhället, innefattande den enskilde individen, privata företag, centrala myndigheter, länsstyrelser, landsting, kommuner, regeringen med flera inklusive offentliga organs relationer med omvärlden.

För det tredje, samhällets krisberedskap avses ha sin bas i den lokala nivån och dess 290 kommuner utifrån ansvars- och närhetsprincipen och utifrån det faktum att kommunerna har ett politiskt ansvar för viktiga funktioner för människor såsom dricksvatten, fjärrvärme, boende, sophämtning med mera. Samhällets krisberedskap ska med andra ord till stor del byggas nerifrån och upp.

För det fjärde, den grundläggande styrningsprincipen för alla de aktörer som bär upp samhällets krisberedskap är samverkan och samordning. Det fordras således att berörda aktörer proaktivt samverkar med varandra för att skapa en samordnad och effektiv krisberedskap. Mot bakgrund av att samhällets krisberedskap ska bygga på en hög grad av decentralisering och på samverkan, och inte på

hierarkisk ordergivning, mellan ett stort antal offentliga och privata aktörer finns inte någon krisledande myndighet för samhällets krishantering. Det finns heller ingen undantagslagstiftning av generell karaktär som existerar i ett flertal länder och som kan tillämpas vid allvarliga händelser.

För det femte, samhällets krisberedskap bygger på vardagens verksamhet och resurser. Vardagens resurser kan vid behov kompletteras med olika förstärkningsresurser från den nationella eller internationella arenan. Uppbyggda specifika förstärkningsresurser, till exempel för skogsbrandsbekämpning, på den nationella arenan är begränsade och i många fall strategiskt utplacerade i landet. En av samhället planerad och storskalig uppbyggnad samt lagerhållning av förstärkningsresurser sker inte.

Scanpix: Kristoffer Pettersson

För det sjätte, utifrån ansvarsprincipen ska varje krisberedskapsansvarig aktör som grundprincip på egen hand bekosta sitt krisberedskapsarbete. Statliga myndigheter ska göra det inom ramen för det egna myndighetsanslaget. Särskilda statliga anslag på krisberedskapsområdet är fokuserade på områden som faller mellan olika aktörers ansvar, särskilda punktinsatser och dylikt. Villkoren för beviljade anslag har blivit mer restriktiva under senare år. Staten har särskilda överenskommelser med kommuner och landsting som ger dem viss ekonomisk ersättning för fullföljande av den lagstiftning som reglerar deras krisberedskap.

För det sjunde, arbetet med samhällets krisberedskap utgår policymässigt från en före-under-efter-ansats med särskild betoning på det förebyggande krisberedskapsarbetet i före-fasen, inte minst med utgångspunkt i ett systematiskt

arbete med risk- och sårbarhetsanalyser (se artikel 3 och 4). Ett sådant arbete ska kontinuerligt genomföras på alla samhällsnivåer och inom alla viktiga samhällssektorer för att identifiera existerande och framtida hot och risker i samhället. Den lagstadgade skyldigheten att regelbundet genomföra risk- och sårbarhetsanalyser är dock förbehållen offentliga aktörer, inte privata aktörer även om de bedriver samhällsviktig verksamhet.

Trots den policymässiga utveckling som skett sedan inrättandet av krisberedskapssystemet 2002 är det ur implementeringssynpunkt fortfarande till delar ett omoget system. Implementeringen befinner sig fortfarande i en uppstartsfas, till exempel är kunskapen om systemet i många fall bristfällig bland ansvariga beslutsfattare och bland allmänheten, det privat-offentliga samarbetet är ofta otillräckligt och medan vissa kommuner har kommit långt i sitt krisberedskapsarbete har andra kommuner haft svårare att komma igång med sitt krisberedskapsarbete.

Det civila försvarets försvinnande och återkomst

Parallellt med ansträngningarna att inrätta och implementera krisberedskaps-systemet har frågor rörande civilt försvar samt höjd beredskap och krig kommit att ligga i träda hos i princip alla samhällsaktörer det senaste decenniet. Idén om att det civila försvaret under höjd beredskap och vid krig skulle stödja det militära försvaret kom i slutet av 1990-talet att ersättas av synsättet att det är det militära försvaret, det vill säga Försvarsmakten, som ska stödja samhället och dess beredskap vid kriser och katastrofer. Försvarsmaktens förmåga att stödja samhället med personella och materiella resurser har emellertid försvårats av det militära försvarets omställning från ett förrådsställt invasionsförsvar till ett slimmat insatsförsvar. I och med försvarsproposition 2008/09:140 *Ett användbart försvar* så har åter frågan om försvarsplanering aktualiserats och därmed också frågorna om civil-militär samverkan och ett civilt försvar vid höjd beredskap och krig (se intervju med Ann Ödlund sidan 26).

Efter att det civila försvaret mer eller mindre har legat i träda i över ett decennium ska nu arbetet med ett civilt försvar återupptas på lokal, regional och nationell nivå. Det är dock inte möjligt att ta vid där man slutade och återskapa kalla krigets civila försvar. Nu handlar det om att skapa ett nytt civilt försvar integrerat med det existerande krisberedskapssystemet och i ett samhälle som i stora stycken fungerar på ett helt annat sätt än för ett drygt decennium sedan. Arbetet med ett nytt civilt försvar och en civil-militär samverkan har så sakteligen startat på den nationella och regionala nivån. Hur den fortsatta färdriktningen och ambitionsnivån ser ut får sägas vara oklart, inte minst när det gäller den lokala nivån. Utmaningarna kommer dock att bli många.

Samhällsstörningar – robusthet, säkerhet och trygghet

Parallellt med inrättandet och utvecklingen av ett nationellt krisberedskapssystem med fokus på större fredstida kriser har det också pågått en utveckling mot att integrera krisberedskapsfrågor med frågor längs övriga hotskalan som rör robusthet, säkerhet och trygghet i samhället. Med andra ord handlar det alltmer om att säkerställa en samlad förmåga; om att förebygga, avvärja och hantera samhällsstörningar, såväl stora som små, dygnet runt.

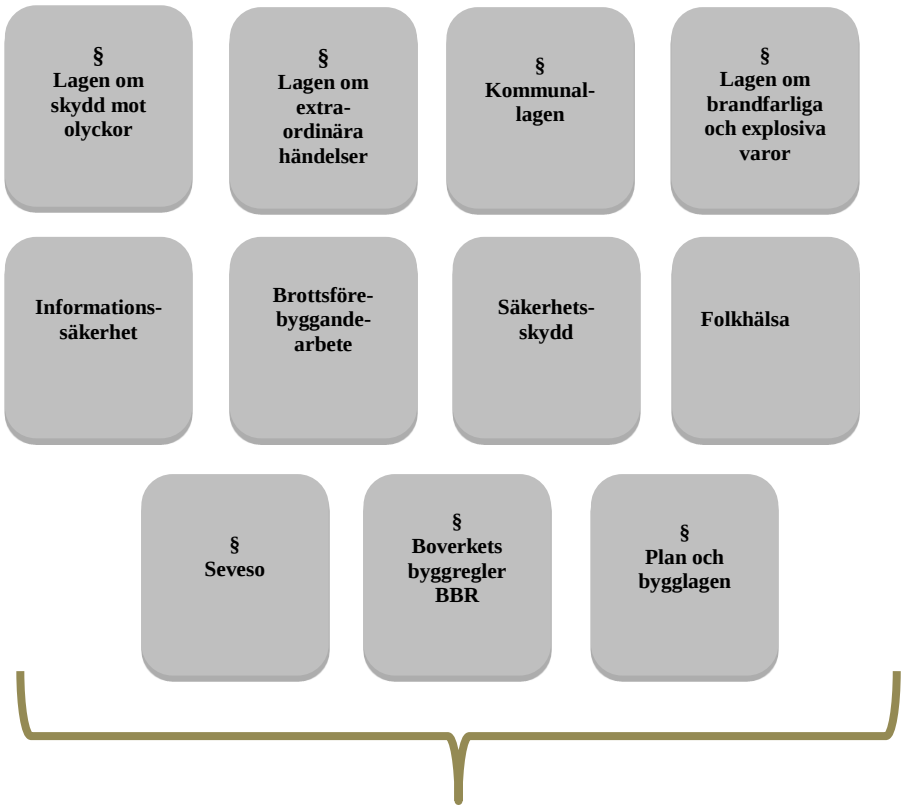
På den nationella nivån manifesterades denna utveckling organisatoriskt i att Myndigheten för samhällsskydd och beredskap (MSB) inrättades 2009, samtidigt som Krisberedskapsmyndigheten, Statens räddningsverk och Styrelsen för psykologiskt försvar lades ner. MSB fick ett brett ansvar längs hela hotskalan. Myndigheten fick ansvar för frågor om skydd mot olyckor, krisberedskap och civilt försvar, i den utsträckning inte någon annan myndighet har ansvaret. Ansvaret avser åtgärder före, under och efter en olycka eller kris. MSB fick därvid ansvar för att utveckla, stödja och driva på arbetet med samhällets krisberedskap, arbeta med samordning, bidra till att minska konsekvenserna av olyckor och kriser, följa upp och utvärdera samhällets krisberedskap samt se till att utbildning och övning kommer till stånd inom myndighetens ansvarsområde. MSB fick också ansvar för att genomföra insatser internationellt med syfte att bistå svenskar vid katastrofer utomlands och att bistå andra länder som drabbas av kris och katastrofer (inklusive förebyggande arbete).

På den regionala nivån har utvecklingen mot att krisberedskapsfrågor alltmer integreras med vardagliga säkerhets- och trygghetsfrågor hittills varit mer diffus. Det finns dock tecken på en sådan utveckling genom bland annat en begynnande trend i form av fysisk samplacering av olika organisationers alarm- och ledningsfunktioner. I Jämtland har det inrättats ett ”Trygghetens hus” i Östersund. I Trygghetens hus inryms polismyndigheten i Jämtlands län, Jämtlands Räddningstjänstförbund, SOS Alarm, landstinget i form av ambulans och sjukvårdsrådgivningen, Åklagarmyndigheten, Tullen, Svenska kyrkan och viss personal från Länsstyrelsen i Jämtlands län. I huset finns även Kriminalvården representerad i form av ett provisoriskt häkte. De framtida ambitionerna är att större insatser vid olyckor och kriser, både nationellt och internationellt, ska kunna samordnas från Trygghetens Hus.

Bild 3: Trygghetens hus i Östersund. Foto: Jan Mårdberg/Sveriges Radio.

I Stockholm har det fattats beslut om att inrätta en regional samverkanscentral i en ny byggnad som ska stå klar 2016. Centralen ska inledningsvis inrymma Storstockholms brandförsvar, SOS Alarm, Trafik Stockholm och Trafikverket. I sydöstra Skåne har det förts diskussioner om ett Trygghetens hus utan att det hittills kunnat realiseras. Inom en snar framtid kommer troligen allt fler lösningar i linje med ”Trygghetens hus” i Jämtland att se dagens ljus i landet. På den regionala nivån arbetar också allt fler landsting/regioner med att inom den egna verksamheten närmare integrera olika frågor rörande krisberedskap och andra mer vardagsnära säkerhetsfrågor som till exempel patientsäkerhet och driftsäkerhet.

Det är emellertid på den lokala nivån, bland kommunerna som utgör basen i krisberedskapssystemet, som utvecklingen mot att krisberedskapsfrågor alltmer integreras med vardagliga säkerhets- och trygghetsfrågor främst ägt rum, en utveckling som understöds av MSB och Sveriges kommuner och landsting (SKL). Av praktiska och kostnadsmässiga skäl samlar allt fler kommuner vissa lagstiftnings- och verksamhetsområden till ett integrerat politikområde som oftast benämns ”trygghet och säkerhet”.



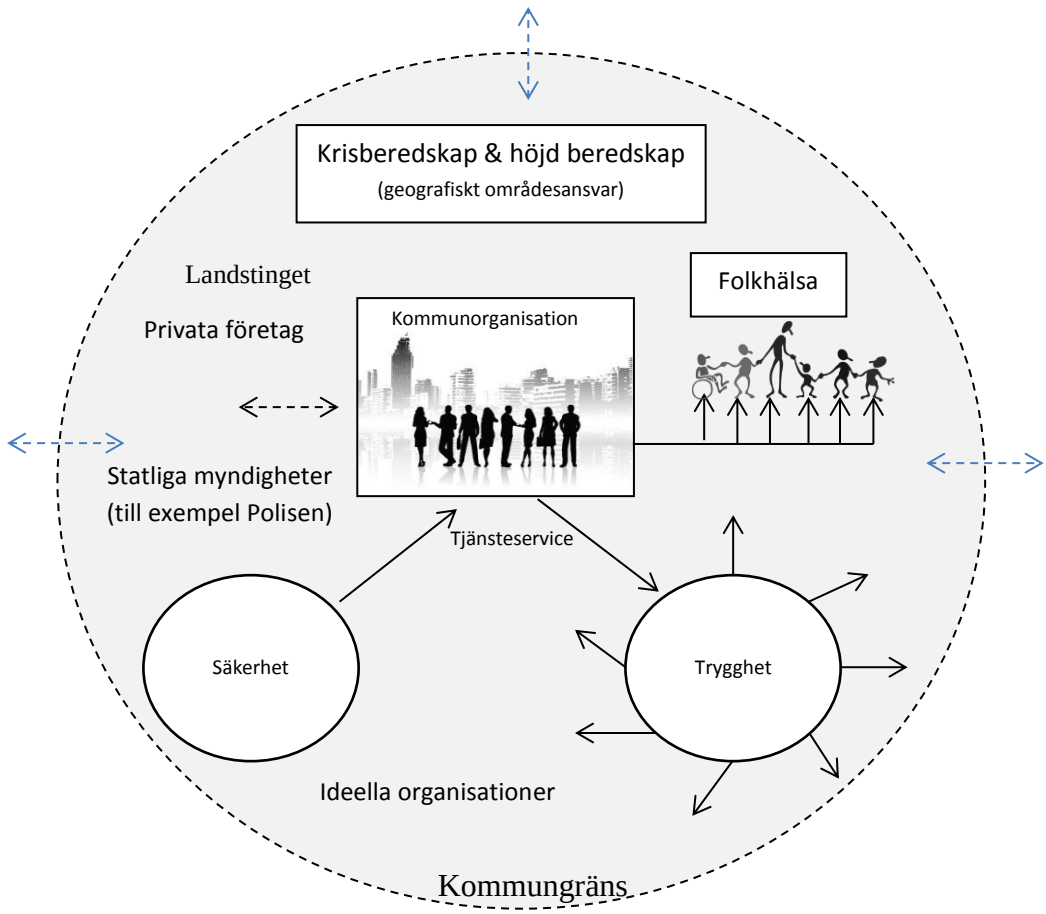
Figur 1. Kommunernas arbete med trygghet och säkerhet (Fritt efter figur i skriften ”Ta ett samlat grepp: Om trygghet och säkerhet”, MSB/SKL, 2012, s.10).

Hur arbetet med trygghet och säkerhet avgränsas skiljer sig betydligt mellan berörda kommuner, men i figuren ovan redovisas verksamhetsområden och styrande lagar som ofta inbegrips i området. Grovt handlar det vanligen om verksamheterna trygghet, säkerhet, krisberedskap och vissa fall även folkhälsa. I det integrerade politikområdet ”trygghet och säkerhet” kan relationerna mellan komponenterna trygghet, säkerhet, krisberedskap och folkhälsa förenklat beskrivas enligt följande; *Trygghet* handlar om att verka ut mot det offentliga rummet för att skapa trygghet för den enskilda individen med avseende på skydd mot olika former av hot och faror, inte minst brottslighet.

Säkerhet handlar om att verka inåt mot den kommunala organisationen för att skydda och säkra dess verksamhet, i samverkan med andra aktörer vid behov, så att kommunen kan leverera de tjänster och den service som den är ålagd att förse

de individer som bor och vistas i kommunen samt de företag som verkar i kommunen, med. Det handlar med andra ord här i stor utsträckning om så kallad kontinuitetsplanering samt inre och yttre säkerhetsskydd för kommunens verksamhet.

Krisberedskap kopplar till det geografiska områdesansvaret på lokal nivå och handlar om att verka geografiskt över kommunens yta för att i samverkan med olika organisationer och företag förebygga och hantera extraordinära händelser inom kommunens territorium. Folkhälsa, till sist, handlar om förebyggande arbete riktat mot den enskilde individen och kommuninvånaren för att stödja denna i vårdnaden av sin fysiska och psykiska hälsa, till exempel alkohol- och drogprevention.



Figur 2. Relationer mellan komponenterna säkerhet, trygghet, folkhälsa och krisberedskap inom det integrerade politikområdet ”trygghet och säkerhet".

Målet med kommunernas arbete kring trygghet och säkerhet är vanligen att skapa en övergripande trygghet och säkerhet för alla som bor, vistas och verkar i kommunen genom att på bästa sätt förebygga och hantera störningar i samhällslivet – från olyckor i vardagen till kriser – som hotar individens trygghet och säkerhet. Individen och dess behov står i centrum. Kommunerna ser arbetet med trygghet och säkerhet som en mycket viktig hörnsten i sitt samhällsbyggande och i förstärkandet av samhällskontraktet med individen. Kommunernas arbete med trygghet och säkerhet syftar också till att bygga ett starkt varumärke som en kommun som står väl rustad mot olika former av samhällsstörningar och därför gör det till en intressant kommun för företag att verka i samt för individer att bosätta sig i.

Kommunerna organiserar vanligen det integrerade politikområdet ”trygghet och säkerhet” i en särskild avdelning eller enhet för trygghet och säkerhet. För att säkerställa tjänsteleveranser gentemot individer och företag i kommunen är kommunorganisationens arbete med samhällets robusthet, säkerhet och trygghet i hög grad, som antytts ovan, inriktad mot så kallad kontinuitetsplanering, det vill säga hur ett företag eller organisation ska leverera produkter eller tjänster även om produktionen störs.

Den beskrivna utvecklingen mot ett alltmer integrerat arbete rörande samhällelig robusthet, säkerhet och trygghet ställer ökade krav på samverkan och samordning inom krisberedskapssystemet. Utvecklingen på den lokala och regionala nivån återspeglas dock inte av samma utveckling på den nationella nivån, med undantag för inrättandet av MSB. Arbetet inom Regeringskansliet och hos centrala myndigheter när det gäller styrningen av den regionala och lokala nivån sker fortfarande i stor utsträckning enligt traditionell stuprörsprincip. Det kan därför antas att kravet på samverkan och samordning på den nationella nivån behöver utvecklas för att den framtida styrningen av krisberedskapsarbetet på lokal och regional nivå ska bli ändamålsenlig och i linje med den utveckling som sker på dessa nivåer.

Den aktuella utvecklingen kan också medföra att MSB medvetet eller omedvetet knyter den direkta hanteringen av allt fler sakfrågor, till exempel social oro och brottslighet, till sitt ansvarsområde på ett sätt som tidigare inte har skett och att det därför riskerar att uppstå ansvarskonflikter med andra myndigheter, om det inte sker i ett uttalat samförstånd. På den nationella nivån står man således inför ett antal möjligheter och utmaningar kring myndigheternas roller och ansvar när det gäller att managera en utveckling mot alltmer integrerat arbete i fråga om samhällelig robusthet, säkerhet och trygghet.

Några viktiga strukturella förutsättningar för krisberedskapen

Den framtida utvecklingen av svensk krisberedskap och ett nytt civilt försvar, oavsett vilka vägval som görs, har att förhålla sig till olika strukturella grundförutsättningar, vilka på ett eller annat sätt är kopplade till den allmänna samhällsutvecklingen. Förutsättningarna har sedan krisberedskapssystemet inrättades i många fall förändrats och är därför viktiga att uppmärksamma i en diskussion om krisberedskapssystemets framtid. Nedan ska några viktiga strukturella förutsättningar för krisberedskapsarbetet och arbetet med ett nytt civilt försvar belysas.

Allt starkare ömsesidiga beroendeförhållanden mellan samhällsviktiga verksamheter

Med samhällsviktig verksamhet brukar vanligtvis avses verksamhet som uppfyller det ena eller båda av följande villkor: 1) Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället. 2) Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad allvarlig kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.

Vad som utgör en samhällsviktig verksamhet är delvis situationsbetingat, men exempel är: produktion och distribution av el, fjärrvärme, bränsle och drivmedel, telefoni och IT-tjänster, dricksvatten samt tjänster som transporter (väg, sjö, järnväg och flyg), sjukvård, räddningstjänst, betalningsförmedling samt utbetalningar från sjuk- och arbetslöshetsförsäkringen och det allmänna pensionssystemet. I takt med den allmänna samhällsutvecklingen växer det fram allt fler och allt starkare ömsesidiga beroendeförhållanden mellan olika samhällsviktiga verksamheter. Med andra ord, om en samhällsviktig verksamhet faller ifrån riskerar även andra att falla ifrån. De ömsesidiga beroendena ställer allt högre krav på samverkan och samordning inom och mellan olika samhällssektorer för att dels förebygga och reducera de sårbarheter som de ömsesidiga beroende-förhållandena skapar, dels kunna hantera uppkomna kriser.

En allt större del av den samhällsviktiga verksamheten bedrivs av privata aktörer och är fördelad på allt fler aktörer

Samtidigt som beroendeförhållandena mellan olika samhällsviktiga verksamheter ökar så bedrivs alltmer av den samhällsviktiga verksamheten inte längre i offentlig utan i privat regi. Det är bland annat en följd av den avreglering som har genomförts inom många samhällssektorer sedan 1990-talet. Idag existerar till exempel inte Televerket längre med sitt de facto monopol på telefoni utan det har ersatts av ett mycket stort antal privata teleoperatörer. Att samhällsviktig verksamhet bedrivs i privat regi ställer ökade krav på en väl fungerande privat-

offentlig samverkan för att möjliggöra inriktning och styrning av krisberedskaps-arbetet eftersom privata aktörer inte har samma skyldigheter att arbeta med krisberedskapsfrågor som offentliga samhällsaktörer har, inte minst vad gäller just samverkan. Som nämnts ovan har till exempel privata aktörer i allmänhet, till skillnad mot kommuner, landsting och myndigheter, ingen laga skyldighet att upprätta risk- och sårbarhetsanalyser.

Men den aktuella utvecklingen kräver inte bara mer privat-offentlig samverkan utan även privat-privat samverkan, det vill säga, att olika privata aktörer direkt sinsemellan arbetar med krisberedskapsfrågor som till exempel på elförsörjningsområdet där krisberedskapssamverkan sker inom ramen för branschorgansationen Svensk energi. Av betydelse för krisberedskapsarbetet är också att inte bara alltmer samhällsviktig verksamhet bedrivs av privata aktörer och att alltmer samhällsviktiga resurser finns i privat ägo utan att själva antalet aktörer hela tiden ökar i konkurrensen på en fri marknad. Det innebär att antalet aktörer i krisberedskapssystemet ökar och att samverkan och samordning många gånger också blir mer tidskrävande och komplicerad.

En alltmer kontraktsbaserad krisberedskap

Många statliga myndigheter är idag inte utförarorganisationer med egna resurser som kan sättas in vid en kris, utan de är i hög grad rena upphandlings-organisationer utan egna fysiska resurser. De upphandlar med andra ord tjänster och resurser från olika privata aktörer på en marknad. Dessa aktörer upphandlar ofta i sin tur vidare tjänster och resurser från olika underentreprenörer. Många gånger utförs därför samhällsviktig verksamhet i långa entreprenörs- och upphandlingskedjor. Statliga myndigheter, kommuner och landsting bolagiserar och upphandlar också delar av sin verksamhet i allt större utsträckning. De inför också i allt högre grad ett köp-och-säljförfarande inom den egna organisationen. Sammantaget får detta direkta återverkningar på krisberedskapsarbetet eftersom det i allt större utsträckning måste bygga på affärskontrakt och olika former av köp- och säljförfaranden.

Statliga myndigheter, kommuner och landsting måste genom affärskontrakt säkerställa att och hur externa utförare av deras verksamhet arbetar med krisberedskapsfrågor samt vid en kris hur och när de ska samverka och samordna sig med andra berörda aktörer. Krisberedskapen blir därmed inte bättre än de kontrakt man skriver med dess utförare (som i sin tur eventuellt måste skriva kontrakt med sina underleverantörer). Idag har krisberedskapen (inklusive det vidgade arbetet med ”säkerhet och trygghet”) således blivit allt mer ”kontraktsbaserad”. Samtidigt är kunskapen generellt bristfällig om hur kontraktsstyrning kan samspela med traditionell förvaltningsstyrning vid inriktning och styrning av krisberedskapssystemet i dess helhet och inom olika sektorer och på olika nivåer.

Ökad internationalisering av samhällsliv, hotbild och krisberedskap

Mycket av den samhällsviktiga verksamheten bedrivs inte bara av privata aktörer utan en stor del är dessutom i utländsk ägo. Att i krisberedskapssammanhang ställa krav mot företag och koncerner med huvudkontor och vitala funktioner, som till exempel driftcentraler, utanför Sveriges gränser är många gånger mer problematiskt än mot inhemska aktörer. Vidare är allt fler av hoten, mot de av regeringen och riksdagen uppställda säkerhetsmålen, av en nationellt gränsöverskridande karaktär, till exempel terrorism och smittsamma sjukdomar hos människor och djur. Dessa hot kan därför inte effektivt förebyggas och hanteras enbart på nationell nivå, utan kräver samarbete med andra länder. Svenskt krisberedskapsarbete är och blir också alltmer invävt i olika former av samarbete med andra länder, framförallt genom det krisberedskapsarbete som sker inom Europeiska unionen (EU).

Samarbetet inom EU omfattar gemensam forskning och kunskapsuppbyggnad kring ömsesidigt stöd av resurser och kompetenser vid kriser, gemensamma utbildningar på till exempel räddningstjänstområdet, gemensamma informations- och varningssystem inom olika sektorer och områden (till exempel för hot i livsmedelskedjan), strukturer på hög politisk nivå för att underlätta samordning av nationella krisberedskapsåtgärder med mera (flera artiklar i denna skrift belyser just samarbete inom EU som FOI är involverad i).

I EU:s fördragstexter (Lissabonfördraget, artikel 196 Civilskydd) fastslås att EU ”ska främja samarbetet mellan medlemsstaterna i syfte att förbättra effektiviteten hos systemen för förebyggande av och skydd mot naturkatastrofer och katastrofer som orsakas av människor”. Vidare heter det bland annat att EU:s insatser syftar till att ”stödja och komplettera medlemsstaternas insatser på nationell, regional och lokal nivå när det gäller förebyggande av risker, beredskapen hos medlemsstaternas aktörer inom området civilskydd [inte att förväxla med civilt försvar] samt insatser vid naturkatastrofer eller av människor orsakade katastrofer inom unionen”. EU utgör mot denna bakgrund en fjärde nivå i det svenska krisberedskapssystemet utöver de tre vanligen omnämnda nivåerna; nationell, regional och lokal. Viktigt att understryka är dock att denna fjärde nivå är av annan karaktär än de tre övriga, inte minst därför den självfallet inte innefattar något geografiskt områdesansvar från EU:s sida.

En minskande redundans i kombination med bland annat kompetensförlust i samband med generationsskifte

Både privata och offentliga organisationer har under en lång tid av ekonomiska skäl strävat efter att hålla minsta möjliga personella bemanning för hantering av den vardagliga löpande verksamheten. Det gör att det idag, inom till exempel kommuner och landsting och av dem kontraktade aktörer, i normalfallet finns mycket begränsad redundans (reservkapacitet) på det personella området. Det i sin tur riskerar att underminera deras krisberedskapsförmåga i fråga om uthållighet vid längre kriser då man snabbt kommer att köra slut på tillgänglig

personal, framförallt olika specialister och nyckelkompetenser. Detta är ett problem som givetvis är svårt att komma åt från ett krisberedskapshåll eftersom krisberedskap inte är styrande i den allmänna samhällsutvecklingen. Det skulle till exempel kräva att det gick att ställa särskilda krav på personell redundans för att få bedriva olika former av samhällsviktig verksamhet, till exempel i samband med upphandling av offentligt finansierade verksamheter som äldreomsorg och kollektivtrafik.

Kopplat till frågan om alltmer personellt slimmade organisationer är också den ökade användningen av personal från bemanningsföretag och olika former av korttidsanställningar i såväl privata som offentliga organisationer. Personal från bemanningsföretag och korttidsanställda i till exempel projekt är oftast så kort tid i en organisation att de inte kan tjäna som organisatoriskt minne när det gäller hur organisationen tidigare har hanterat allvarliga störningar och kriser, vare sig övade eller verkliga sådana. Vid krissituationer är det oftast svårt att ersätta operativ och strategisk överblick som kommer av erfarenhet. Kopplad till frågan om erfarenhet är i sin tur frågan om kompetensöverföring vid generationsskifte. Idag saknar många privata och offentliga organisationer, som ansvarar för samhällsviktig verksamhet, väl fungerande former för systematisk överföring av krisberedskapsrelaterad kompetens och erfarenhet vid pensions- och andra avgångar. Individer tar med sig sin och delar av organisationens krisberedskaps-kompetens när anställningen avslutas.

En tilltagande ”krisberedskapsklyfta”

Det finns idag tecken på att det håller på att växa fram en ”krisberedskapsklyfta” eller åtminstone en ”krisberedskapsspricka” på lokal nivå. Klyftan, eller sprickan, går mellan å ena sidan de kommuner som aktivt och målinriktat arbetar med att verkställa gällande nationell lagstiftning på krisberedskapsområdet eller som själva proaktivt driver arbetet längre än så (till exempel ifråga om att arbeta med trygghet och säkerhet) och å andra sidan kommuner vars krisberedskapsarbete är klart eftersatt och reaktivt. I det första fallet tenderar det att handla om resursstarka kommuner i storstads- och tillväxtregioner och/eller kommuner som är väldigt motiverade att arbeta med krisberedskapsfrågor, till exempel eftersom de oftare är utsatta för allvarliga olyckor eller kriser.

I det andra fallet verkar det handla om resurssvaga kommuner i glesbygd eller utanför storstads- och tillväxtregioner och/eller kommuner som inte är motiverade att arbeta med krisberedskapsfrågor, till exempel på grund av att de inte har varit utsatta för allvarliga olyckor eller kriser. Stora skillnader i krisberedskapsförmåga till följd av olika ambitioner på krisberedskapsområdet försämrar bland annat möjligheten att producera och aggregera nationellt heltäckande lägesbilder uppåt i systemet som kan resultera i återkopplad styrning och inriktning från nationell nivå samt möjligheten att grannkommuner effektivt ska kunna samverka och ömsesidigt stödja varandra vid kriser. En

krisberedskapsklyfta är därför ett problem för det nationella krisberedskaps-systemet och dess sammanhållning, inte bara ett problem för berörda kommuner.

Individens förväntningar och egenansvar på krisberedskapsområdet
Troligen står idag samhällets resurser och förmågor inte i paritet med många individers förväntningar på i vilken omfattning och hur snabbt samhället kan bistå den enskilde vid olika former av störningar och kriser. Med andra ord kan förväntningarna antas vara orealistiska på grund av bristande kunskaper om samhällets olycks- och krisberedskap och om det egna ansvaret i sammanhanget. En allt snabbare puls i samhällslivet gör dessutom att människors acceptans för avbrott och störningar kan antas minska alltmer. Orealistiska förväntningar och bristande kunskap om samhällets beredskap medför i sin tur att man på det individuella planet är otillräckligt förberedd för att i ett initialskede kunna hantera olyckor och kriser innan man från samhället sida har möjlighet att vidta åtgärder; till exempel kan det handla om att ha en brandsläckare och ett mindre matförråd i hemmet.

Till saken hör vidare att i takt med att det svenska samhället blir alltmer heterogent får vi också ett samhälle där frågan om riskuppfattning och riskacceptans blir mer mångfacetterad än tidigare. En stor pedagogisk utmaning i krisberedskapsarbetet framöver är därför att nå ut med kunskap till människor om vad de realistiskt kan förvänta sig av samhällets krisberedskap och rusta dem med den kunskap som behövs för att de ska kunna ta ett egenansvar på krisberedskapsområdet. Ideella organisationer torde här ha en viktig funktion att fylla.

Avslutning

I artikeln har utvecklingen av svensk krisberedskap i form av ett nationellt krisberedskapssystem beskrivits. Krisberedskapen har utvecklats från det vardagliga arbetet med skydd mot olyckor samt från arbetet med ett civilt försvar under det kalla kriget till dagens ökade fokus på en generell förmåga att förebygga och hantera allvarliga händelser och kriser. Det finns idag också en utveckling mot att arbeta integrerat med frågor som rör krisberedskap, säkerhet och trygghet, framförallt på den lokala nivån. Samtidigt återupptas försvarsplaneringen och därmed arbetet med ett nytt civilt försvar, det gamla har legat i träda i ett drygt decennium. I artikeln har det också pekats på ett antal strukturella förutsättningar som skapar särskilda utmaningar för dagens och morgondagens arbete med krisberedskap, trygghet och säkerhet samt civilt försvar.

En av dessa strukturella förutsättningar avser det allt större inslaget av nya marknadslösningar såsom avreglering samt köp-och-säljförfarande i offentlig verksamhet som gjort krisberedskapen och trygghets- och säkerhetverksamhet till

stora delar ”kontraktsbaserad”. Man kan idag därför tala om ”kontraktsbaserad samhällssäkerhet” som en realitet. Denna utveckling kräver nya styrmedel för att krisberedskapssystemet effektivt ska kunna inriktas och styras då traditionell förvaltningsstyrning inte längre räcker till.

Sammantaget har det svenska krisberedskapssystemet efter ett drygt decennium kommit till en punkt där det krävs en tydlig färdplan för nästkommande decennium. Arbetet med att utveckla en sådan färdplan måste involvera alla berörda aktörer i samhället, men är ytterst ett ansvar för regering och riksdag. Om det första decenniet till stor del handlat om att lägga fast krisberedskaps-systemets olika komponenter (strukturer, principer och resurser med mera) så behöver det kommande decenniet fokusera på att få dessa olika komponenter att fungera tillsammans som ett sammanhängande system. Nämnda färdplan måste baseras på en klar bild av rådande samhällsförutsättningar och på vad vi kan skönja av ett framtida samhälle, inte på en invand och förlegad bild av samhället.

INTERVJU

2 Ett nytt civilt försvar och förstärkt civil-militär samverkan

Intervju med Ann Ödlund

***Ann Ödlund** är fil. kand. i beteendevetenskap och förste forskare. Ann har arbetat med krishantering både gentemot Försvarsmakten och civila myndigheter, idag främst Myndigheten för samhällskydd och beredskap, sedan mitten av 1990-talet. Ann är doktorand inom organisations- och socialpsykologi vid Stockholms universitet. Avhandlingsämnet "interorganisatorisk samverkan i svensk krishantering" växte fram genom erfarenheter av analyser av olika kriser, där samverkan ofta beskrevs som nödvändig men problematisk.*

Ett nytt civilt försvar

– Det blir svårt att bygga vidare på det gamla civila försvaret och formerna för den civil-militära samverkan som existerade under kalla kriget. Stora förändringar i organisation och verksamhet har genomförts, både kvalitativt och kvantitativt. Det krävs en nystart och ett nytt tänk understryker Ann Ödlund som är forskare vid FOI och som arbetat med frågor kring krishantering och civilt försvar sedan början av 1990-talet. Det civila försvaret har i princip varit borta från agendan i ett decennium. Frågor som nu aktualiserats handlar om att återuppta planering för det territoriella försvaret av Sverige, bygga ett nytt civilt försvar och en förstärkt civil-militär samverkan, både i fredstida kriser och i samband med höjd beredskap.

Utmaningarna och behoven är många. För det första handlar det, enligt Ann Ödlund, om att från grunden identifiera vilken roll som ett civilt försvar ska fylla i dagens och morgondagens samhälle och vilka behov som finns utöver det som redan hanteras inom krisberedskapssystemet. Det handlar om verksamhet som planering och övning, men även om hur det civila försvaret ska organiseras och hur förmåga till beslut, till exempel kring nödvändiga prioriteringar, ska säkerställas.

Utifrån vilka hotbilder ska man bygga ett civilt försvar frågar Ann retoriskt? Ett traditionellt militärt anfall mot hela eller delar av landet, terrorbombningar mot civilbefolkning eller ett cyberkrig som lamslår viktiga samhällsfunktioner, kanske i kombination med riktade militära operationer? Ann Ödlund betonar också att det är av största vikt att regeringen, Regeringskansliet och Myndigheten

för samhällsskydd (MSB) lägger vikt vid att förankra planerna om ett civilt försvar hos kommuner, landsting, centrala myndigheter och privata aktörer. Här förväntas principer för finansiering bli en brännande fråga, tror Ann Ödlund.

För det andra handlar det, enligt Ann Ödlund, om att identifiera vilka behov Försvarsmakten har av det civila försvaret för att kunna lösa sina uppgifter vid höjd beredskap. Inom ramen för den återupptagna försvarsplaneringen måste arbetet med det civila och militära försvaret gå hand i hand. Det krävs med andra ord en integrerad utvecklingsprocess, där inte minst gemensamma övningar är en viktig komponent. I sammanhanget finns det också behov av att se över gällande regelverk samt de militära och civila beredskapssystemen som används för fredstida kriser.

För det tredje måste, enligt Ann Ödlund, ett nytt civilt försvar bygga vidare på det existerande krisberedskapssystemet och dess processer. Men det går samtidigt inte att göra utan att förstå att krisberedskap och ett civilt försvar för höjd beredskap och krig handlar om hantering av väsensskilda förutsättningar. Vi har att göra med antagonistiska hot i en storskalig omfattning. Vi behöver tänka kring befolkningsskydd som skyddsrum, evakuering av städer under pågående stridshandlingar, hur man bygger upp civila motståndsrörelser och hur information ska förmedlas. Det vill säga åtgärder som inte inbegrips i det vanliga krisberedskapsarbetet, betonar Ann Ödlund. Ofrånkomliga frågor är hur pliktsystemet för soldater och sjömän med flera ska aktiveras, mobilisering ske och vad detta har för roll i dag.

Förstärkt civil-militär samverkan

Regeringen har nyligen tydligare signalerat att den civil-militära samverkan måste stärkas avseende både krisberedskap och vid höjd beredskap och krig. På frågan om vilka som är de främsta utmaningarna och behoven här sett ur Försvarsmaktens perspektiv lyfter Ann Ödlund fram följande.

För det första handlar det om hur Försvarsmakten ska hantera de samverkansuppgifter som myndigheten har idag, det vill säga a) ordinarie myndighetssamverkan till exempel vid planering och stödinsatser, b) totalförsvarssamverkan, som avser samverkan med främst bevakningsansvariga myndigheter vid försvarsplanering och andra förberedelser inför och vid höjd beredskap samt c) samverkan med internationella organisationer och aktörer.

För det andra är det ett problem vid planering inför stöd till samhället i fredstid att det råder osäkerhet om i vilken omfattning och med vilka förmågor Försvarsmakten kan stödja samhället. Uppgiften får inte vara dimensionerande för Försvarsmaktens verksamhet och det finns en osäkerhet hos civila aktörer och även inom Försvarsmakten, om vad som vid en viss given tidpunkt finns fysiskt gripbart. Det innebär att civila myndigheter ibland inte heller vet vad man kan efterfråga. Vidare konstaterar Ann Ödlund att Försvarsmakten inte längre finns

fysiskt representerad över hela landet och att informella, vardagliga kontakter därför riskerar att begränsas till vissa orter där Försvarsmakten fortfarande har verksamhet. Den folkförankring som grundades i geografisk närvaro, allmän värnplikt och allmän information som telefonkatalogens avsnitt ”Om kriget kommer”, går inte att räkna med längre, vilket också är viktigt att fundera kring.

För det tredje handlar det om frågan om hur Försvarsmakten ska beredas utrymme och integreras i arbetet inom de centrala myndigheternas samverkansområden, där mycket informationsutbyte sker mellan civila myndigheter. Regionalt, där militärregionstaber nu ersatt de så kallade SäkSamsektionerna är det viktigt att ta hänsyn till tidigare upparbetade nätverk och olika regionala förutsättningar och samverkansbehov, påpekar Ann Ödlund. Inte att förglömma är kommuner och landsting. De spelar en viktig roll i sammanhanget. Vad behöver Försvarsmakten av dem och vice versa?

– Man måste ha tålamod när man nu ska skapa ett nytt civilt försvar och förstärka den civil-militära samverkan. Det kommer att krävas mycket arbete på olika håll och nivåer i samhället. Det kan verka överväldigande om man tänker på att det civila försvaret ska omfatta all verksamhet som ska bedrivas i krig, men vi har ju både hyfsat bra författningar även för höjd beredskap och dessutom ett utbyggt krisberedskapssystem att luta oss mot. Ett tips är att ta ett djupt andetag, göra det enkelt i början och inte krångla till det i onödan, konstaterar avslutningsvis Ann Ödlund.

3 Vad hotar oss?

Lotta Ryghammar och Per Larsson

Scanpix: Thure Wikberg

”Vår beredskap är god” sa han i sitt berömda tal, statsminister Per Albin Hansson den 27 augusti 1939 på Skansen. Och han talade inte om miljökatastrofer eller cyberattacker. Oavsett vad uttalandet exakt avsåg utgick den svenska beredskapen under ytterligare årtionden uteslutande från krigshotet, innan utvecklingen i vår omvärld och i vårt samhälle i grunden förändrade synen på och förutsättningarna för hot och beredskap (se vidare artikel *Från civilt försvar till kontraktsbaserad samhällssäkerhet*). Samhället utvecklas ständigt och med denna utveckling följer nya och ofta komplexa hot och risker (se vidare artikel *Komplexa risker – utmaningar för samhällets riskbedömning)*. Nu ska också det civila försvaret efter ett decennium i träda återupplivas i enlighet med förvarsplaneringen. Listan på hot och risker blir allt längre. Vilka är de idag och vilken förmåga har vi att hantera dem? FOI har på uppdrag av Försvarsdepartmentet studerat myndigheternas risk- och sårbarhetsanalyser 2012. Den här artikeln redovisar det sammanställda resultatet av risk- och sårbarhetsanalysernas olika delar.

Ett nationellt system för risk- och sårbarhetsanalyser

Samtliga statliga myndigheter, landsting och kommuner ska i syfte att stärka sin egen och samhällets krisberedskap årligen göra en risk- och sårbarhetsanalys med tillhörande förmågebedömning. De myndigheter som har ett särskilt ansvar för krisberedskapen (23 centrala myndigheter och 21 länsstyrelser) och de myndigheter som Myndigheten för samhällsskydd och beredskap (MSB) beslutar i enskilda fall (10 centrala myndigheter 2012), ska enligt *förordning (2006:942) om krisberedskap och höjd beredskap* och föreskrifter från MSB lämna en redovisning baserad på risk- och sårbarhetsanalysen till Regeringskansliet och MSB. Myndigheter med ett sektorsansvar ska redovisa ett analysresultat för såväl den egna myndigheten som sektorn som helhet.

Förutom att utgöra en grund för myndighetens eget krisberedskapsarbete utgör risk- och sårbarhetsanalyserna bland annat ett underlag för MSB:s årliga bedömningar av samhällets förmåga att motstå och hantera allvarliga händelser samt identifiering och planering av förbättringsåtgärder. För respektive departement kan analyserna användas som ett av flera underlag i den departementala styrningen av myndigheterna. Försvarsdepartementets enhet för samordning av samhällets krisberedskap använder analyserna som en del i arbetet med att inrikta och utveckla området samhällets krisberedskap.

En sammanställning av myndigheternas risk- och sårbarhetsanalyser för år 2012

Utifrån ovan angivna myndigheters risk- och sårbarhetsanalyser av sina respektive ansvarsområden ska här de mest frekvent förekommande hoten, riskerna samt sårbarheterna och kritiska beroendena sammanställas och redovisas utan någon rangordning. Därutöver ska också kortfattat belysas hur myndigheterna ser på sin krisberedskapsförmåga, brister i den och åtgärder med anledning av den gjorda bedömningen. Artikelns redovisade sammanställning följer i stort MSB:s föreskrifter för hur myndigheternas risk- och sårbarhetsanalyser ska redovisas. Myndigheterna ska i det sammanhanget, inom sitt ansvarsområde, redovisa identifierade hot och risker, sårbarheter samt kritiska beroenden och bedömning av förmågan att motstå och hantera identifierade hot och risker samt åtgärder med anledning av risk- och sårbarhetsanalysens resultat. De olika komponenterna beskrivs i nämnd ordning nedan.

Vilka är de allvarligaste hoten och riskerna?

Enligt MSB:s definition omfattar *hot* en aktörs kapacitet och avsikt att genomföra skadliga handlingar. Ett hot kan även bestå av en händelse eller en företeelse som i sig framkallar fara mot något eller någon utan att det i sammanhanget förekommer aktörer med kapacitet och avsikt att orsaka skada. *Risk* är en sammanvägning av sannolikheten för att en händelse ska inträffa och de konsekvenser händelsen kan leda till.

HOT OCH RISK	KOMMENTAR
Allvarlig smitta	Hotar såväl människor som djur.
Antagonistiska hot	Utgörs av till exempel terrorism.
Olyckor med farliga ämnen	Sker till exempel inom transportsektorn.
Naturolyckor	Handlar till exempel om skogsbränder.
Extrema väderförhållanden	Avser bland annat isstormar.
Dammbrott	Kan få förödande konsekvenser för befolkningen, omöjliggöra elproduktion och skapa konflikter mellan olika samhällsintressen. Var ska man låta det svämma över och vem har mandatet att fatta ett sådant beslut?
Kärntekniska olyckor	Bland annat måste återväxten av viktig kompetens saknas.
Bränslebrist	Kan till exempel leda till utslagna transportsystem.
Störningar i kommunala försörjningssystem	Avser dricksvatten, avlopp, fjärrvärme etc. Störningar uppstår nära befolkningen och får snabbt effekt.
Störningar i teknisk infrastruktur	Avser el, elektroniska kommunikationer etc. som utgör fundament för samhällets alla sektorer.

Tabell 1: Hot och risker av traditionell karaktär

De uppräknade hoten och riskerna är av traditionell karaktär och årligen återkommande i myndigheternas risk- och sårbarhetsanalyser. Författarna noterar vidare själva att det också finns redovisade hot och risker av karaktären ”bubblare” som myndigheterna i sina redovisningar lyfter i allt större omfattning. Dessa hot och risker är inte okända eller nya för samhället i stort, men de är ”bubblare” i den meningen att de behandlas i myndigheternas analyser på ett allt mer framträdande sätt. Det är hot och risker som i hög grad berör många samhällssektorer och därför medför stora behov av samverkan mellan olika myndigheter och andra organisationer.

HOT OCH RISK	KOMMENTAR
Social oro	Uppstår till följd av sociala klyftor. Kan till exempel yttra sig i våld mot yrkeskategorier som brandmän samt ambulans och sjukvårdspersonal eller skadegörelse. Uppmärksammas även i högre grad på mindre orter.
Kriminalitet och organiserad brottslighet	Kopplar i allt högre grad till internationell kriminalitet och utvecklas i en transnationell riktning. Till exempel finns problem med illegal hantering (stölder och transporter) av avfall och metallskrot, främst pga. de stigande metallpriserna på global nivå. Sannolika risker är påverkan på infrastruktur som järnvägar, elektroniska kommunikationer (stöld av kopparkablar) och miljöförstöring.
Klimatförändringar	Medför ökande behov av samverkan, från lokal till internationell nivå, samt av att i ordinarie planering av verksamheten hantera klimatförändringar och inte längre betrakta dem som extraordinära händelser. Utvecklingen av ekosystem sker snarare språngvis.
Allvarliga hälsohot och antibiotikaresistens	Att bakterier har utvecklat resistens mot antibiotika bedöms av Världshälsoorganisationen (WHO) som ett av de största folkhälsoproblemen. Till exempel är sjukvården beroende av verksamma antibiotika vid cancerbehandlingar.

Tabell 2: Hot och risker av karaktären ”bubblare”

Vilka är de allvarligaste sårbarheterna och kritiska beroendena?

Enligt MSB:s definition betecknar *sårbarhet* hur mycket och hur allvarligt samhället eller delar av samhället påverkas av en händelse. De konsekvenser som en aktör eller samhället – trots en viss förmåga – inte lyckas förutse, hantera, motstå och återhämta sig från anger graden av sårbarhet. *Kritiska beroenden* utgörs av beroenden som är avgörande för att samhällsviktiga verksamheter ska kunna fungera. Sådana beroenden karakteriseras av att ett bortfall eller en störning i levererande verksamheter relativt omgående leder till sådana funktionsnedsättningar som kan få till följd att en allvarlig händelse inträffar. Den drabbade verksamheten kännetecknas av att den saknar uthållighet, redundans och möjlighet att ersätta eller fungera utan den resurs som fallit bort.

SÅRBARHETER OCH BEROENDEN	KOMMENTAR
Avsaknad av prioritering av resurser och tjänster till samhällsviktig verksamhet	Avser sektorer såsom transporter och elektroniska kommunikationer.
El, elektroniska kommunikationer, transporter, vatten	Stora beroenden finns också mellan dessa områden.
Systemsäkerhet	I högre grad komplexa system samt styrning av industriella processer över nätet ökar sårbarheten mot antagonister till exempel Otillbörlig systemöverssikt kan ske via offentlig information.
Expertstöd	Oklarheter råder avseende vilket expertstöd det finns att tillgå respektive ska finnas att tillgå.
Entreprenörsberoenden	I takt med ett ökat antal och fler privata aktörer har en otydlighet skapats kring ansvarsförhållanden. Fler aktörer innebär också fler beroenden att förhålla sig till. Många anlitar samma entreprenörer vilket gör det svårt att få en överblick över vilka resurser som faktiskt finns tillgängliga när flera aktörer drabbas vid en störning.
Centralisering, koncentrering	Av effektivitets- och samordningsskäl centraliseras och koncentreras viktig verksamhet till en eller ett fåtal platser, vilket gör verksamheten mer sårbar.
Fragmentisering	Gäller till exempel landstingets verksamhet. Efter avreglering har landstinget att samverka med ett mycket större antal och privata vårdgivare och andra entreprenörer, Samverkansbehoven inom krisberedskapssystemet blir betydligt mer komplicerade att tillgodose.
Redundans; personal och lager	Slimmade organisationer, svårersatta kompetenser högre personalomsättning, generationsskiften utan kunskapsöverföring och brist på återväxt inom vissa yrken utgör sårbarheter. Exempel på det senare är tank-bilförare, tekniker och ingenjörer inom elbranschen samt tekniker och fysiker inom kärnkraftsområdet. För att hålla nere kostnaderna för lagerhållning tillverkas inget förrän kunden lagt sin beställning enligt principen just-in-time.

Tabell 3: Sårbarheter och beroenden

Vilken förmåga, vilka brister och vilka åtgärder redovisas?

Myndigheterna ska i sina risk- och sårbarhetsanalyser med tillhörande förmågebedömning redovisa sin egen respektive sin sektors (i det fall man har ett sektorsansvar) bedömda generella krishanteringsförmåga respektive förmåga att i samhällsviktig verksamhet motstå störningar. Bedömningskategorierna är 1) behövs ej 2) mycket bristfällig 3) bristfällig 4) god med viss brist och 5) god. Flertalet myndigheter bedömer sammantaget förmågan som *god med vissa brister*. Återkommande brister handlar exempelvis om uthållighet över tid i såväl den egna organisationen som i den egna sektorn. Det gäller inte minst informationsfunktionen, där man befarar problem med att tillgodose såväl krav på säkerhet som ett allmänt behov av kommunikation samt att samla in, hantera och samverka kring information under pressade omständigheter. Många myndigheter anger också brister vad gäller viktig reservkraft och möjligheten att flytta samhällsviktig verksamhet till annan plats. Mot bakgrund av bland annat händelsen i Fukushima och stormen Sandy uppmärksammar flera myndigheter i sina analyser för såväl den egna organisationen som den egna sektorn brister i planeringen inför utrymning och evakuering.

Sårbarheter och brister i förmåga kan ofta vara av komplicerad natur och kräva sektorsövergripande och i tid och rum med andra aktörer samordnade åtgärder. Att som myndighet själv bemöta sådana behov och formulera konkreta åtgärder är inte enkelt. Ofta är åtgärdslistorna som myndigheterna redovisar kopplade till övning, utbildning, samverkansstrukturer samt utveckling av tekniska stödsystem och reservkraft.

Utmaningar - några sammanfattande slutsatser

I risk- och sårbarhetsanalyserna för 2012 noterar författarna att myndigheterna ofta i någon form återkommer till vissa utmaningar som kortfattat beskrivs nedan.

Marknadslösningar
Marknadslösningar i form av avreglering, privatisering, bolagisering och köp- och säljsystem inom offentlig förvaltning (New Public Management) har skapat nya spelregler för arbetet före, under och efter en allvarlig händelse vilket förutsätter ett nytt förhållningssätt till inriktning och styrning av krisberedskapsområdet (se vidare artikel *Från civilt försvar till kontraktsbaserad samhällssäkerhet*). Sammantaget komplicerar denna utveckling den strategiska planeringen av svensk krisberedskap och frågan om avvägning mellan kostnadseffektivitet och ambitionsnivå för krisberedskapen markeras allt tydligare.

Prioritering av resurser till samhällsviktig verksamhet
Inte sällan råder det oklarheter kring vilka resurser som faktiskt finns tillgängliga när flera aktörer med samma leverantörer drabbas vid en omfattande störning. Samtidigt anger flera myndigheter att det såväl under en allvarlig händelse som i återställningsarbetet finns behov av en ordning som möjliggör prioritering av samhällsviktig verksamhet, exempelvis inom sektorn elektronisk kommunikation. Hur ska den nationella nivån förhålla sig till det av myndigheterna ofta angivna behovet av prioriteringar?

Personalförsörjning
Ett problem kopplat till personalförsörjningen och förmågan att upprätthålla en god krisberedskap är bristande återväxt inom vissa yrkesgrupper, exempelvis inom ingenjörsyrket. Ett annat problem gäller det expertstöd som finns på många myndigheter. Många experter är inte integrerade i krisberedskapsarbetet på ett systematiskt sätt. De finns tillgängliga under ordinarie arbetstid, men under övrig tid är myndigheterna som efterfrågar expertstöd beroende av experternas välvilja och frivillighet. Också vad gäller expertstöd kan prioriteringar enligt ovan bli nödvändiga.

Informationsfunktioner
Att uthålligt och dygnet runt kunna hämta in, hantera, samverka kring och leverera information kräver en adekvat personalstyrka, numerärt och kompetensmässigt. Samverkan kring information är en grundbult i det svenska krisberedskapssystemet och de brister som myndigheterna redovisar vad gäller information och kommunikation torde få negativa återverkningar genom hela systemet vid en allvarlig händelse.

Sociala hot och risker
Sociala hot och risker är ofta kopplade till upplevda eller reella sociala klyftor. Social oro kan uppstå till följd av upplevda kränkningar, motsättningar, och/eller utanförskap bland människor som kan yttra sig i skadegörelse eller hot och våld mot myndighetspersonal samt leda till ökad belastning på samhällsviktiga verksamheter och hota samhällets grundläggande värden. Sociala faktorer kan också bidra till kriminalitet. Sociala hot och risker, kriminalitet och organiserad brottslighet behandlas alltmer frekvent i myndigheternas risk- och sårbarhetsanalyser. Sådana hot och risker ställer också krav på omfattande tvärsektoriell samverkan mellan olika myndighetsområden.

Kärnkraft
Länsstyrelsernas beredskapsplanering för omedelbara åtgärder vid haverilarm bygger delvis på ett trettio år gammalt synsätt och följer inte helt den internationellt rekommenderade standarden. Mot bakgrund av detta och andra faktorer anses en översyn vara nödvändig. I flera myndigheters risk- och sårbarhetsanalyser har frågan aktualiserats i hög grad med anledning av händelsen i Fukushima. Vidare kommer inom de närmaste åren specialistkompetenser att försvinna genom pensionsavgångar. Det finns därför

behov av en målmedveten och strategisk satsning på utbildning och återväxt av nya specialister.

Avslutande reflektion

Efter att ha redovisat en sammanställning av myndigheternas risk- och sårbarhetsanalyser och lyft några utmaningar, ger författarna här en avslutande personlig reflektion över resultatet. Analyserna utvecklas och förbättras över tiden. De håller generellt god kvalitet och medger ofta olika jämförelser. Listan över hot, risker, sårbarheter och beroenden blir dock allt längre. De traditionella hoten, riskerna, sårbarheterna och beroendena kvarstår som centrala i myndigheternas analyser samtidigt som nya tillkommer. Oavsett utvecklingen bedöms förmågan årligen som *god med vissa brister*. Att risk- och sårbarhetsanalyserna inte på ett mer påtagligt sätt föranleder förändringar av den generella förmågan väcker frågor. Att risk- och sårbarhetsanalyserna heller inte i till synes tillräcklig omfattning omsätts i, strategiska och operativa, konkreta åtgärder väcker också frågor. Samhället utvecklas förvisso i en mer komplex riktning, men oaktat detta förhållande föreligger svårigheter att urskilja var och hur framsteg har gjorts avseende krisberedskapen och därmed också hur framtida inriktning och styrning ska genomföras.

”Vår beredskap är god – med vissa brister” torde han ha sagt idag, Per Albin, där på Skansen.

4 FORSA-modellen: Ett verktyg för att analysera risker och hot

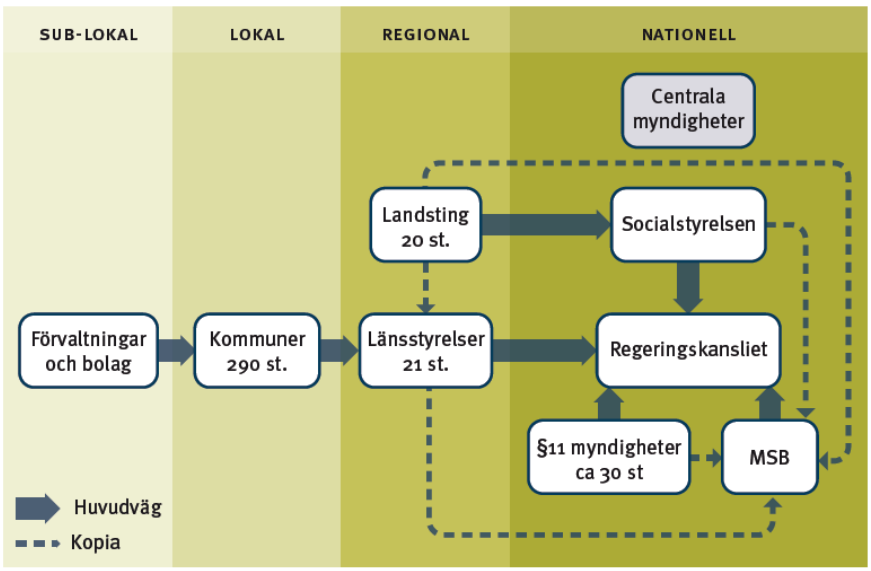
Björn Nevhage

Att genomföra en kvalificerad risk- och sårbarhetsanalys för en organisation, till exempel en kommun, är oftast en komplicerad och tidskrävande arbetsuppgift som förutsätter en genomtänkt metodik att utgå ifrån. I den här artikeln belyses arbetet med risk- och såbarhetsanalyser i Sverige och FORSA som är en modell för risk- och sårbarhetsanalyser som har utvecklats vid FOI.

Risk- och sårbarhetsanalys (RSA) i Sverige

Risk- och sårbarhetsanalys (RSA) är en central del i arbetet med samhällets krisberedskap. Analyserna belyser myndigheternas största risker och beskriver hur väl rustade de är för att hantera eventuella oönskade händelser. Förutom en riskanalys inkluderar en RSA – som namnet antyder – också en sårbarhetsanalys; vilket innebär att myndigheterna också bedömer hur en viss störning påverkar deras verksamhet. Sårbarhetsanalysen är ett viktigt steg där man utreder hur motståndskraftig, eller resilient, en organisation är. En resilient verksamhet upprätthåller en kontinuitet i sin verksamhet oavsett störning.

Ytterst beslutar regeringen, genom lagar och förordningar, *vad* berörda aktörer inom krisberedskapsområdet analyserar och rapporterar. Myndigheten för samhällsskydd och beredskap (MSB) är av regeringen utnämnd ansvarig myndighet inom området RSA och föreskiver sedan år 2010 i detalj vad myndigheterna ska rapporterar in. Figur 1 visar hur RSA-arbetet i Sverige är uppbyggt samt rapporteringsvägar genom hela krisberedskapssystemet (från lokal till nationell nivå).



Figur 1. RSA-kedjan i Sverige. Med § 11 myndigheter avses myndigheter med särskilt utpekat krisberedskapsansvar enligt beredskapsförordningen (2006:942). Därtill tillkommer myndigheter som särskilt utpekas av Myndigheten för samhällsskydd och beredskap.

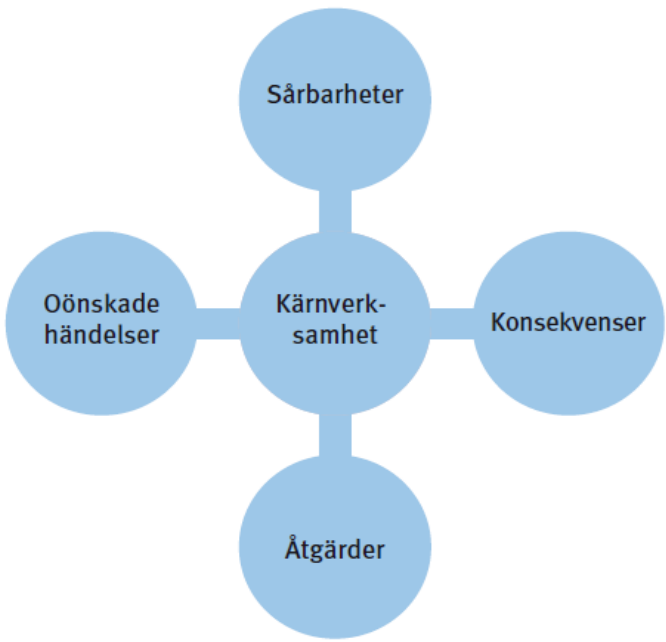
Det framgår dock inte i figuren att informationsutbytet mellan nivåerna sker i båda riktningarna. Tanken med RSA-kedjan är att verksamheterna för det första bidrar med information uppåt i systemet och för det andra tar tillvara på information och underlag nedifrån. Syftet med systemet är att aktörerna tillsammans potentiellt åstadkommer mer än var och en för sig själv. Därför är det viktigt att aktörerna tar fram sina RSA:er på ett likartat och jämförbart sätt; med liknande metoder och arbetsformer och att de analyserar samma händelser. Det generar en bra helhetsbild av riskerna och sårbarheterna på de olika nivåerna, vilket utgör en grund för diskussion och samarbete genom hela krisberedskaps-systemet, vilket i sin tur är en förutsättning när man tar fram en nationell riskbild.

Detta samarbete kan liknas vid att aktörerna tillsammans lägger ett pussel där varje pusselbit representerar en aktörs ansvarsområde och hantering i händelse av en oönskad händelse eller kris. Om en aktör inte gör sin RSA på ett tillräckligt

tillförlitligt sätt representerar denna pusselbit inte den verkliga situationen, vilket gör att pusslet inte går ihop. Ett gemensamt språkbruk och gemensamma modeller för RSA reducerar sannolikheten att pusslet inte går ihop. Föreskrifter och vägledningar beskriver alltså *vad* beslutsfattare och exempelvis säkerhetsamordnare analyserar i systemet, men de behöver ofta stöd i *hur* de rent konkret lägger upp RSA-processer. FOI har därför utvecklat en modell (och arbetsform) för detta arbete, FORSA, som syftar till just detta.

FORSA - FOI:s modell för risk- och sårbarhetsanalys

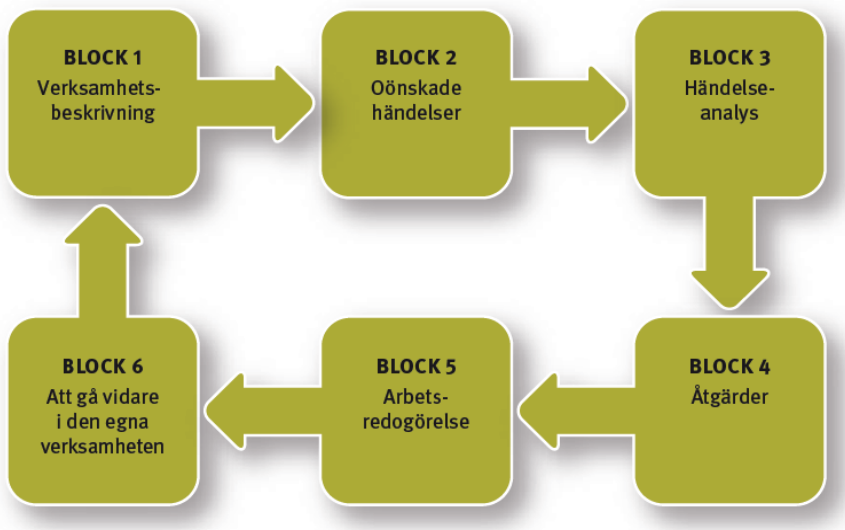
FORSA utvecklades till största del under åren 2007-2010 inom ramen för ett projekt där FOI stöttade Stockholm stad i deras riskhantering. En viktig utgångspunkt för FORSA är att den fokuserar på en aktörs kärnverksamhet (se tankemodell i figur 2); vilket utgör en myndighets, företags eller annan aktörs huvudsakliga uppgifter. Tankemodellen bygger sedan på att en rad olika oönskade händelser potentiellt påverkar kärnverksamheten. Beroende på hur sårbar en verksamhet är leder denna påverkan till mer eller mindre allvarliga konsekvenser. Om man anser att konsekvenserna är oacceptabelt höga måste man sätta in åtgärder som reducerar kärnverksamhetens risknivå.



Figur 2. Tankemodellen i FORSA

FORSA-modellen är ett förslag på hur en verksamhet (myndighet etc.) utifrån den ovan illustrerade tankemodellen lägger upp sitt RSA-arbete. FORSA är således inte bara en modell utan även ett förslag på en arbetsgång, vilket illustreras i figur 3 som visar FORSA-modellen i sin helhet. Den beskrivs vidare i en handbok till stöd för beslutsfattare som ansvarar för att ta fram RSA-rapporter och förslag på åtgärder som minskar riskerna och sårbarheterna[1]. Därför är FORSA enkel och pedagogisk samtidigt som den bygger på vetenskapligt vedertagna teorier och resultat. Beslutsfattare får genom modellen en bättre förståelse för sin verksamhets sårbarheter och den utgör ett stöd för dem i sitt beslutsfattande rörande hanteringen av dessa sårbarheter.

FORSA är applicerbar på alla typer av verksamheter, trots att terminologin främst riktar sig till offentliga aktörer såsom kommuner, landsting, länsstyrelser och centrala myndighetet. Några av dem som idag använder modellen är Stockholms stads samtliga bolag och förvaltningar, Stadledningskontoret i Stockholms stad och FOI. De här verksamheterna skiljer sig mycket åt och befinner sig på olika nivåer (lokal-regional-nationell) i krisberedskapssystemet, men modellen fungerar trots detta för samtliga. Flera andra myndigheter och några privata aktörer håller just nu på att implementera FORSA i sina verksamheter.



Figur 3. FORSA-modellen i sin helhet. Modellen består av sex arbetsblock (Block 1-6 i figuren).

[1] Winehav, M. & Nevhage, B. FOI:s modell för risk- och sårbarhetsanalys (FORSA). 2011. FOI-R--3288--SE.

FORSA består av sex arbetsblock (se figur 3) som tillsammans borgar för en RSA-rapport av god kvalitet. Syftet med respektive block i FORSA är att besvara ett antal frågor som sedan utgör underlag till nästa block i modellen. Upplägget i arbetsblock, med tillhörande förslag på medverkande befattningshavare etc., underlättar för den som genomför en RSA. Om personer med rätt mandat och kompetenser är med i processen skapar det acceptans för arbetet, samtidigt som det sprider information om risker och sårbarhetet i en verksamhet.

FORSA är inte den enda modellen för RSA i Sverige. Några andra exempel är IBERO (instrument för beredskapsvärdering av områdesansvar), MVA (mångdimensionell verksamhetsanalys) och ROSA. Modellerna skiljer sig åt på några punkter[2]. De fokuserar på olika delar i en RSA, riktar sig till olika typer av verksamheter och resulterar i olika typer av resultat. FORSA-modellen lämpar sig för samtliga nivåer (lokal-regional-nationell) i RSA-kedjan (se figur 1) vilket andra modeller inte gör. Övriga modeller är främst framtagna för aktörer med ett geografiskt områdesansvar på lokal (kommuner) och regional nivå (länsstyrelser). Dessutom finns för FORSA som nämnts en handbok med en detaljerad handledning som är direkt kopplar till MSB:s föreskifter för RSA, vilket de andra modellerna inte har.

Framtidsfrågor för arbetet med risk- och sårbarhetsanalys

Som avslutning ska det här pekas på några framtidsfrågor när det gäller arbetet med risk- och sårbarhetsanalyser. För det första, det räcker inte med att myndigheter analyserar och hanterar sina risker och sårbarheter. Riskreducering i samhället måste involvera både offentliga och privata aktörer. Gemensamma risk- och sårbarhetsanalyser (RSA) som privata och offentliga aktörer tar fram tillsammans är eftersträvansvärt och till med nödvändigt för samhällets krisberedskap i det långa loppet. Privata aktörer (både i Sverige och utomlands) äger och driver mycket av vår samhällsviktiga verksamhet. Det finns därför starka globala beroenden, vilket innebär nya utmaningar för svensk krisberedskap och arbetet med risk- och sårbarhetsanalyser.

För det andra är gemensamma RSA-modeller, för såväl offentliga som privata aktörer, nödvändiga för att tillförlitligt kunna jämföra RSA-analyser. Aggregering (sammanvägning) av olika analyser är nämligen oftast problematisk och förenad med hög osäkerhet. Det är lätt att det blir fel, att riskbilden inte stämmer, särskilt om man inte beaktar analysernas förutsättningar och osäkerheter. En felaktig sammanvägning av analyser leder till att man underskattar eller överskattar risken, vilket i värsta fall leder till ineffektiva

[2] Winehav, M. & Nevhage, B. FOI:s modell för risk- och sårbarhetsanalys (FORSA). 2011. FOI-R--3288--SE.

åtgärdsförslag då man inte uppnår en lika hög reducering av risken i jämförelse med om man lägger samma resurser på en mer effektiv åtgärd.

Vidare läsning

- Winehav, M., Nevhage, B. FOI:s modell för risk- och sårbarhetsanalys (FORSA). 2011. FOI-R--3288--SE.

5 Nationell risk- och förmågebedömning

Ester Veibäck

Scanpix: Mark Earthy

I denna artikel belyses det nystartade svenska arbetet med en nationell risk- och förmågebedömning inom ramen för Europeiska unionens (EU) gemensamma säkerhet och krisberedskapsarbete. Inom EU deltar Sverige och övriga medlemsstater i ett allt mer utvecklat gemensamt säkerhet- och krisberedskapsarbete. Det gemensamma arbetet har bland annat resulterat i att Europeiska kommissionen har utvecklat en övergripande säkerhetsstrategi för EU, som bland annat ger ett ramverk för hur kommissionen och respektive medlemsstat ska arbeta med att förebygga och förhindra att katastrofer uppstår. Mot denna bakgrund inbjöds samtliga medlemsstater 2011 att genomföra nationella riskbedömningar och att inrapportera dessa till kommissionen.

Ramverket och medlemsstaternas nationella riskbedömningar ska leda till en ökad gemensam förståelse av risker och hot inom EU och i slutändan resultera i förslag på åtgärder som minimerar konsekvenserna av en katastrof. Katastrofer inkluderar i detta fall både naturkatastrofer och katastrofer som uppkommer på grund av mänsklig aktivitet. Kommissionens mål är också att bedömningarna ska underlätta samarbete mellan medlemsstaterna och reducera gränsöverskridande risker/oönskade händelser som kan spilla över från en medlemsstat till andra

medlemsstater, till exempel en kärnkraftsolycka som leder till radioaktivt nedfall i flera medlemsstater. Dessutom ska de stimulera till ökad medvetenhet om, och förståelse för, vilka kapaciteter det finns inom EU för att hantera inträffade katastrofer. Medvetenheten och förståelsen ska i sin tur underlätta planering av denna kapacitet.

I Sverige är Myndigheten för samhällsbeskydd och beredskap (MSB) ansvarig för arbetet med den nationella riskbedömningen. MSB har i sin tur givit FOI i uppdrag att utveckla en metod för att genomföra en nationell riskbedömning i Sverige. Metoden som kort ska belysas nedan grundar sig på de av EU-kommissionen framtagna riktlinjer för nationell riskbedömning samtidigt som den anpassats för det svenska krisberedskapssystemet. FOI var djupt involverat i genomfördet av den första nationella riskbedömningen i Sverige, som genomfördes 2012. FOI är också djupt involverad i genomförandet av den pågående nationella risk- och förmågebedömningen för 2013 som innebär en vidarutveckling av 2012 års riskbedömning.

En första nationell riskbedömning 2012

Den första nationella riskbedömningen 2012 resulterade i att 27 särskilt allvarliga händelser identifierades som lämpliga för att ingå i en nationell analys. Dessa 27 händelser baserades främst på myndigheternas risk- och sårbarhetsanalyser från 2010 och 2011, samt ytterligare identifieringsarbete för att hitta gränsöverskridande och ”nya” risker. Av de 27 händelserna valdes sju ut för både utveckling av händelsescenarier och analys utifrån sannolikhet, konsekvens och osäkerhet (i bedömningarna). De sju scenarier som analyserades, med stöd av ett flertal berörda myndigheter, kommuner, landsting och andra organisationer, under 2012 är:

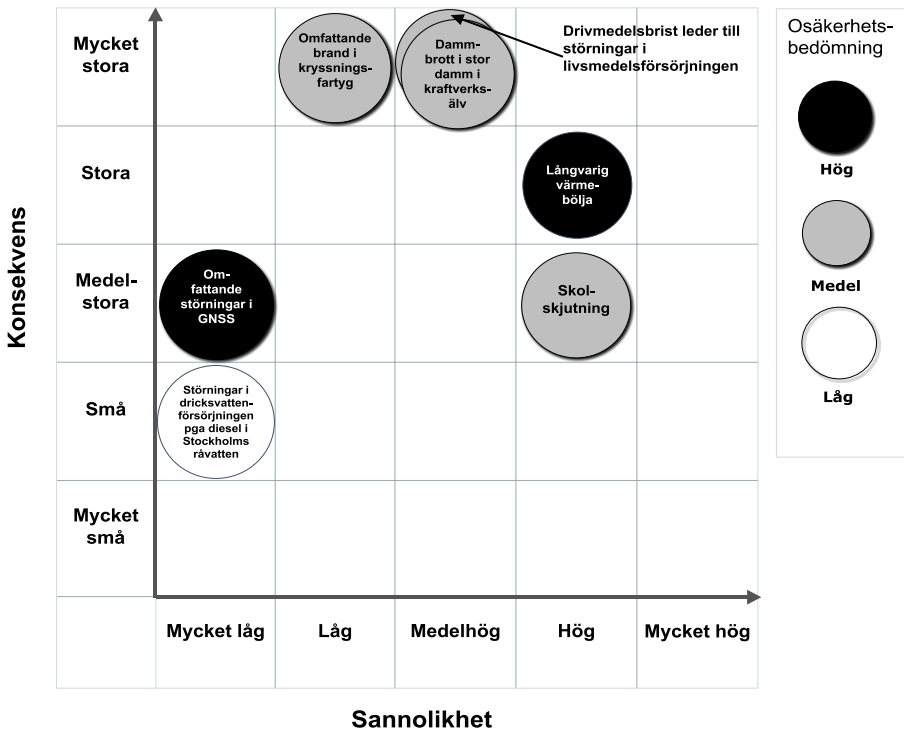
- omfattande störningar i GNSS (Global Navigation Satellite Systems),
- en skolskjutning,
- störningar i dricksvattenförsörjningen på grund av dieselutsläpp i Stockholms råvatten,
- störningar i livsmedelsförsörjningen på grund av drivmedelsbrist,
- en omfattande brand i ett kryssningsfartyg,
- ett dammbrott i en stor damm i en kraftverksälv,
- samt en långvarig värmebölja.

Konsekvenser analyserades i förhållande till de områden som MSB för den nationella riskbedömningen beslutat är det primärt skyddsvärda:

- människors liv och hälsa,
- samhällets funktionalitet,

- demokrati, rättssäkerhet och mänskliga fri- och rättigheter,
- ekonomiska värden och miljön och
- nationell suveränitet.

Av de sju bedömda scenarierna fick följande tre scenarier högst värden vid en sammanvägning av sannolikhet, konsekvens och osäkerhet: 1) drivmedelsbrist leder till störningar i livsmedelsförsörjningen, 2) dammbrott i en stor damm i kraftverksälv och 3) långvarig värmebölja. Den högsta graden av osäkerhet fanns i bedömningarna av scenarierna långvarig värmebölja och omfattande störningar i GNSS. Att osäkerheten i bedömningarna var hög innebär att det fanns ytterst lite data och statistik att grunda bedömningarna på, vilket gjorde att det fanns ett betydande utrymme för fel. När scenarierna placeras in i en riskmatris, vilket förspråkas i EU-kommissionens riktlinjer och regeringens anvisningar, blir bilden som följer:



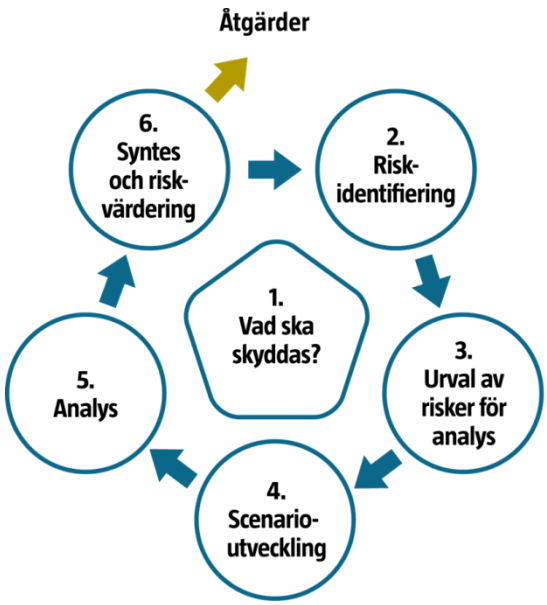
Figur 1: Riskmatris för de analyserade scenarierna i den nationella riskbedömningen 2012. Dessa representerar inte nödvändigtvis de största riskerna i Sverige, utan är de risker som hittills analyserats genom den nationella riskbedömningen. Se vidare rapport MSB-545: Risker och förmågor 2012.

Riskmatrisen ger en översikt av den sammanvägda bedömning som har gjorts för varje händelse. Händelsernas placering i matrisen baseras på de kunskaper som låg till grund för bedömningen. Att kunskapsläget inom de olika områdena som händelserna representerar varierar framgår av osäkerhetsbedömningen. Fördjupade studier kan leda till att bedömningarna kan komma att ändras.

För varje scenario har konsekvenser och sannolikhet bedömts kvantitativt (i intervall). Skalor för dessa går att finna i rapporten *Risker och förmågor 2012* (MSB-545). Konsekvenserna har bedömts efter de specifika scenarierna, medan sannolikheten gäller för att typhändelsen ska ske någonstans i Sverige (undantaget dricksvatten, där sannolikhetsbedömningen gjorts på det specifika scenariot).

Tillvägagångssätt

För genomförandet av den nationella riskbedömningen 2012 togs en särskild metod fram av FOI. Metoden är under fortsatt utveckling. Den av FOI framtagna metoden och dess olika steg kan beskrivas utifrån figuren nedan och inkluderar sex steg:



Figur 2: Metoden för nationell riskbedömning består av sex steg.

I det första steget (Vad ska skyddas) fastställs vad som är mest värdefullt och därmed skyddsvärt i Sverige, och är utgångspunkt för hela processen. Dessa skyddsvärden som har beskrivits ovan ligger tillsvidare fast och detta steg är

således redan genomfört inför kommande årliga nationella riskbedömningar. I det andra steget (Riskidentifieringen) identifieras händelser som på något sätt kan hota eller orsaka negativa konsekvenser för det skyddsvärda. I det tredje steget (Urval av risker för analys) görs ett urval av risker som ska analyseras eftersom det inte är möjligt att analysera samtliga risker. I det fjärde steget (Scenarioutveckling) utvecklas händelsescenarier för de risker som har valts ut i urvalssteget. I det femte steget (Analys) analyseras händelsescenarierna utifrån sannolikhet, konsekvens och osäkerhet. I det sjätte steget (syntes) dras slutsatser från resultatet av scenarioanalysen, scenarierna presenteras i en riskmatris där scenariernas konsekvenser, sannolikhet och osäkerhet relateras till varandra. Efter att ha identifierat nationella risker är ett slutligt steg att översiktligt identifiera, värdera och prioritera handlingsåtgärder. Utfallet av detta steg ska vara ett stöd för ansvariga aktörer att lättare systematiskt inrikta och styra det svenska krisberedskapsarbetet och påverka det europeiska krisberedskapsarbetet. Detta steg är fortfarande under utveckling.

Utveckling

Under 2013 genomförs den andra nationella riskbedömningen. Denna gång sker det med vissa justeringar och mer fokus på samhällets förmåga att förebygga och hantera eventuella konsekvenser av riskerna i form av störningar och kriser i samhället. Denna andra nationella riskbedömning kommer därför att benämnas *nationell risk- och förmågebedömning.* Den nationella risk- och förmåge-bedömningen kommer i fortsättningen att kompletteras med ett antal analyser årligen, så att riskbilden efter hand blir mer komplett. Följande scenarier kommer med stöd av ett flertal myndigheter att analyseras under 2013:

- Allvarlig pandemi orsakat av influensavirus A/H5N1 (fågelinfluensavirus)
- Terrorattentat i Stockholm stad – bomber på Sergels torg och T-centralen
- Våldsamma upplopp i svenska städer
- Kärnkraftshaveri i Sverige med radioaktivt utsläpp
- Omfattande värmebölja – fördjupad analys

Dessutom utvecklas under året två nya scenarier för framtida analyser: en översvämning till följd av ett kraftigt skyfall och ett scenario där hela södra Sverige drabbas av en farlig svaveldimma efter ett vulkanutbrott på Island.

Arbetet med den nationella risk- och förmågebedömningen kommer också att synkroniseras mer med den i krishanteringssystemet etablerade processen för risk- och sårbarhetsanalys och den särskilda förmågebedömningen som görs samtidigt med risk- och sårbarhetsanalysen och som avser krishanteringsförmåga

och förmåga att motstå störningar i samhällsviktig verksamhet. (se artikel 3 och 4). FOI deltar på uppdrag av MSB för närvarande i ett målbildsarbete som ska resultera i hur ett sådant system skulle kunna se ut. I framtiden kommer det också att behövas ett utvecklingsarbete för att kunna identifiera och analysera ”komplexa” och framtida risker i analysen. Med komplexa risker avses sådana som kommer smygande, där konsekvenserna kommer efter viss fördröjning, eller där orsakssambanden är icke-linjära. (se artikel 7). Ett ytterligare utvecklingssteg i framtiden kommer att vara att inkludera hela hotskalan från olycka till katastrof i denna risk- och förmågebedömning. Metodarbetet inom den nationella riskbedömningen har uppskattats av flera aktörer inom krisberedskapssystemet, som har efterfrågat mer systematik och metodstöd på området.

Vidare läsning

- Risker och förmågor 2012 – Redovisning av regeringsuppdrag om nationell riskbedömning respektive bedömning av krisberedskapsförmåga MSB 545.
- Underlag till nationell riskbedömning 2012 – Resultat från den svenska nationella riskbedömningen 2012 FOI-R--3612--SE.

INTERVJU

6 EU:s betydelse för svensk krisberedskap

Intervju med Eva Hagström Frisell

*Fyra frågor till **Eva Hagström Frisell** som är förste analytiker med fokus på Europeiska unionens (EU:s) gemensamma säkerhets- och försvarspolitik, EU:s krisberedskapsarbete samt internationella insatser. Hon är projektledare för projektet Atlantisk säkerhet och europeisk krishantering. Under 2012 analyserade Eva utvecklingen av EU:s krishanteringsförmåga på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB).*

Varför är EU-dimensionen viktig för svensk krisberedskap?

– Under de senaste dryga tio åren har ett omfattande samarbete växt fram inom EU för att förebygga och hantera naturkatastrofer, terrorism och tekniska olyckor. Detta samarbete har stor betydelse för svensk krisberedskap eftersom många av dagens hot och risker är gränsöverskridande. En stärkt beredskap inom EU kan förhindra att kriser sprider sig till oss. Vid en krissituation kan vi också få erbjudande om förstärkningsresurser från andra EU-länder. Det finns utvecklade moduler för till exempel pumpning med hög kapacitet, vattenrening, bekämpning av skogsbränder, sök och räddning, sjukvård, upptäckt och provtagning samt sök och räddning i kemisk, biologisk, radiologisk och nukleär miljö. Det största mervärdet är dock att EU-samarbetet genom utarbetandet av gemensamma riktlinjer, erfarenhetsutbyte och övningar stärker de enskilda medlemsländernas krishantering.

Vad är på gång inom EU just nu?

– När Lissabonfördraget trädde i kraft 2009 skapades nya förutsättningar för EU:s krisberedskapsarbete på många områden. Sedan dess har bland annat Generaldirektoratet för humanitärt bistånd och civilskydd (DG ECHO) stärkt sin roll. Dessutom har ett nytt lagförslag om civilskydd förhandlats fram under våren 2013. Centrala delar i detta förslag är att alla medlemsstater ska göra nationella hot- och riskbedömningar, att en gemensam insatskapacitet ska skapas inom EU genom en frivillig resurspool samt att ett förstärkt centrum för katastrofberedskap

ska byggas upp inom DG ECHO. Därutöver kommer det att finnas möjligheter att erhålla utökad finansiering från EU när det gäller transport av förstärkningsresurser samt utveckling av förmågor som saknas i medlemsstaterna. I Lissabonfördraget finns därtill den så kallade solidaritetsklausulen som befäster medlemsstaternas gemensamma politiska åtagande att bistå varandra vid kriser och katastrofer. För närvarande pågår diskussioner inom EU om klausulens praktiska genomförande.

Hur kan Sverige påverka den framtida utvecklingen inom EU?

– Sverige har deltagit aktivt i utvecklingen av EU:s krisberedskapsarbete och bland annat satt ökad fokus på det förebyggande arbetet. Eftersom det finns olika visioner för EU-samarbetet i olika delar av Europa är det viktigt för Sverige att ha en tydlig målsättning för vilken roll EU ska spela i kris- och katastrofhantering och vad som sköts bäst nationellt eller inom andra internationella organisationer, till exempel FN. Sverige har också ett intresse av att EU utvecklas på ett effektivt sätt och undviker att duplicerande eller konkurrerande strukturer byggs upp inom organisationen.

Vad har FOI gjort på området?

– Forskare vid FOI Försvarsanalys har i mer än tio år följt utvecklingen av EU:s kris- och katastrofhanteringförmåga på uppdrag av olika uppdragsgivare, bland andra Försvarsdepartementet och MSB. År 2009 publicerade FOI tillsammans med Springer förlag en bok om EU:s krisberedskapsarbete: *Crisis Management in the European Union, Cooperation in the Face of Emergencies*. I rapporten *EU och krishantering – strategiska frågor för MSB* från 2012 behandlas den senaste utvecklingen inom EU för att kunna identifiera vilka strategiskt viktiga frågor MSB behöver bevaka de närmaste åren.

7 Komplexa risker – utmaningar för samhällets riskbedömning

Malin Mobjörk

En hörnpelare i svensk krisberedskap är arbetet med risk- och sårbarhetsanalyser, vilket sker på olika nivåer och inom olika sektorer i samhället (se artikel 3,4 och 5). Arbetet med att identifiera och bedöma risker i samhället inrymmer dock många utmaningar. En sådan utmaning är svårigheterna att identifiera och bedöma vad som kan benämnas ”komplexa” risker. I denna artikel sätts fokus på vilka utmaningar komplexa risker ställer på riskbedömningar i samband med risk- och sårbarhetsanalyser samt hur dessa bedömningar ska kunna utvecklas så att de bättre förmår hantera aktuella utmaningar.

Riskbedömning – en kontextberoende process

I en konventionell ansats till riskbedömning sätts fokus på sannolikheten för att en händelse ska inträffa och dess negativa konsekvenser. Risk förstås därmed som funktionen mellan sannolikhet och konsekvens. Eftersom en sådan ansats är inriktad mot en statistisk analys för att en viss händelse ska inträffa i kombination med en kvantitativ analys av dess konsekvenser förutsätts tillgång

till data i fråga om både sannolikhet och konsekvenser. Båda dessa delar medför olika typer av utmaningar i riskbedömningen.

Sannolikhetsbedömningen förutsätter exempelvis att händelsen inträffar relativt ofta, vilket innebär att händelser som sker sällan, eller som ännu inte har inträffat, inte behandlas på ett korrekt sätt. Konsekvensanalysen, å andra sidan, tar utgångspunkt i att det föreligger ett nära samband mellan händelse och konsekvens. Konsekvensanalysen innebär även att ett urval av konsekvenser görs vilka sätts i fokus för analysen. Förlust av liv, ekonomisk skada och påverkan på det demokratiska samhället utgör tre konsekvenser som ofta ligger till grund för konsekvensanalysen. Att sätta just dessa faktorer i förgrunden innebär emellertid att ett val har gjorts och detta val speglar värderingar om vad som anses vara centralt i en riskbedömning. Ett viktigt bidrag från sociologisk riskforskning har varit att uppmärksamma att det är just *val* som är gjorda och att vi alltså kan göra andra val och därmed komma fram till andra slutsatser om både vad som utgör risker och hur allvarliga dessa är.

Att ”risk” i grunden är något relativt och kontextberoende är i sig inte kontroversiellt. Det svenska arbetet med nationell risk- och förmågebedömning, vars analysmodell presenterades i artikel 5, utgår exempelvis från att det första steget i analysen utgörs av att bestämma *vad* som är det skyddsvärda och det andra steget att identifiera vad som hotar detta skyddsvärda. Att identifiera och värdera hot påverkas emellertid av vilka metoder som används liksom hur bedömarna förhåller sig till olika slags risker, vilken acceptans eller tolerans bedömarna har samt vilken grad av osäkerhet som accepteras.

Sätter vi fokus på att göra en sannolikhetsbedömning för en viss händelse så förutsätts tillgång till statistik för händelsen, vilket i sin tur förutsätter att det är en händelse som inträffar relativt ofta. Nästa steg i analysen, konsekvensanalysen, bygger i sin tur på att det föreligger en förhållandevis nära relation – idealt sett ett orsak-verkan-förhållande – mellan händelsen och dess konsekvenser och att det finns god kännedom om vilka sårbarheter som finns. Även detta förutsätter tillgång på kunskap om denna relation liksom att händelse och konsekvens är förhållandevis nära i tid.

Alla risker passar emellertid inte in i denna beskrivning. Det är långt ifrån en likartad grupp händelser vi talar om, vilket leder till att det finns stora skillnader i fråga om varför de skiljer sig åt, vilket i sin tur också har betydelse för hur vi kan förvärva kunskaper om dem. Gemensamt för dem är att de grundar sig i komplexa strukturer, vilka inbegriper indirekta och icke-linjära effekter som innebär att såväl osäkerheten kring en händelses faktiska inträffande, som konsekvenserna av densamma, är stor. Händelserna utmärks även av tvetydigheter i fråga om huruvida de är att betrakta som risker. Ytterst handlar det alltså om att det kan råda oenighet om vilka tolkningar som är korrekta. Även om dessa risker, vilka här benämns ”komplexa” risker, har inbördes olika kvalitativa skillnader kan man särskilja dem som grupp från de risker som sker

ofta och där orsak-verkan-förhållandet är känt, vilka i sin tur benämns ”enkla” risker. För både enkla och komplexa risker utgör värderingar en viktig del och båda formerna beror också av social och kulturell kontext. Den stora skillnaden utgörs dock av att kunskaperna om riskerna skiljer sig väsentligt åt och tolkningsutrymmet är generellt sett större för komplexa risker. Detta har betydelse inte bara för hur en korrekt riskbedömning ska göras utan även för vilka angreppssätt som kan vara fruktbara.

Olika former av komplexa risker

För att kunna förbättra förmågan att bedöma komplexa risker kan det vara viktigt att beakta vilka olikheter som finns dem emellan, det vill säga på vilka olika sätt de utmanar vår förmåga att förvärva kunskaper om dem. Tre olika karaktärsdrag kan urskiljas som visar på kunskapsrelaterade utmaningar, de är komplexitet, vetenskaplig osäkerhet och socio-politisk tvetydighet.

Det första karaktärsdraget – **komplexitet** – syftar på såväl möjligheten att identifiera en händelse på förhand som möjligheten att kvantifiera de bakomliggande orsakssambanden. Till stor del beror denna komplexitet på en icke-linjär relation mellan orsak och verkan, det vill säga att effekterna blir synliga först i andra eller tredje led. Det finns olika faktorer bakom denna komplexitet. Två centrala aspekter utgörs av eftersläpningsperiod och återkopplingsmekanismer.

Med *eftersläpningsperiod* avses att det föreligger en fördröjning från att en händelse inträffar till att effekterna synliggörs. Ett exempel på sådana eftersläpande effekter kan ses i användandet av akrylamid, ett vanligt ämne i industriproducerade färdigrätter, vars hälsoeffekter först identifierades långt efter att människor blivit exponerade. Den andra aspekten utgörs av *återkopplingsmekanismer*, vilka förenklat handlar om att det finns ett antal variabler som påverkar varandra så att mönstret blir oförutsägbart liksom att det även kan bildas kaskadeffekter där olika skeenden förstärks och påskyndar händelseutvecklingen avsevärt. Ett exempel på detta är skogsbränderna i Ryssland 2010 vars spridning ökade markant av den kraftiga blåsten som i sin tur även innebar en ökad spridning av luftföroreningar.

Det andra karaktärsdraget utgörs av **vetenskaplig osäkerhet**. Bristen på data eller bearbetad information utgör ett grundläggande problem för att kunna göra såväl sannolikhets- som konsekvensbedömningar. Förenklat kan man säga att ju mindre data eller observationer man har, desto fler antaganden och uppskattningar krävs för att förklara en händelse eller företeelse.

Ett antal utmaningar kan identifieras med avseende på vetenskaplig osäkerhet. Vad gäller rent statistiska utmaningar kan nämnas att den naturliga variationen bland urvalet kan vara väldigt stor. Detta gäller exempelvis inom

klimatforskningen där avvikelser såsom väderfenomenet El Niño ofta tas med i beräkningar men modelleringen av dess effekter skiljer sig åt. Det kan även finnas slutledningsproblem då en begränsad mängd data extrapoleras (det vill säga ”förlängs”) för att förklara större skeenden eller som i fall då resultat från djurförsök får representera människors respons på mediciner. En tredje utmaning handlar om i vilken mån händelsen kan leda till oförutsägbara effekter, vilka kan bottna i rent slumpmässiga sammanträffanden eller på invecklade men på förhand svåridentifierbara sambandsförhållanden såsom i fallet med kärnkraftsolyckan i Fukushima i Japan.

Det tredje karaktärsdraget som utmärker komplexa risker handlar om **socio-politisk tvetydighet**, vilket handlar om normer och tolkningar om vad som bör betraktas som en risk. Ofta skiljer man mellan tolkningsrelaterad tvetydighet och normativ tvetydighet. Båda dessa utmaningar relaterar till begreppet ”riskkontrovers”, som sätter fokus på den grad av debatt som kan råda i samhället ifråga om en viss händelse är att betrakta som en risk.

Tolkningsrelaterad tvetydighet uppstår då antaganden krävs på grund av otillräcklig data vid riskbedömningen. Framförallt kvalitativa bedömningar öppnar upp för debatt och i dessa har ofta experter tolkningsföreträde, även om dessa i likhet med lekmän också är påverkade av personliga preferenser, moral och olika grupptillhörigheter. Med *normativ tvetydighet* sätts fokus på frågor som tolerans och acceptans liksom hur pass allvarlig en risk ska antas vara för att den ska bli prioriterad. Det kan här handla om olika normer kring livskvalitet, men baseras även på kostnadskalkyler: Är risken värd att ta i relation till den eventuella nytta som kan genereras? Till viss del handlar denna aspekt om att risker kan politiseras och föras fram eller åsidosättas i den offentliga debatten.

De här tre karaktärsdragen – komplexitet, vetenskaplig osäkerhet och socio-politisk tvetydighet – medför olika typer av utmaningar för riskbedömningen. Det är alltså ingen likartad grupp risker vi talar om även om vi använder ett samlingsnamn, komplexa risker. Olikheten återspeglas även i att det finns många olika slags benämningar för olika typer av komplexa risker. De olika benämningarna, som förvisso har åtskilliga beröringsytor, sätter ofta fokus på specifika karaktärsdrag hos riskerna och genom att beakta dessa olikheter kan vi lättare identifiera vari utmaningarna ligger för att analysera dem. Här ska fyra olika begrepp uppmärksamas som ofta används och gör det i ett led för att åskådliggöra var de primära utmaningarna finns för att bedöma riskernas omfattning.

- **Framväxande risker**: Dessa risker saknar historiska data och handlar framförallt om framtida risker. Utmaningar att analysera dem är därför beroende de framtida händelserna i sig liksom framtida sårbarheter och framtida uppfattningar om vad som utgör en risk. Klimatförändringar, förlust av biologisk mångfald och social oro utgör tre slags framväxande risker där vi idag kan identifiera att dessa företeelser kommer att föra med sig risker,

men där vi endast kan ha begränsade kunskaper om exakt på vilket sätt. Utvecklingen är även avhängig samspelet mellan olika faktorer, däribland anpassningsförmåga och samhällsförändringen i stort, vilket försvårar bedömningen.

- **Systemiska risker**: Dessa risker sätter fokus på olika former av beroendeförhållanden inom system liksom på spridnings- och sekundäreffekter över systemgränser. Utgångspunkten för systemiska risker tas ofta i den sårbarhet som uppstår i ett modernt och effektiviserat samhälle. Ett exempel utgörs av samhällets elförsörjningssystem och hur starkt beroende många samhällsfunktioner är av el. Beroendeförhållanden och sammankopplingen mellan olika system ligger även till grund för att många systemiska risker också är fyllda med tvetydigheter i fråga om bedömningen av riskernas omfattning. Sammankopplingen av elförsörjningssystemet i Europa betraktas därför både som en risk genom de beroenden som byggs upp och som en tillgång då dessa beroenden även för med sig positiva effekter, exempelvis genom att främja redundans (reservkapacitet).

- **Sällanhändelser**: För händelser som sker sällan, såsom finanskriser, vulkanutbrott och meteroitnedslag, saknas möjligheten att göra korrekta statistiska analyser. Generellt sett har själva riskuppfattningen stor betydelse för vilka bedömningar som görs och en tendens är att sällanhändelser som precis inträffat överskattas medan de som inte inträffat underskattas. Likaså överskattas ofta även händelser som på kort tid för med sig allvarliga konsekvenser medan händelser vars konsekvenser sker över en längre tidsrymd underskattas. Dessa skevheter i bedömningarna gäller inte bara sällanhändelser, utan risker generellt.

- **Svarta svanar**: Begreppet svarta svanar kommer historiskt av att det togs för givet att alla svanar var vita tills det att svarta svanar upptäcktes i Australien. Begreppet svarta svanar sätter fokus på risken för att vi drar felaktiga slutsatser när de huvudsakligen baseras på teoretiska antaganden utifrån ett begränsat antal observationer och innebär att en enda observation kan ligga till grund för att omkullkasta den rådande uppfattningen. Svarta svanar har applicerats på en rad olika områden däribland finanskriser och den arabiska våren, och åskådliggör en brist som finns i de metoder som används för att bedöma risker. Kärnan i kritiken handlar om att de flesta metoder tar utgångspunkt i en föreställning om att mäta linjära och direkta effekter, men tillämpas för komplexa och dynamiska företeelser där människor lever och interagerar.

För att sammanfatta vad komplexa risker kännetecknas av så handlar det just om komplexitet; komplexitet i fråga om vilka samband som finns mellan olika händelser och mellan händelser och konsekvenser liksom om komplexa relationer mellan olika system. Det här innebär att de kunskaper vi kan ha om komplexa risker alltid är fyllda med stora osäkerheter. En del osäkerheter kan

minskas över tid genom att fler observationer tillkommer eller bättre analysmetoder utvecklas, medan andra osäkerheter är bestående, exempelvis om de bottnar i oförutsägbara effekter. Även om en del osäkerheter alltså kan minskas så kommer osäkerhetsdimensionen till viss del alltid att kvarstå. Detta gör att osäkerhetsfaktorer är en viktig aspekt att integrera i riskbedömningen. Komplexiteten och osäkerheterna ligger även till grund för att tolkningsutrymmet blir större. Härvidlag blir alltså de perspektiv vi utgår från av stor betydelse liksom vilka värderingar som ligger till grund för bedömningen. Själva riskuppfattningen blir därmed en viktig aspekt att beakta.

Hur förbättra möjligheterna till att bedöma komplexa risker?

Vilka är då de största utmaningarna för den konventionella riskbedömningen från komplexa risker? Hur kan riskbedömningen förbättras givet de utmaningar komplexa risker ställer? Dessa två frågeställningar är nära förbundna med varandra. Avslutningsvis ska det därför föras fram ett par aspekter som kan ligga till grund för att förbättra möjligheterna till att bedöma, och därmed även hantera, komplexa risker. Det är ingen uttömmande lista, men den speglar olika reflektioner gjorda i artikelförfattarens egna och i andras arbeten med att analysera, bedöma och hantera komplexa risker.

Att det föreligger osäkerheter i riskbedömningen är en självklarhet och de flesta riskbedömningar inkluderar att osäkerheten, eller tillförlitligheten, ska beaktas. Det fokus som idag finns på sannolikhet och konsekvens tenderar emellertid att medföra att osäkerheterna reduceras för att bättre passa in i den analysmodell som präglar riskbedömningen. Detta görs exempelvis genom att avgränsa analysen i tid och rum, vilket underlättar möjligheterna att analysera konsekvenserna av en händelse men som innebär att eftersläpningseffekter eller indirekta effekter inte uppmärksammas. Genom fokus på kvantitativa beskrivningar tonas även de värderingsmässiga delarna i riskbedömningen ned. Ett sätt att förbättra osäkerhetsbedömningen kan vara att strukturera osäkerheterna och beakta vad som ligger till grund för osäkerheterna. Några centrala aspekter utgörs av:

- *Utbredning*: här ligger tonvikten på att analysera vilka konsekvenser en händelse får i rummet. Det handlar dels om att inbegripa effekter även om de går utanför geografiskt administrativa gränser, dels om att undersöka spridning av skadliga effekter mellan människor (eller de ting som står i fokus för analys).
- *Påverkanstid:* fokus här ligger på att analysera distributionen av de negativa effekterna över tid, vilket innebär att fördelningen mellan generationer ska tas med i beaktande.

- *Irreversibilitet:* analysen ska även omfatta riskerna med irreversibla, det vill säga återkalleliga, effekter, vilket inkluderar en analys av möjligheterna för systemet att bli återställt till sitt ursprungliga tillstånd.
- *Eftersläpning:* sätter fokus på vilken fördröjning som kan finnas mellan att en händelse inträffar till dess att effekterna blir synliga. Fördröjningen kan bero på allt från lång reaktionstid hos bedömare, långsam utveckling av skeenden eller på grund av intrikata beroendekedjor vilka påverkar varandra så att effekter först framträder när de är av större omfattning.
- *Möjligheter till mobilisering:* mobilisering innebär vilken acceptans eller tolerans som individer eller samhällen har liksom vilken potential det finns för att få individer att agera på ett annat sätt. Denna aspekt är särskilt viktigt för risker som utmärks av kontroverser i fråga om vilka bedömningar som är gjorda.

Förutom dessa fem dimensioner kvarstår betydelsen av att bedöma en händelses sannolikhet och konsekvens liksom tillförlitligheten i dessa bedömningar. Förtjänsten med de fem dimensionerna är att de kan användas för att strukturera beskrivningen av osäkerheterna och därmed synliggöra var kunskapsbrister finns. Detta kan i sin tur leda till att underlätta identifiering av om det är kunskapsbrister som kan reduceras genom analys eller om det är inneboende osäkerheter som vi helt enkelt bara måste förhålla oss till. En följd av dessa olikheter i fråga om hur bedömningarna är gjorda – på vilka kunskapsgrunder – handlar om hur olika risker bör presenteras och kommuniceras.

En annan central aspekt som är utmärkande för komplexa risker är betydelsen av riskuppfattning och de olika tolkningar och uppfattningar som finns ifråga om risker. Eftersom olika perspektiv och tolkningar har betydelse så blir det viktigt att bredda perspektiven. Utgångspunkten är helt enkelt att en mer mångfacetterad beskrivning av vilka risker som finns och hur allvarliga de bedöms vara är positivt för den samlade riskbedömning som behöver göras där olika risker kan värderas och jämföras med varandra. Det handlar därmed om att bredda vilka aktörer som ingår i riskbedömningsprocessen och att aktivt föra in personer med olika perspektiv såväl som social och kulturell bakgrund.

Ett tredje aspekt handlar om hur vi kommunicerar och presenterar risker där en vanlig form i dag utgörs av en riskmatris som åskådliggör olika risker givet dimensionerna sannolikhet, konsekvens och osäkerhet. Med denna tvådimensionella modell reduceras den dynamik som har legat till grund för bedömningen där olika risker är bedömda på olika kunskapsgrunder och är förknippade med olika slags osäkerheter. Det kan här finnas anledning att undersöka hur en mer dynamisk presentationsform skulle kunna se ut som ett led i att främja möjligheten till mer tillämpliga och korrekta jämförelser mellan olika slags risker.

Ett fjärde sätt, vilket föregår själva riskbedömningen, är att se över hur risker identifieras. Det handlar om att öppna upp rummet för vilka perspektiv som får ta plats i riskidentifieringsprocessen, men även om vilka olika metoder som kan användas. I expertpaneler, som många gånger används för att identifiera risker vi vet lite om, blir just mångfald i perspektiv en viktig del. För åtskilliga systemiska risker, som till exempel avancerade tekniska system, kan det i stället handla om att analysera beroendekedjor och identifiera kritiska delar i systemet. Denna analys kan både lägga grund för vad som kan omkullkasta de kritiska flödena, men också vilka indirekta effekter som kan följa om något kritiskt flöde stryps. För risker präglade av kontroverser, det vill säga av olikheter i vilka bedömningar som är gjorda, kan det i stället vara viktigt att studera just riskkontroversen. Det handlar alltså om att systematiskt analysera vad kontroversen utgörs av och strukturera analysen och visa var skiljelinjer finns, vilket i sin tur kan ligga till grund för att bättre kunna avgöra vad skiljelinjerna bottnar i.

Avslutningsvis, ett alternativt till riskanalys är att analysera vilka sårbarheter som finns i samhället. Detta kan exempelvis göras med hjälp av beroendekedjor eller genom kvalitativa bedömningar beroende på vad i samhället som står i fokus för analys. Att just sätta fokus på sårbarhet kan vara en viktig del för att främja förebyggande arbete och åtgärder som kan fungera mot olika typer av utmaningar. Givet de osäkerheter som finns i många, framförallt komplexa, risker så kan helt enkelt inte krisberedskapssystemet utformas för att kunna svara mot en bestämd uppsättning risker, utan en öppnare och mer flexibel ansats behövs. Härvidlag kan själva grundansatsen i utformningen av politiken behöva förändras så att krisberedskapssystemet som idag tenderar att vara reaktivt utvecklas till att bli mer proaktivt. Att utgå från sårbarhetsanalys, tillämpa försiktighetsprinciper (om till exempel osäkerhet föreligger om ett ämnes farlighet skall det betraktas som farligt) liksom att arbeta med kombinationen explorativa scenarier som utforskar olika framtider samt förvarning kan i sammanhanget bli en viktig utgångspunkt och fungera som ett komplement till den ansats som dominerar dagens krisberedskap.

Vidare läsning

- Sonnsjö, H. och Mobjörk, M. 2013. Om indirekta, komplexa och oönskade händelser: Att analysera risker med stor osäkerhet. FOI-R--3649--SE.
- Winehav, M. m fl. Förslag till metod för nationell riskbedömning. Resultat av metodutveckling 2011-2012, FOI-R--3423--SE.
- Klinke, A. & Renn, O. 2012. Adaptive and integrative governance on risk and uncertainty, *Journal of risk research*, 15:3.

8 Konsekvenser av IT-angrepp mot kritisk infrastruktur

David Lindahl

Antag för ett ögonblick att mobiltelefoner skulle sluta fungera. Våra kalendrar och adressböcker finns i dem. Vi är vana att hela tiden kunna nå andra och vara nåbara, men utan mobiltelefonerna försvinner den möjligheten. Vi skulle bli tvungna att ändra vårt beteende på många olika sätt, men det skulle ändå vara praktiskt genomförbart. Det skulle vara enerverande, men inte allvarligt.

Men vad skulle vi göra om elektriciteten försvann? Inte bara en timme, utan flera timmar? Eller i dagar? Hur mycket kontanter har vi hemma? Utan el kan vi inte handla med kort eller ta ut pengar i en bankomat. Belysning, värme och internet fungerar inte längre. Efter något dygn ligger mobiltelenätet nere och batterierna till datorer och telefoner är tömda. Bilar står stilla av bränslebrist. Varor levereras inte till butiker.

Vad skulle vi göra om dricksvattnet stängdes av? Hur många liter flaskvatten måste vi bära upp till våra lägenheter varje dag? Hur mycket vatten finns det i butikerna? Kan Hemvärnet köra ut vatten till alla som behöver det?

Större delen av samhället är idag helt beroende av IT för att kunna fungera. Det är kanske inte ett uttalande som förvånar någon, med tanke på hur viktiga de flesta människor tycker att deras datorer är för dem. Men vad som kanske är mer

förvånande är att det inte är hemdatorerna eller mobiltelefonerna som vi är mest beroende av. *Nästan alla tjänster i samhället* är direkt eller indirekt beroende av datoriserade styrsystem för att fungera.

Under de senaste trettio åren har datorer för styrning, reglering och övervakning av processer i den tekniska infrastrukturen gått från att vara undantag till att vara oundgängliga. Industriella kontrollsystem förekommer i en rad olika processer och industrier, bland annat inom samhällskritiska verksamheter som flygande och spårbunden trafik, produktion och distribution av energi, el, vatten och drivmedel med flera.

För den enskilde individen innebär det här att el, dricksvatten, avlopp, elektroniska kommunikationer, transporter och kortterminaler kan sluta fungera om en framgångsrik datorattack drabbar deras leverantörer. För samhället innebär det att allvarliga påfrestningar och stora kostnader kan bli konsekvenserna om landets kritiska infrastrukturer är sårbara för IT-angrepp i någon större utsträckning.

Exempel 1: Kärnkraftverket Davis-Besse

I januari 2003 kom datormasken Slammer in i datorsystemen hos det amerikanska företaget First Energy. En säkerhetsuppdatering mot masken i fråga hade redan funnits ute i sex månader men företagets datorer hade inte uppdaterats. Masken kom in i nätet eftersom företaget tillät underleverantörer att kringgå brandväggar och andra säkerhetsåtgärder av effektivitetsskäl och direkt koppla in sig på First Energys nätverk.

På bara några sekunder spred sig masken från dator till dator och överbelastade nätverket med trafik. De anställda kunde inte skicka epost, skriva ut dokument, eller ladda ner filer. Även om det var irriterande och kostade pengar i uteblivet arbete var det ändå inte allvarligt.

Vad som var värre var att det fanns en dataförbindelse från First Energys kontorsnät in i kärnkraftverket Davis-Besse. Det var en förbindelse som säkerhetspersonalen på kärnkraftverket inte kände till. Kontorsdatorerna inne i kärnkraftverket hade inte heller uppdaterats, så masken spred sig även där med samma konsekvenser som för huvudkontoret. Men maskens överbelastning hade även en annan effekt. Kärnkraftverkets kontrollrum använde ett datornät sammankopplat med kontorsnätet. Överbelastningen när masken försökte sprida sig ledde till att kontrollrummets primärsystem för styrning kopplades ur under flera timmar.

Hur fungerar SCADA-system?[3]

SCADA (Supervisory Control and Data Acquisition) är specialiserade datorsystem som kontrollerar industriell utrustning.

I takt med att datorerna blivit billigare och mer kraftfulla har människor plockats bort från allt fler industriprocesser. En dator som mäter temperaturförändringar kan reagera snabbare än någon människa och kommer aldrig att somna eller ha en dålig dag. Dessutom, och viktigast, datoriseringen kan minska personalbehovet drastiskt och därmed spara mycket pengar.

Idag styr digitala styrenheter enskilda maskiner, pumpar och andra komponenter. Dessa, så kallade PLC:er (Programmable Logic Controller) eller RTU:er (Remote Terminal Unit), är i praktiken datorer i sin egen rätt. De har operativsystem, kör program och kommunicerar via nätverk, trådbundna eller trådlösa WiFi-nät[4].

För att övervaka och styra fysiska processer i realtid behövs information direkt från de övervakade processerna. En komplicerad industriprocess som idag styrs med SCADA kan omfatta hundratals olika styr- och mätdatorer spridda över stora geografiska områden som samlar in tusentals mätdata per sekund från var och en av hundratals sensorer. Mätdata skickas sedan över internet till den plats där kontrollrummet ligger. Denna kan ligga hundratals kilometer från den fysiska processen som skall styras. Dessa data sammanställs och bearbetas av andra datorer som skickar dessa vidare till skärmar och högtalare för att de övervakande människorna ska få en överblick över processen. Operatörerna fattar beslut och beordrar förändringar i processen via kontrollrummens reglage. Orderna behandlas av systemet, och hundratals styrorder skickas till tusentals olika komponenter som är inblandade i processen. Det kan vara order till ventiler att minska ett flöde med några milliliter per sekund, eller till en turbin att öka effekten med hundratals kilowatt.

Eftersom de kritiska processerna ofta är känsliga för olika former av störningar är det av yttersta vikt att den information som presenteras är korrekt och verkligen visar processens nuvarande och verkliga tillstånd. Lika viktigt är det naturligtvis att de styrorder som sänds genom systemet är korrekta så att styrdatorerna inte försätter systemet i ett osäkert läge.

Fördelarna med SCADA-system är att man kan ha anläggningar utspridda utan att behöva betala dyra pengar för att ha personer på plats som övervakar dem. Man kan även bygga systemen med mycket mindre felmarginaler än man skulle

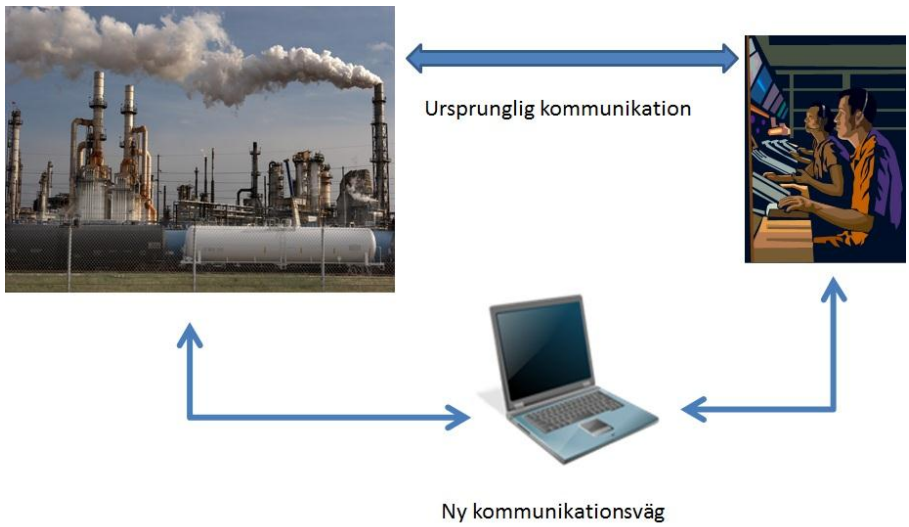
[3] I den här artikeln använder vi termen SCADA i vid bemärkelse. Det vi talar om är alla typer av datorsystem som styr fysiska industriella processer.

[4] Wi-Fi uttyds Wireless Fidelity; Wi-Fi är en teknik för trådlösa datornätverk som baseras på standarden IEEE 802.11.

ha behövt om en människa skulle ha skött maskinerna manuellt, med den brist på precision och hastighet som människor har jämfört med datorer.

Nackdelarna med SCADA är för det första att operatörerna blir beroende av att systemet ger dem korrekt information. För det andra kommer systemet att utföra styrkommandon utan den eftertanke som en människa skulle ha.

Mellan operatörer och process finns det lager efter lager av tekniska system som alla har sårbarheter av olika slag. Det här öppnar upp för en angripare att ta över och styra processerna samtidigt som operatörerna ges information som felaktigt visar att allt är normalt. Detta kallas också för en mannen-i-mitten attack.



Figur 1. ”Man-i-mitten-attack”. Inget av offren inser att de kommunicerar med en bedragare. Angriparen kan därmed lura offren att göra som han vill.

Dagens industriella system kopplas i allt högre grad samman med andra datorsystem och med internet. Det här gör att en angripare kan sitta var som helst i världen och ändå komma åt sitt mål. Att någon vill koppla upp kraftvärmeverk mot internet verkar kanske underligt, men i och med automatiseringens framgångar kan man effektivisera och minska kostnader genom att ha en eller ett par övervaknings-/kontrollcentraler i stället för många lokala. Det är alltså en åtgärd som är tänkt att spara pengar, och för det mesta väljer man då lösningar som är billiga vilket innebär kommersiellt tillgängliga internetlösningar. Dessutom kräver många av de SCADA-system som finns på marknaden att leverantören kan nå dem via internet för att kunna uppdatera programvaran. I många fall är den enda säkerheten ett standardiserat lösenord, samma för alla system av en viss modell.

Exempel 2: Vattenverket i Maroochy Shire

År 2000 fick IT-teknikern Vitek Boden avslag på sin ansökan om att börja arbeta för vattenverket i Maroochy Shire, i Australien. Upprörd över detta beslöt sig Boden, som tidigare hade installerat SCADA-systemen på vattenverket, att hämnas. Han använde sig av sina kunskaper om systemen, stulna radiokomponenter och en laptop för att vid minst 46 tillfällen göra datorintrång på vattenverket och styra processerna för avloppshantering via radio. Resultatet blev utsläpp av över åtta hundra kubikmeter avloppsvatten i lokala parker, vattendrag och i ett fall området utanför ett hotell med stora skador på lokalt djur- och växtliv.

StuxNet - Det första moderna IT-vapnet

Antivirusspecialisten Sergey Ulasen på företaget VirusBlokAda upptäckte i juni 2010 vad han då trodde var en rutinmässig konflikt mellan program på en kunds Windowsdatorer. Det visade sig att han hade gjort en historisk upptäckt. Det han hade hittat skulle komma att kallas StuxNet och det är det första IT-vapen riktat mot kritisk infrastruktur som har hittats utanför laboratorier. Under flera månaders arbete lyckades säkerhetsexperter världen över gradvis pussla ihop hur det fungerade.

Vapnet spred sig från ett vanligt USB-minne[5], in till Windowssystem och vidare från dator till dator genom nätverken tills det hittade en server vars uppgift det var att uppdatera SCADA-utrustning. Väl där tog det över uppdateringsprogrammet och lade till extra programkod i de uppdateringar som installerades på SCADA-systemets datorer. För att få rättigheter att göra detta hade vapnet två digitala säkerhetscertifikat från olika företag som visade att uppdateringen var legitim.

Av det som framkommit verkar målet för attacken ha varit Irans uranupparbetningsanläggning i Natanz. Det som troligen har hänt är att centrifuger som anrikar uran har styrts av en typ av datorutrustning från Siemens. StuxNet har ändrat styrprogrammet i denna utrustning. Styrdatorn har i stället för att hålla en jämn hastighet på centrifugen då och då minskat eller ökat farten till varvtal som orsakat självsvängningar. Detta har lett till att kullager och annan utrustning har gått sönder i stor omfattning vilket i sin tur sannolikt har inneburit stora förseningar i den iranska uranframställningen.

Kapaciteten hos StuxNet är imponerande:

- Det använde sig av minst sex olika sårbarheter för att ta sig in i de olika delsystemen.

[5] USB - Universal Serial Bus, är en teknisk standard för snabb seriell dataöverföring.

- Av dessa sex var fyra helt okända för allmänheten innan angreppet.
- Med tanke på att helt nya sårbarheter av den här kalibern rapporteras endast tre till fyra gånger per år är det väldigt ovanligt att så många finns i ett enda vapen.
- Två digitala säkerhetscertifikat måste ha stulits från olika företag och använts för att kryptografiskt signera vapenlasten. Genom signeringen kunde StuxNet kringgå olika säkerhetssystem i de drabbade dator-systemen.
- Vapnet hade funktionalitet för att skydda sig mot upptäckt medan det sökte sig genom nätverket.
- Dessutom hade det en förmåga att kontakta datorer på internet, i Danmark och Malaysia, dit den kunde skicka underrättelsedata, och hämta ned uppdateringar till sig själv.
- När vapnet slutligen infekterade SCADA-systemen var det konstruerat så att det endast angrep om systemet såg ut på ett mycket specifikt sätt.
- Detta tyder på att vapnet hade byggts för att angripa ett specifikt mål.

De flesta IT-vapen som dyker upp beter sig helt annorlunda: De angriper allt de kan för att infektera så många system som möjligt. De bryr sig inte om skadliga sidoeffekter eller att hitta enskilda mål. StuxNet betedde sig mer som ett militärt sabotageförband. Det tog sig in utan att väcka uppmärksamhet, agerade försiktigt för att inte upptäckas och slog till först när målet var identifierat.

Enligt New York Times (SANGER, 2012) har trovärdiga källor inom USA:s ledning bekräftat att USA och Israel tillsammans har tillverkat och använt StuxNet i vad som påstås ha kallats *Operation Olympic Games*. Det skulle i så fall vara ytterligare en sak som gör StuxNet unikt, nämligen att det är det första bekräftade exemplet på stater som har angripit en annan stat med hjälp av skadlig programvara.

Var StuxNet en engångshändelse?

På världens hackerkonferenser och säkerhetsforum har medvetenheten om SCADA-systemens sårbarhet blivit allt mer spridd. År efter år demonstreras sårbarheter och angreppsmetoder. Detta leder till ett ökat intresse för området, och i förlängningen till en allt högre kompetens hos angriparna. Samtidigt har det skett en utveckling mot cybermiliser och hacktivism runt om i världen. Det vill säga att personer som är politiskt motiverade i allt högre grad utför IT-angrepp för att förändra politiken hos sina meningsmotståndare.

Sättet på vilket SCADA-systemen byggs förvärrar denna situation. De befintliga styrsystemen har mycket lång livslängd och har tillverkats för att köras utan avbrott under många års tid. De är oerhört komplexa och det är vanligt att leverantörerna enbart säljer system under förutsättningen att kunden aldrig ändrar i dem. Normen är att det inte finns några säkerhetsmekanismer över huvud taget för att hantera IT-intrång. Att stänga av och återstarta systemet vid fel är helt uteslutet, eftersom den fysiska processen inte får stoppas när som helst. Resultaten skulle kunna bli allt från överjäst bröd till en explosion i ett raffinaderi.

SCADA-systemen kopplas samman med kontrollrum på stora avstånd via internet med datorsystem som är designade för att till låg kostnad kunna fungera i kontorsmiljö, där omstarter är rutinlösningar på problem och där säkerheten är beroende av ständiga uppdateringar och ändringar.

Resultatet blir hybridsystem där kontorsnätverkens säkerhetsnivå kombineras på sämsta tänkbara sätt med SCADA-systemens åtkomst till fysiska processer. Det behövs nya metoder, både tekniska och organisatoriska, för att kunna skydda systemen som nu växer fram. Samtidigt måste de metoder som finns användas på ett så effektivt sätt som möjligt för att täta de största säkerhetshålen under tiden som branschen mognar.

Vilka konsekvenser skulle ett IT-angrepp kunna få för svensk del?

Det är oerhört svårt att förutsäga vad som skulle bli konsekvenserna av ett IT-angrepp. I nordöstra USA skedde under sensommaren 2003 ett strömavbrott som följd av felkonfigurerade styrdatorer och ett träd som fällde en matarledning. En femtedel av USA:s och Kanadas abonnenter, omkring 55 miljoner människor blev utan el. Delar av tågtrafiken stannade. Dricksvattensystemen i flera städer förlorade tryck och dagvatten kom in i ledningarna så att folk råddes att koka allt vatten. Teletrafiken fungerade oregelbundet. Avbrottet varade i två dygn. Detta var resultatet av en mindre olycka, och en dittills okänd sårbarhet hos styrsystemen. Sårbarheten är nu korrigerad, men hade inte olyckan skett är det troligt att sårbarheten fortfarande hade funnits kvar och kunnat användas av en angripare som systematiskt hade letat upp den. Skulle något sådan kunna hända i Sverige*? Ingen vet.*

Det finns idag heller ingen som egentligen vet hur säkra styrsystemen i kritisk infrastruktur är. I dag drivs stora delar av infrastrukturen av privata företag som agerar för sina ägares intressen. Den kontroll som fanns när statliga verk drev stora delar av infrastrukturen finns inte längre. De beredskapslagar som kunde användas för att tvinga fram investeringar som inte var direkt kopplade till vinst

finns inte längre. Dessutom är vår infrastruktur nu sammankopplad med våra grannländer och därmed beroende av deras infrastruktur.

Framtiden

FOI har på uppdrag av Myndigheten för Samhällsskydd och beredskap (MSB) byggt upp ett nationellt centrum för säkerhet i industriella styrsystem, NCS3[6]. Inom ramen för centrets verksamhet har deltagare från olika samhällsviktiga verksamheter deltagit i kurser i styrsystemsäkerhet och föreläsningsträffar med internationella experter.

Forskare från FOI har analyserat IT-vapen och genomför tekniska studier för att förbättra kunskapen inom styrsystemssäkerhet. FOI har också besökt företag och myndigheter för att sprida medvetenhet om behoven avseende IT-säkerhet i SCADA-system samt besökt flera samhällsviktiga anläggningar för att ge råd om IT-säkerhet. Efter upptäckten av StuxNet har ett ökat intresse märkts för området även bland svenska politiker.

Ett fortsatt arbete med att skapa medvetenhet om området och dess utmaningar inom flera delar av samhället bedöms dock som ytterst viktigt. Med medvetenhet kommer också behov av kunskap om vilka hot som finns, vilka sårbarheter i styrsystemen som dessa bygger på, vilka risker det resulterar i och hur dessa kan minskas. Detta ställer stora krav på kunskapsutveckling och kunskapsspridning inom området. Dessa utmaningar och behov delas av alla länder och utrymmet för innovationer är stort. De organisationer och samhällen som kan hantera riskerna med IT-angrepp kommer sannolikt att ha stor fördel av detta i framtiden.

Förhoppningsvis kommer samarbetet mellan NCS3 och industrin att öka och leda till att framtidens infrastruktur kommer att vara stabil och säker i proportion till hur beroende vi är av den.

[6] Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet.

9 Lägesförståelse i informationssamhället

Ulrik Franke, Joel Brynielsson, Tommy Gustafsson, Jonas Hallberg och Pontus Svenson

Informationsteknik blir en allt viktigare del av samhället. Vi arbetar, umgås, utbildar oss och interagerar med myndigheter via nätet i en omfattning som var otänkbar för bara tio år sedan. Samtidigt förekommer brottslighet, terrorism-relaterade aktiviteter och krigföring på internet – alltifrån enklare intrångsförsök och överbelastningsattacker genomförda av enskilda amatörer till näthat eller mer sofistikerade attacker som kriminella organisationer eller främmande stater bedöms ligga bakom. Det moderna informationssamhällets vinster leder alltså också till ökad sårbarhet. En del av dessa sårbarheter tas upp i artikel 8, som diskuterar IT-angrepp på kritisk infrastruktur. Andra aspekter tas upp i artikel 21, som handlar om informationssamhällets krav på myndigheters kriskommunikation och interaktion med medborgarna. I den här artikeln diskuterar vi möjligheter och problem med att skapa lägesförståelse utifrån information på internet.

Lägesförståelse – vad och varför?

Lägesförståelse är ett mångfacetterat begrepp som kan studeras ur flera perspektiv. Den tekniska aspekten av lägesförståelse handlar om att sammanställa, bearbeta, kvalitetssäkra, jämföra och fusionera information. Detta är dock inte så mycket värt utan den kognitiva aspekten: att förstå och kunna dra slutsatser ur den tekniska lägesinformationen. Därför vill man helst mäta hur människor uppnår lägesförståelse samt lyckas behålla och vidareutveckla den över tiden. De klassiska frågeställningarna, formulerade av Mica Endsley på 1990-talet, rör beslutsfattarens förståelse för (i) vad som händer, (ii) varför det händer och (iii) vad som kommer att hända. Alla tekniska hjälpmedel för lägesförståelse syftar i grunden bara till att hjälpa beslutsfattaren besvara dessa frågor.

Intrångsförsök och överbelastningsattacker (”denial of service”) pågår hela tiden på internet. *Vad* som händer går i viss mån att överblicka. CERT-SE[7] vid Myndigheten för samhällsskydd och beredskap presenterar exempelvis en lägeskarta över infekterade datorer i Sverige på sin hemsida (se inledande figur). Men *varför* händer det? Lägesförståelse för internet handlar också om att tyda tecknen och skilja allvarliga kriser från pojkstreck och enklare cybervandalism. Ett exempel är IT-säkerhetsföretaget Symantecs avslöjande år 2012 av hur IT-brottslingar använder sig av överbelastningsattacker mot banker som avledande manövrar. När IT-driftpersonalen (ofta nattskiftet) är fullt upptagen med att hålla hemsidan uppe genomför man allvarligare intrång i andra system, som möjliggör stölder av miljoner dollar i kreditkortsbedrägerier. Detta illustrerar utmaningen i att gå från *vad* till *varför* och att sedan prioritera rätt. När är angreppen som beskrivs i artikel 8 bara en angelägenhet för det omedelbart drabbade företaget eller branschen och när är det en pusselbit i ett större sammanhang?

I det gamla totalförsvaret talade man om skymningsläget: en gråzon mellan krig och fred präglad av skenbart oförklarliga strömavbrott, sjukdomsfall och olyckor till följd av fientligt sabotage. I informationssamhället är det självklart att sådana sabotage i ökad omfattning kommer att äga rum via internet. Lika självklart är det att vi måste kunna skilja angreppen från varandra: vi kan inte förklara att riket befinner sig i krig eller krigsfara och kalla in riksdagens krigsdelegation varje gång som någon initierar en överbelastningsattack mot Regeringskansliets hemsida. Lägesförståelse på internet blir i förlängningen en förutsättning för fungerande säkerhetspolitik.

[7] CERT-SE (Computer Emergency Response Team) är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. Verksamheten bedrivs vid Myndigheten för samhällsskydd och beredskap (MSB).

I artikel 8 beskrivs hur industriella styrsystem har utvecklats från fristående till internetuppkopplade för att öka effektiviteten i styrningen av allt från enskilda pumpar till hela infrastrukturer – och vilka risker det medför. Vore det då inte klokt att satsa på att koppla bort all kritisk IT-utrustning från internet? Det är vad vi ser i Iran, där regimen håller på att skapa ett nationellt fristående internet som går att övervaka och styra. Det riskerar att bli dyrt. Att skärma av ett helt land från omvärlden får ödesdigra konsekvenser för handel, innovation och tillväxt. Teknisk isolering och lagar som begränsar utbytet och handeln med omvärlden kan omintetgöra fördelarna med informationssamhället. En bättre strategi är alltså att acceptera uppkopplingarna och korsberoendena i det moderna samhället – men att se till att ha en adekvat lägesförståelse för vad som sker.

IT-sensorer och experiment

För att skapa lägesinformation som kan bidra till ökad lägesförståelse på internet krävs flera olika tekniker. Relevanta ”IT-sensorer” behöver samla in information om överbelastningsattacker och intrångsförsök. På internet finns det massor av hot från brottslingar, reaktioner från offer, skryt från förövare, information om sårbarheter och uppmaningar till angrepp som behöver skannas av. Framförallt behöver man kunna sammanställa och analysera all den information som finns tillgänglig. Informationsfusion är det forskningsområde som handlar om hur man kan väga samman data från heterogena källor för att förstå vad som sker.

Ökad lägesförståelse kräver experiment för att avgöra både vilken lägesinformation som är möjlig att ta fram och hur den ska användas för att skapa lägesförståelse hos beslutsfattare. Delvis för detta ändamål utvecklar och underhåller FOI CRATE (Cyber Range And Training Environment), en avancerad laboratorieresurs som används för att skapa datornätverk för experiment, tävlingar och övningar i IT-säkerhet. I CRATE går det att konfigurera tusentals virtuella maskiner i en kontrollerad miljö – ett slags simulerat internet, komplett med trafik som påminner om verkligt användarbeteende.

I CRATE-miljön planeras just nu ett antal experiment med inriktning mot lägesförståelse. Tidigare forskning har ofta fokuserat på hur systemadministratörer ska titta på datorernas trafik- och paketloggar för att skapa sig en teknisk lägesförståelse. Det är en viktig del, men den behöver kompletteras med förståelse på en högre nivå. Ett planerat experiment handlar om det som brukar kallas för *information overload*. Genom att utsätta ett blått (försvarande) lag som angrips för en blandning av relevant och irrelevant information går det att utvärdera hur beslutsfattarna reagerar och skapar sin lägesförståelse. I förlängningen möjliggör det också datorverktyg för att bringa reda i kaoset. Ett annat experiment handlar om *insider*-hot. En medlem av det blåa laget får en hemlig uppgift: att agera angripare från insidan. Olika detektionssystem kan då

utprovas och testas för att se om de kan fånga sådana hot. I ett tredje experiment deltar fyra olika lag, varav ett slumpmässigt i varje omgång väljs ut att vara angripare. Uppgiften för den som angrips blir att identifiera vem det är som angriper. Just detta – attributionsproblemet – har orsakat mycket huvudbry, inte minst inom juridiken.

I alla experimenten finns det många utmaningar: hur ska information om exempelvis intrångsförsök kombineras med annan information (från bloggar eller Twitter) för att hjälpa oss att bedöma hur farlig en viss aktivitet är? Hur kan informationen sammanställas med bibehållet integritetsskydd? Vilka aktiviteter går det överhuvudtaget att hitta spår av? Att systematiskt studera dessa frågeställningar via experiment är enda sättet att få tillförlitliga svar.

Andra frågor är svårare att studera laborativt: Vilken information är viktig för aktörer som Myndigheten för Samhällsskydd och beredskap (MSB), Post- och telestyrelsen och polisen att ha för att skapa lägesförståelse för internet? Hur kan man använda internet för att skapa bättre förståelse för händelser i den fysiska världen, till exempel vid en pandemi? Hur kan man använda internet för att kommunicera med allmänheten i händelse av allvarlig kris? På FOI utvecklas teknik för att just kunna ta tillvara på och dra slutsatser från sociala medier med avseende på allmänhetens reaktioner i samband med kris. Genom att analysera den inhämtade informationen erhålls värdefull kunskap avseende hur väl ett utskickat krismeddelande har, eller inte har, uppfattats av den tänkta målgruppen. Arbetet omfattar både teknisk utveckling av maskininlärning för IT-sensorer och kognitiva aspekter som hur man bäst ska visualisera information för beslutsfattare.

Sensorer och visualisering är dock bara första steget. Lägesförståelse måste också omsättas i handlingsförmåga, vilket kan kräva nya och anpassade ledningsprocesser där den nya informationen kommer till nytta. Det kan exempelvis krävas att man har tillgång till uppdaterade listor över vad som är skyddsvärt på internet. Banker och industriella styrsystem är kanske uppenbara skyddsvärda objekt, men de IT-system som används för att styra logistiken hos stora matvarukedjor kan vara nog så viktiga att skydda. Infrastrukturen för kriskommunikation med allmänheten är kanske ytterligare ett exempel (se artikel 21), liksom nyckelbefattningshavare i samhället.

Svårigheter och begränsningar

Tieto-haveriet i november 2011, när fel hos en enda leverantör ledde till att mängder av annars orelaterade verksamheter som Apoteket, Bilprovningen och Stockholms stad fick problem, visar att det inte alltid är självklart vilka konsekvenser som störningar får eller vad som bör skyddas. Idag säljs IT ofta som en tjänst med tillgänglighetsavtal (Service Level Agreements, SLA). Olika verksamheter har olika krav: Där IT-tjänster styr fysiska industriprocesser med

stora logistikkedjor, exempelvis stålverk, vill man ha så få avbrott som möjligt även om de blir längre. Där IT-tjänster bara hanterar information, exempelvis kortbetalningar i detaljhandeln, är det bättre med många korta avbrott. Lägesförståelse måste innefatta även förståelsen för vad som egentligen står på spel i en värld av komplexa korsberoenden.

En annan komplicerande faktor är att enskilda aktörer ofta saknar incitament att sammanställa information för ökad lägesförståelse. Tvärtom kan det vara förknippat med kursras på börsen att offentliggöra intrång i IT-system eller att systemen ligger nere. Den här svårigheten är en del av ett större problemkomplex: Hur vet man att man baserar sin lägesförståelse på rättvisande uppgifter? IT-sensorerna kanske bara täcker de företag som släpper information, de drabbade som twittrar, de brottslingar som skryter, de cyberspioner som klantar sig, de angripare som använder gamla kända sårbarheter och de hot som man har tänkt på i förväg. Kan man kompensera för dessa skeva urval och ändå skapa sig en korrekt lägesuppfattning? Lägg därtill risken för avsiktlig vilseledning på internet. Vi vet att det finns gott om aktörer som avsiktligt sprider falsk information och att det finns en uppsjö av metoder för att lyckas.

Trots svårigheterna så är frågan om lägesförståelse viktig om vi vill fortsätta att njuta av informationssamhällets fördelar utan att utsätta oss för större risker än nödvändigt. Vare sig teknisk eller juridisk avskärmning från omvärlden är bra sätt att hantera informationssamhällets hot. En bättre strategi är att göra dynamiska riskbedömningar av hoten och medvetna avvägningar mellan kostnad och nytta (se även artikel 2-5). Det är i sin tur bara möjligt om vi hela tiden gör vårt bästa för att hålla reda på vad som händer, varför det händer och vad som kommer att hända i framtiden.

Vidare läsning

- Brynielsson, J., Johansson, F. and Lindquist, S. Using video prototyping as a means to involving crisis communication personnel in the design process: Innovating crisis management by creating a social media awareness tool. Proceedings of the 15th International Conference on Human-Computer Interaction, Las Vegas, Nevada, juli 2013. Yamamoto, S. (Ed.): HIMI/HCII 2013, Part III, LNCS 8018, pp. 559–568, Springer-Verlag Berlin Heidelberg 2013.
- Franke, U. Information operations on the internet, FOI-R--3658--SE, 2013.
- Sommestad, T. and Hallberg, J. “Cyber security exercises and competitions as a platform for cyber security experiments,” Proceedings of NordSec, 2012.

10 Skolskjutare och spår i den digitala sfären

Fredrik Johansson och Lisa Kaati

I denna artikel belyser författarna hur man genom digitala spår kan upptäcka och förhindra potentiella skolskjutare. Det har nämligen visat sig att det vid skolskjutningar i förhand har funnits flera spår på sociala medier och webbsidor. Tekniker för att hitta spåren är under utveckling på FOI. Författarna belyser också vilka framsteg som gjorts vid analys av sociala medier för att ge polis och andra aktörer en bättre lägesbild.

Bakgrund

Problematiken med så kallade skolskjutningar har under de senaste åren aktualiserats gång på gång genom incidenter och attacker runt om i världen. Även om Sverige lyckligtvis inte har haft så många fall med skolskjutare så har våra grannländer (och då framför allt Finland) på senare år haft ett flertal incidenter. Två tragiska exempel är de välkända skolskjutningarna i Jokelaskolan (2007) och Kauhajoki (2008). En annan mycket känd skolskjutning som fått stor massmedial uppmärksamhet runt om i världen är den så kallade Columbine-massakern som utfördes 1999 på Columbine High School i USA. Dessa är dock bara ett litet urval eftersom hundratals skolskjutningar har ägt rum i världen

under det senaste årtiondet. För svensk del inträffade den senaste skolskjutningen med dödlig utgång 1961 när en 17-åring steg in i Kungälvs läroverks gymnastiksal, drog upp en pistol och började skjuta. Följden av attacken blev att sex elever skadades och en avled. Även om Sverige varit relativt förskonat från skolskjutningar har det även här förekommit ett flertal fall där elever har hotat att utföra våldsdåd mot skolor och i ett fall 2004 stoppades en planerad massaker mot Slottsstadens skola i Malmö.

Flera olika definitioner av vad begreppet skolskjutare innefattar förekommer i litteraturen, men en ungefärlig beskrivning som stämmer in på de flesta förekommande definitioner är att det ska röra sig om en elev eller en före detta elev som utför en planerad attack gentemot skolkamrater, lärare eller andra personer som uppehåller sig på skolan eller campus. Denna beskrivning utesluter alltså attacker där någon helt plötsligt får ett vansinnesutbrott och skadar eller dödar sina kamrater, samt attacker som utförs av vuxna individer utan koppling till skolan. Själva termen skolskjutning antyder att attacken skulle utföras med hjälp av skjutvapen, men det finns också ett flertal exempel där gärningspersonen använt sig av rörbomber, Molotov-cocktails eller stickvapen som också vanligtvis faller under etiketten skolskjutning.

Svensk polis utbildas numera för att kunna hantera skolskjutningar eftersom det anses vara troligt att antalet incidenter kan öka i framtiden. Myndigheten för samhällsskydd och beredskap (MSB) uppskattar i 2012 års nationella riskbedömning respektive bedömning av krisberedskapsförmåga att sannolikheten för att en skolskjutning ska inträffa i Sverige ligger på runt 10 % på årsbasis. I rapporten målas ett skrämmande men realistiskt scenario upp där en elev i en liten svensk kommun skjuter ihjäl en lärare och sex elever för att sedan ta sitt eget liv. I samband med händelsen blir det ett stort tryck från allmänheten och media, vilket bland annat får till följd att ett omfattande utbyte av såväl korrekt information som rykten äger rum i sociala medier.

I denna artikel beskriver författarna hur just analys av sociala medier kan komma till användning dels för att i ett *proaktivt* syfte kartlägga och identifiera potentiellt intressanta grupper och individer innan en skolskjutning faktiskt äger rum (genom att samla in och fusionera digitala spår som tyder på att någon planerar en skolskjutning), dels användas *reaktivt* för att ge bättre lägesförståelse för polis och andra beslutsfattare när katastrofen väl har inträffat. För att förebygga och hantera problemet med skolskjutningar krävs tvärvetenskaplig forskning och samarbete mellan skola, polis och socialtjänst. Författarna belyser dock främst problemet från ett datavetenskapligt perspektiv. Det är viktigt att förstå att teknikutveckling i sig inte ensamt kan lösa problemet, eftersom inte minst etiska och legala aspekter måste vägas in. Ytterligare en viktig aspekt är att tekniska verktyg i bästa fall kan stödja polisen i sitt arbete, snarare än att ersätta deras analytiska förmåga.

Digitala spår i sociala medier

I merparten av alla skolskjutningar sedan 2005 har förövarna enligt existerande forskning lämnat spår på sociala medier och andra typer av webbsidor. När en skolskjutning har inträffat har det därför från olika håll, inte minst från massmedia, antytts att polisen borde ha kunnat förutse vad som var på väg att hända och agerat mer proaktivt. Polisen i Finland sägs lägga stora resurser på att övervaka diskussioner på olika forum på internet för att kontrollera eventuella hotbilder, speciellt när skolskjutningar i andra länder har inträffat eftersom man då oroar sig för så kallade *copycats*, det vill säga att någon ska ta efter och försöka imitera de gärningar som har utförts.

Att manuellt övervaka alla tänkbara sociala medier med syftet att hitta potentiella hot som tyder på en ökad risk för en skolskjutning är inte möjligt eftersom det kräver orimliga resurser. Detta faktum visar på ett behov av metoder och automatiska eller semi-automatiska verktyg för att kunna rikta in övervakningen på de forum och så kallade *communities* som är av störst intresse för att sedan kunna identifiera och värdera möjliga hot mot skolor eller andra digitala spår med så lite inverkan på den personliga integriteten som möjligt. I den här artikeln fokuserar författarna enbart på vilka digitala spår kopplat till skolskjutningar som går att hitta i sociala medier. Det är noterbart att andra typer av indikatorer så som uttalade hot mot lärare eller elever också givetvis bör vägas in, något som dock ligger utanför fokus för denna artikel.

Vad finns det då för digitala spår som skulle kunna förvarna om en möjlig attack? Om man börjar med de mest uppenbara eller explicita spåren så är det vanligare än man skulle kunna tro att gärningspersonen innan en attack har lämnat uttryckliga skriftliga hot i sociala medier. Ofta lämnas dessa i publika forum där de är åtkomliga för alla, inklusive polisen. I vissa fall är dock meddelandena inte åtkomliga publikt utan riktas till en sluten grupp mottagare. I de senare fallen finns det inte mycket mer att göra än att hoppas på att någon lämnar ett tips till polisen. De riktade hoten kan givetvis vara mer eller mindre explicita. I flera tidigare fall har gärningspersoner annonserat sina planer på YouTube i en film innan en attack, postat budskap av typen ”ready for action” och ”you will die next” eller laddat upp (politiska) manifest på olika forum. En annan form av digitalt spår som varit vanligt förekommande innan skolskjutningar är att gärningspersonen har postat bilder eller videor där denne poserar med automatvapen, liknande de bilder som efter Anders Behring Breiviks terrorattentat i Norge publicerades i många tidningar. Vanligt förekommande är också bilder där man poserar i utstyrsel och utrustning liknande den som bars av Eric Harris och Dylan Klebold vid Columbine-massakern. Att på detta sätt posera med vapen behöver givetvis inte vara olagligt, men kan fungera som en form av indikator på att något kanske inte står helt rätt till. Just referenser till tidigare skolskjutningar i allmänhet och Columbine-massakern i synnerhet är för övrigt väldigt vanligt. Exempel på detta är de

användarnamn som olika gärningspersoner har använt på sociala medier. För att nämna några så har användarnamnen ”*Todesengel*” (dödsängel), ”*verlassen4_20*” (anspelning på datumet för Columbine-massakern och Hitlers födelsedag) och ”*naturalselector89*” använts på YouTube och olika diskussionsforum av personer som senare utfört skolskjutningar. Utöver detta så finns det även ett flertal webbsidor eller forum där människor som blivit inspirerade av tidigare skolskjutningar ofta diskuterar tidigare händelser i positiva ordalag, inte helt olikt de forum som används för att sprida högerextrema eller jihadistiska budskap som manar till attacker mot samhället eller upplevda antagonister. Enligt befintlig forskning har många skolskjutare varit aktiva i denna typ av ”skolskjutar-communities” innan de har utfört sina attacker.

Det urval av digitala spår som har nämnts ovan kan användas för att på ett tidigt stadium upptäcka potentiella skolskjutare. Allt från explicita hot, bilder och videor där man poserar med vapen i hand, valda användarnamn och inlägg i kontroversiella webbforum kan användas som indikatorer på att allt inte står helt rätt till. Dessa indikatorer eller svaga signaler är ofta inte tillräckligt starka tagna var och en för sig, men kan genom att kombineras användas som tecken på att polis eller sociala myndigheter bör agera. På FOI bedrivs forskning om identifikation och fusion av svaga signaler på internet. Detta har tänkbara tillämpningsområden som exempelvis att identifiera potentiella skolskjutare eller ensamagerande terrorister men kan också användas för helt andra syften så som detektion av naturkatastrofer eller nya konflikthärdar.

Tekniker för att identifiera potentiella skolskjutare

För att kunna upptäcka potentiella skolskjutare behövs verktygsstöd för att kunna göra relevanta sökningar i sociala medier i syfte att identifiera forum, grupper eller användare som på ett eller annat sätt relaterar till ämnet skolskjutningar. Detta steg är ett exempel på så kallad *targeting*, där man försöker rikta in sina tillgängliga resurser på vad som bör övervakas. För att vara användbart bör sökningar kunna utföras på ett flertal sociala medier som exempelvis diskussionsforum, Twitter och YouTube. Det bör också finnas möjlighet att söka på en rad olika begrepp som relaterar till skolskjutningar och få resultatet presenterat på olika sätt, exempelvis som en lista på forum eller användarnamn, eller i form av sociala nätverk där kopplingar mellan olika användare beaktas. Dessa kopplingar kan utgöras av relationer som exempelvis vem som är vän med vem på Facebook, vem som följer vem på Twitter, eller vem som kommenterat någons inlägg eller uppladdade filmer på ett diskussionsforum eller YouTube. Den här formen av nyckelordsbaserad sökning är ett trubbigt verktyg men ger ändå möjlighet att på stor skala snabbt söka igenom stora mängder data och filtrera ut den information som är av intresse, något som är omöjligt med

manuella medel. Det finns idag flera olika företag som har specialiserat sig på att möjliggöra sökningar på specifika nyckelord i olika sociala medier. I forskning gjord av ryska och finska forskare har man använt sig av liknande tekniker för att skapa sociala nätverk över användare på LiveJournal som har intressen som relaterar till exempelvis skolskjutningar, massmord eller massmördare. I denna kartläggning identifierade man ett stort antal communities och användare som innehöll kända skolskjutare och deras ”vän-kopplingar”.

Sannolikt är flertalet av de användare som identifieras med en grov nyckelordssökning personer som har just ett intresse för skolskjutningar, snarare än planer på att själva genomföra en sådan handling. Med andra ord är en nyckelordssökning bara användbart för att filtrera ut information som kan vara av ett potentiellt intresse och som bör analyseras i mer detalj. När ett nätverk med potentiellt intressanta personer har extraherats kan det analyseras genom att använda sig av så kallad *SNA* (*social network analysis*). Inom detta område har FOI stor kompetens, inte minst vad gäller analys av icke-fullständiga eller osäkra sociala nätverk, vilket ofta är en fundamental egenskap hos de nätverk som tas fram på det sätt som beskrivits ovan. Analys av sociala nätverk kan användas för att identifiera inflytelserika personer, hitta delgrupperingar eller olika centrala aktörer. Den här typen av analys kan användas för att filtrera ut det mest intressanta aktörerna som bör analyseras vidare.

Nästa steg i analysen är att återgå till de indikatorer som kan tyda på att någon har intention att begå en skolskjutning. Genom att applicera sofistikerade text-, bild- och videoanalystekniker kan man automatiskt försöka identifiera denna typ av indikatorer. Inom textanalys finns det exempelvis forskning gjord på FOI där man kan träna upp algoritmer för att identifiera känslostämningar i text. På samma sätt skulle man kunna träna algoritmerna med exempel på hotfulla respektive icke-hotfulla textmeddelanden i syfte att lära systemet att automatiskt kunna känna igen hot i text. Ett alternativ till detta är att skapa lingvistiska regler för vad som karakteriserar ett hot, något som dock vanligtvis kräver djupare språklig expertkunskap. För att kunna känna igen bilder eller videor där någon poserar med vapen behövs mer forskning. Inom så kallad *CBIR* (*content-based information retrieval*) arbetar man med att ta fram algoritmer för att känna igen bilder baserade på innehåll snarare än textuell beskrivning. Denna typ av funktionalitet börjar nu återfinnas i en rad kommersiella produkter, vilket tyder på en ökad mognadsgrad som inom några år borde göra det möjligt att med relativt god precision kunna identifiera bilder eller videor där någon poserar med vapen.

Genom att använda sig av diverse olika tekniker för att kunna identifiera indikatorer som tyder på att någon har intention att begå en skolskjutning är nästa problem att indikatorerna var och en för sig inte alls behöver betyda att personen faktiskt tänker begå en skolskjutning. Det är fullt möjligt att någon har ett iögonfallande användarnamn som *natural_selector* och skriver inlägg som

handlar om skolskjutningar utan att denne har någon tanke på att utföra en skolskjutning i praktiken. Något förenklat kan man säga att indikatorerna var och en för sig kan peka på ett potentiellt hot med varierande styrka och att ju fler indikatorer som är uppfyllda, desto mer sannolikt är det att användaren planerar något, eller i varje fall att det blir desto mer relevant att göra ytterligare undersökningar kring användaren. Genom FOI:s forskning inom *informationsfusion* så finns kompetens att kunna ställa upp sannolikhetsteoretiska hotmodeller för när något ska klassas som ett tillräckligt stort hot för att en mänsklig analytiker ska studera denne individ och dess inlägg närmare.

Ett problem som knyter an till det ovanstående är att individer inte sällan använder olika alias på olika sociala medier. Eftersom det är en persons sammantagna inlägg som är av intresse vid bedömning om det föreligger någon hotbild så är det viktigt att kunna identifiera om flera olika alias tillhör en och samma individ. Detta är ett relevant forskningsproblem där en kombination av ett flertal olika tekniker såsom tidsprofilering, författarigenkänning, *SNA (social network analysis)* och namnmatchning verkar ge goda resultat enligt pågående forskning. När en användare väl har identifierats som intressant återstår problemet att knyta dennes alias till en fysisk person. Detta kan exempelvis göras genom att polismyndigheter efter en juridisk prövning begär ut information från den som tillhandahåller tjänsten för det sociala mediet i fråga, samt internetleverantörer. Det bör betonas att även om mycket av den teknik som har diskuterats ovan av nödvändighet måste automatiseras till en stor del för att minska belastningen på de mänskliga analytikerna så är det alltid den mänsklige analytikern som måste göra en slutgiltig bedömning om insamlad data är tillräckligt intressant att gå vidare med. På samma sätt föreligger vid all typ av automatiserade eller semi-automatiserade system en risk för falsklarm, där personer som egentligen inte har tänkt utföra någon skolskjutning utan ”skämtar” eller av någon annan anledning följer denna typ av diskussioner och skriver tvivelaktiga inlägg pekas ut som misstänkta eller potentiella skolskjutare. I dessa fall skulle dock ett samtal från polisen eller socialtjänsten troligtvis ändå inte skada som en väckarklocka innan något värre händer. Vidare så är det återigen alltid en mänsklig analytiker som ska ha sista ordet om vad som ska göras.

Användning av analys av sociala medier för att identifiera skolskjutningar och ge beslutsfattare en bättre lägesbild

Om ett scenario som det som har målats upp av MSB i dess nyligen utgivna rapport skulle inträffa i verkligheten i Sverige är det viktigt att polis och andra berörda myndigheter på ett så tidigt stadium som möjligt kan få en lägesbild över vad som händer på skolan. I denna typ av krissituationer används sociala medier i en allt ökande utsträckning, i takt med att användandet av sociala medier i

mobiler och surfplattor sprider sig. Sociala medier kan därför vara en viktig källa till information i sådana situationer, vilket exempelvis har visat sig vid terroristattentaten i Norge, kärnkraftsolyckan i Japan och diverse olika naturkatastrofer. Det pågår därför en hel del forskning som involverar framtagande av prototyper för att söka i och analysera data från sociala medier i real-tid, vilket möjliggör att beslutsfattare kan få en bättre lägesbild. Detta är bland annat ett viktigt forskningsproblem i EU-projektet Alert4All där FOI spelar en viktig roll. Ett problem vid analys av sociala medier är de stora mängder icke-relevant och felaktig information som cirkulerar och behöver kunna filtreras ut. Att kunna bedöma källors tillförlitlighet samt sakriktigheten i information är långtifrån ett löst forskningsproblem, men allt talar för att användningen av analys av sociala medier i kriser kommer att öka i framtiden.

Avslutning

Skolskjutningar är ett samhällsproblem som svenska myndigheter måste förbereda sig inför. Under 2013 har Rikspolisstyrelsen påbörjat en landsomfattande utbildning för svensk polis för att kunna hantera skolskjutningar taktiskt. För att kunna stoppa skolskjutningar innan de äger rum bör man även överväga att utveckla teknik för att ha möjligheten att upptäcka indikatorer för att denna typ av händelse håller på att inträffa. Det är inte bara potentiella skolskolskjutare som lämnar digitala spår på internet. Det finns många andra incidenter som exempelvis terrorbrott eller andra former av attentat riktade mot personer där man skulle kunna använda sig av liknande tekniker för att upptäcka digitala spår som tyder på att ett brott planeras.

Det finns dock en hel del problem som man bör adressera innan man kan börja analysera sociala medier för att kartlägga och identifiera individer som visar en ökad risk för att begå ett brott av något slag. Utöver existerande tekniska begränsningar finns även etiska och lagliga överväganden som måste beaktas. Exempelvis skulle det utifrån ett tekniskt eller rent operativt perspektiv kunna vara givande att sätta upp en så kallad ”honungsfälla” där man själv skapar ett alias eller ett forum där man utger sig för att ha ett osunt intresse av skolskjutningar och sprida olika typer av inlägg för att se vilka användare eller personer som väljer att följa ens inlägg. Detta beteende skulle dock vara högst moraliskt och juridiskt tvivelaktigt då det skulle kunna riskera att göra personer mer intresserade av skolskjutningar eller indirekt uppmana till brott. Framtida forskning behöver därför fokusera på att komplettera de tekniska möjligheterna med etiska och legala aspekter, för att på så sätt fungera som beslutsunderlag för huruvida denna typ av preventiv övervakning ska göras möjlig eller inte. Överlag saknas det med några få undantag publicerade forskningsresultat om tekniska aspekter på hur man skulle kunna förhindra eller i varje fall kartlägga potentiella skolskjutare. Detta kan jämföras med de hyllmeter som har skrivits om skolskjutningar från olika psykologiska och sociologiska aspekter. Den

existerande forskningen är av yttersta vikt men bör också kompletteras med forskning på hur man kan gå tillväga för att på ett tidigt stadium faktiskt upptäcka och förhindra uppkomsten av skolskjutningar genom att analysera vad som publiceras inom den digitala sfären. Genom vidare forskning skulle man kunna få en bild över hur effektiva den här typen av tekniker kan vara. Detta skulle göra det möjligt att ställa den förväntade nyttan gentemot negativa aspekter så som risk för att människor skulle känna sig övervakade eller risk för falsklarm.

Vidare läsning

- Brynielsson, J., Horndahl, A., Johansson, F., Kaati, L., Mårtenson, C. and Svenson, P. ”Analysis of Weak Signals for Detecting Lone Wolf Terrorists”, Proceedings of the 2012 European Intelligence and Security Informatics Conference, 2012.
- Dahlin, J., Johansson, F., Kaati, L., Mårtenson, C. and Svenson, P. ”Combining Entity Matching Techniques for Detecting Extremist Behavior on Discussion Boards”, Proceedings of 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2012.
- Johansson, F., Brynielsson, J. and Narganes Quijano, M. ”Estimating Citizen Alertness in Crises using Social Media Monitoring and Analysis”, Proceedings of the 2012 European Intelligence and Security Informatics Conference, 2012.

11 Ibland är det bra att bli sedd – övervakningskameror med automatisk bildanalys ger säkerhet och integritet

Niclas Wadströmer

Det blir allt vanligare med övervakningskameror. De finns i mataffären, i banken, på torget, i trafiken, i bussar och tåg, på skolor och många andra platser. Samtidigt har alla rätt att slippa bli bevakade och kartlagda. Övervakningskameror för med sig en motsättning mellan rätten till integritet och rätten till säkerhet. Motsättningen beror på att dagens kameraövervaknings-system kan se mycket mer än det som strikt sett är motiverat av syftet med övervakningen. Om systemen enbart kan se att en överträdelse av någon regel eller rättighet skett så sker ingen orättfärdig kränkning av någons rättigheter. Men när den enda möjligheten är att använda en kamera så kommer mycket att synas som skyddas av rätten till privatliv.

Vi behöver fokusera forskningen på system som bara ser det som är syftet med övervakningen och är blint för andra förhållanden. Det som idag är en motsättning kommer att försvinna i takt med att övervakningssystemen blir allt mer specifika.

Automatisk bildanalys ger en möjlighet att bygga bättre övervakningssystem som i en högre grad respekterar rätten till integritet och rätten till säkerhet.

Övervakningssystem och lagen

Övervakningssystem får bara användas för något specifikt syfte. Ofta handlar det om att upptäcka och förebygga brott. I många sammanhang finns det handlingar och aktiviteter som är otillåtna, men övervakningssystemen ser mycket mer än det som är brottsligt och otillåtet. När en oskyldig person fångas av en övervakningskamera kränks personens integritet. Övervakningskameror för med sig en motsättning mellan rätten till säkerhet och rätten till integritet. Därför finns det en lag som reglerar användningen av kameraövervakning. Lagen säger att det krävs tillstånd från länsstyrelsen för att få sätta upp en kamera som kan riktas mot en plats dit allmänheten har tillträde. I lagen anges att kameraövervakning ska ske med tillbörlig hänsyn till enskildas personliga integritet. Länsstyrelsen ska ge tillstånd om intresset för övervakning väger tyngre än den enskildes intresse av att inte bli övervakad, särskild hänsyn ska tas om övervakningen behövs för att förebygga brott och förhindra olyckor. Även om lagen ska säkerställa den enskildes intresse av att inte bli övervakade så känner många ett obehag inför alla kameror och en oro att uppgifter från övervakningen ska komma på avvägar. En viktig detalj är att lagen om kameraövervakning bara begränsar användning av kameror som kan användas för personövervakning. Den gäller alltså kameror där man kan känna igen eller identifiera enskilda individer.

Det finns många situationer där det inte är intressant att kunna känna igen enskilda personer men där man fortfarande kan öka säkerheten genom övervakningskameror. Det kan gälla en lokal där det finns krav på att veta hur många personer som befinner sig i lokalen, man behöver veta vart personer är på väg för att kunna dirigera om resurser, i trafiken vill man kunna styra signaler för att förbättra flödet av både fordon och personer.

Utvecklingen av automatisk behandling av video har gjort stora framsteg och det är idag möjligt att med automatisk analys av video ta fram information om vad som händer på en plats, som till exempel hur många personer som finns på platsen, hur de rör sig och om någon fallit omkull.

Aktiva och passiva övervakningssystem

Kameraövervakningssystem kan delas in i aktiva och passiva system. Passiva system har som syfte att lagra information som kan användas för att utreda händelser i efterhand. Vid utredning av brott är det väsentligt att kunna identifiera och känna igen personer som är inblandade eller kan lämna information om händelsen. Aktiva system används för att övervaka en plats i realtid och för att kunna upptäcka och reagera på oönskade händelser direkt när

de sker. Vid aktiv övervakning är det sällan väsentligt att kunna känna igen och identifiera personer.

Passiva system spelar in video och lagrar denna för den händelse ett brott eller annan incident inträffar då man tar fram bildmaterialet för att kunna utreda vad som hänt. Så länge ingen incident har inträffat så ska ingen titta på bilderna. Det finns dock en risk att bilder sprids på ett otillåtet sätt. Om systemet använder öppna kommunikationsnät, så som internet, så finns det en risk att någon lyckas göra ett otillåtet intrång. Det finns exempel där övervakningskameror för internt företagsbruk har varit helt öppna, då existerande skyddssystem inte varit aktiverade. Det kan också vara så att någon anställd eller andra som har tillträde till lokalerna där bildmaterialet lagras kan komma åt bilderna. Det finns dock goda möjligheter att med organisatoriska och tekniska skydd hindra att bilder och information från systemet kommer på avvägar.

Aktiva system används för att övervaka en plats i realtid. I aktiva system är den enskildes identitet i allmänhet oväsentlig för övervakningens syfte. I många fall är dessutom de flesta personer som rör sig inom bevakningsområdet oskyldiga som har rätt att slippa bli igenkända. De aktiva systemen finns för att man ska kunna se om situationen är normal och upptäcka brott och andra oönskade händelser så tidigt som möjligt. Om det är möjligt ska systemet ge en varning innan själva brottet sker så att det går att avstyra. I en del av dessa system är den visuella bilden i sig inte det som är intressant utan utgör bara ett medel. System skulle istället kunna leverera en sammanställd information till bevaknings-operatören och ge larm när specifika händelser inträffar eller om situationen avviker från det som är normalt för platsen.

Idag har aktiva övervakningssystem en operatör som konstant eller periodvis aktivt tittar på videobilderna. Det finns i många fall alldeles för många kameror för att operatören ska kunna överblicka alla bilder. Bild 1 visare ett exempel på hur det kan se ut i en lednings- och övervakningscentral.

Det är lätt att tro att en operatör med hjälp av videokameror aktivt kan övervaka ett stort område, men praktisk erfarenhet och forskning har visat att det ofta är svårt att hålla koncentrationen på topp under lång tid. Redan efter en kort tid sjunker koncentrationen avsevärt, vilket gör att operatören lätt kan missa även väsentliga händelser. Men med hjälp av övervakningskamerorna kan en operatör, som uppmärksammas på en händelse, snabbt flytta sin uppmärksamhet och avgöra vad som sker och därmed kunna fatta beslut om vad som behöver göras.

Bild 1. En typisk övervaknings- och ledningscentral. På skärmarna visas bilder från ett fåtal kameror som finns tillgängliga. Scanpix: Miguel Medina

Oftast används aktiva system för att operatören ska kunna kontrollera vad som händer när det kommit ett larm. Larmet kan vara automatiskt, till exempel att en branddörr öppnas, att en person går åt fel håll eller att en väska blir övergiven. Det kan också vara ett manuellt alarm från en väktare eller någon annan person som befinner sig i området och blir varse att något inte är som det borde. Kameran som visar området som larmet kom ifrån aktiveras och operatören kan se vad som händer och kan därmed avgöra om och i så fall vilka åtgärder som är lämpliga. Operatören kan också växla runt mellan kamerorna för att se om något anmärkningsvärt händer inom de områden som bevakas med kameror.

Operatören behöver i första hand ha information om förändringar i läget som är eller kan leda till något otillåtet. När sådana händelser inträffar måste operatören bestämma vad som ska göras. Den information som operatören behöver från det aktiva kamerasystemet är inte alltid bilder. Det kan vara bearbetad information om hur läget utvecklar sig, till exempel antalet personer i området, var de befinner sig och hur de rör sig. Det kan vara andra egenskaper i bildmaterialet som är intressanta, så som hur personer rör sig kroppsligt, vilken pose de intar, om en person ligger ner utan att röra sig, om en person rör sig på spåret, går in i en tunnel avsedd för spårbunden trafik, etc. Den bearbetade informationen kan komma från automatisk analys av övervakningsbilder. Bild 2 visar ett exempel från en lobby som övervakas av fyra kameror. I kamerabilderna finns spår inlagt som visar hur personerna i bilden rört sig i lobbyn. Spåren har tagits fram av en

automatisk bildanalysalgoritm. Algoritmen tar reda på var det finns människor i bilderna och räknar ut deras position.

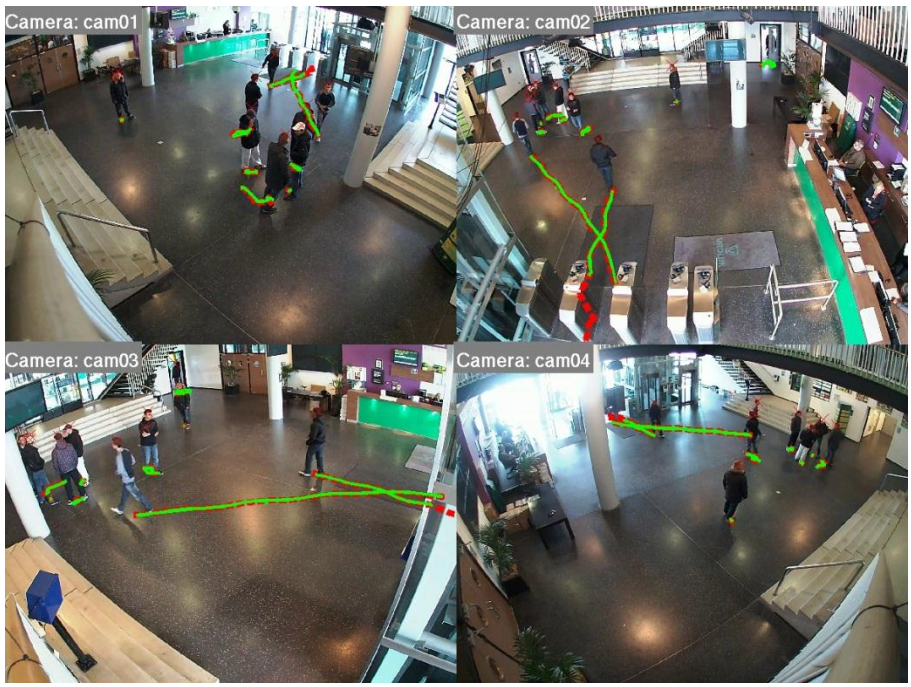
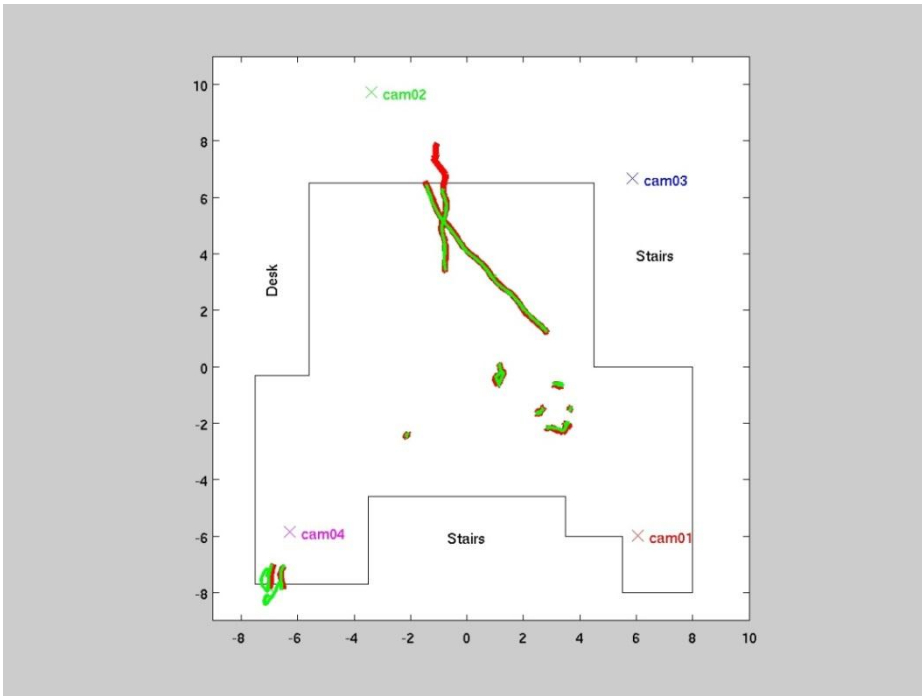


Bild 2. Bilder från fyra övervakningskameror som ser en lobby. Spåren visar hur personerna rört sig från en kort tid tillbaka och fram till aktuell bild. Spåren har tagits fram av en automatisk bildanalysalgoritm.

Genom att systemet visar rörelsespåren i en schematisk bild över den övervakade lobbyn kan man få en bra överblick av läget och händelseutvecklingen, se figur 1 nedan. I en del lägen ger översiktsbilden bättre information om läget i lobbyn än de fyra ursprungliga kamerabilderna. Om man bara visar översiktsbilden för operatören så kan denne inte känna igen eller identifiera personerna i lobbyn.



Figur 1. En schematisk figur över området som bevakas av de fyra kamerorna i bild 2. I kartan visas också spåren efter de personer som är i bild.

Det är kostsamt att ha konstant närvaro av väktare. Det kan dessutom uppfattas som påträngande i sammanhang där situationen oftast är lugn. En lösning på detta problem är att överföra en väktares uppmärksamhet mellan olika områden genom att montera upp kameror vars bilder överförs till en bevakningscentral. En eller flera operatörer kan då snabbt förflytta sin uppmärksamhet mellan olika områden. En nackdel är att det tar längre tid för väktare att komma till platsen för incidenter, eftersom väktarna måste förflytta sig till platsen. Fördelen är dock att ett fåtal operatörer kan övervaka ett stort område. En annan nackdel är, som sagts tidigare, att det är svårt för operatörer att behålla skärpan i sin uppmärksamhet under lång tid.

Det finns en risk att bilder och information kommer på avvägar. Det kan till exempel ske genom att en operatör otillåtet sprider uppgifter som denne har tagit del av via kamerabilder. Alla uppgifter som kommer på avvägar innebär en kränkning av personers integritet. I bästa fall så stannar kränkningen vid en risk att uppgifter kommer på avvägar. Uppgifter som kan associeras med en identifierbar person är känsliga. Ofta kan personer som syns i bilder från övervakningskameror identifieras eller kännas igen vilket gör att bilderna är känsliga.

När det går att göra övervakningssystem med kameror som levererar data och information på ett sådant sätt att det inte går att känna igen enskilda personer så kommer dessa system att kunna användas för många fler syften. Den som driver verksamheten kommer att kunna övervaka hur personer rör sig och vad de gör för att till exempel kunna ge så bra service till sina kunder som möjligt. Det kan gälla antal personer, väntetid, kölängd, hur personen rört sig, vilka varor de har tittat på, andra personliga egenskaper som är information som behövs för att styra och dimensionera verksamheten.

När många brott och olyckor sker så finns inte personer i närheten som kan larma. Det kan till exempel vara en person som attackeras på en tunnelbaneperrong, en lastbilschaufför som attackeras på en öde P-plats, biltjuvar som letar fordon att stjäla i ett P-hus eller terrorister som förbereder intrång på en samhällsviktig anläggning. Genom att använda automatisk bildanalys kan mängden bilder som lagras och skickas vidare väsentligt minskas. I de fall bilderna aktivt granskas kan operatörens effektivitet väsentligt öka eftersom denna bara behöver titta på bilder när det händer något som är misstänkt.

Övervakningssystem med bildanalys

Om man kopplar ihop en övervakningskamera med en dator som har programmerats för att analysera bildinnehållet och endast rapportera läget i det bevakade området så behöver inte den fullständiga videoströmmen skickas vidare. Systemet kommer då att avlasta operatören i övervakningscentralen genom att denne inte behöver sköta övervakningen manuellt via kameran utan operatören kan koncentrera sig på de områden och den tid då det händer något väsentligt i bevakningsområdet. Dessutom skyddar man integriteten hos de personer som rör sig i det bevakade området.

Automatisk bildanalys kan användas för att upptäcka specifika händelser och situationer som operatören borde uppmärksamma. Vad som ska upptäckas bestäms utifrån övervakningens syfte och begränsas av vad som är tekniskt möjligt att åstadkomma. Samtidigt kan man bestämma hur man ska agera om de specifika händelserna inträffar. Bildanalys kan också användas för att upptäcka onormala händelser. Systemet lär sig utifrån det specifika scenariot vad som är normalt och larmar när en situation avviker från det normala. När ett larm ges är det nödvändigt att en operatör avgör om händelsen är oönskad och vilken åtgärd som ska vidtas. Onormala händelser behöver inte vara oönskade och i så fall avstår operatören från åtgärder.

I vissa fall kan systemet använda operatörens bedömning av en händelse för att förbättra sin analys om vad som är normalt och vad som är hotfullt och på så sätt successivt minska antalet felaktiga larm. Detektion av onormala tillstånd kallas ofta anomalidetektion. Bild 3 visar ett exempel på en metod som kan användas för att automatiskt upptäcka snabba rörelser som kan tyda på våldsamt beteende.

Algoritmen följer ett antal punkter i bilden och spårens kurvighet ger en indikation på våldsamt beteende.

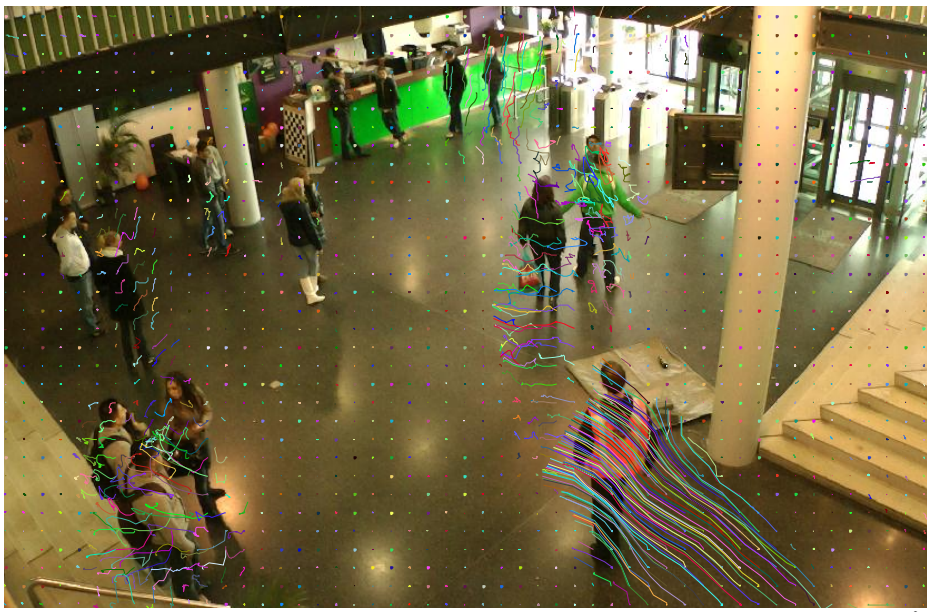


Bild 3. Automatisk bildanalys kan användas för att upptäcka rörelser som kan tyda på våldsamma handlingar. En operatör larmas och får avgöra om det krävs åtgärder. Algoritmen följer ett antal punkter i bilden och spårens kurvighet ger en indikation om våldsamt beteende förkommer.

Övervakning med större respekt för integriteten

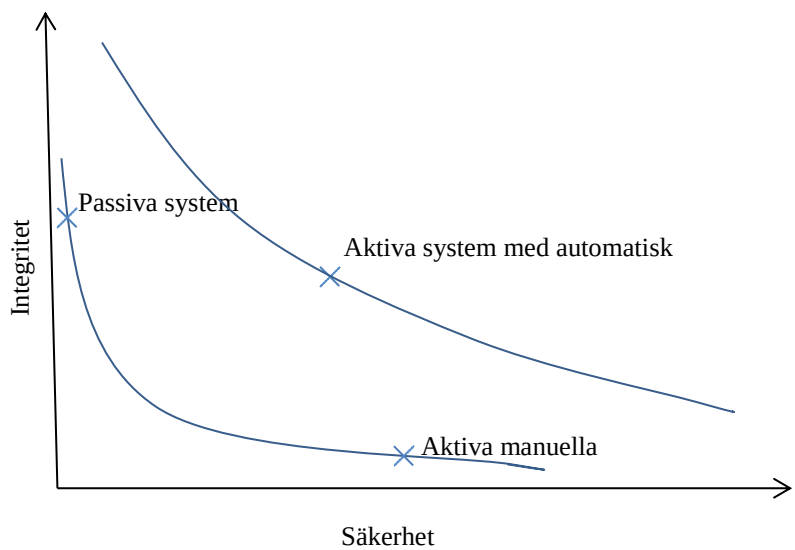
Det finns åtgärder man kan genomföra för att bättre tillgodose integritetsbehov vid övervakning. Man tar hjälp av automatisk analys av bilder vilken ger information och bilder behöver inte presenteras för operatören. Den automatiska analysen kan integreras i kameran och systemet kan konstrueras så att det inte kan lämna ut bilder. Det finns många praktiska skäl till att man vill komma åt bilder på distans till exempel för att underhålla och sköta systemet. Man kan behöva verifiera att systemet fungerar och ett test är att titta på bilderna. Men om det är ett väsentligt krav att inga bilder ska komma ut så kan systemet konstrueras så att detta är omöjligt, till exempel genom att informationen från kameran skickas via SMS. Det blir då praktiskt omöjligt att skicka bilder från kameran eftersom varje SMS rymmer väldigt lite information. Dock är det svårt för allmänheten att veta vilken sorts system som kameran används till. De som ser övervakningskameran måste lita på att systemet är sådant som det sägs vara.

Övervakningssystemen blir mindre och mindre och därmed mindre påträngande. Förr var kameror stora och hade ett stort objektiv, ett öga som tittade på omgivningen. Det var lätt att känna sig uttittad. Idag är kameror betydligt mindre

och själva linsen kan vara så liten att den är svår att upptäcka, vilket gör att man inte behöver känna sig uttittad. Å andra sidan så är förstås risken större att det finns övervakningskameror som man inte upptäcker, och man alltså inte ens behöver vara medveten om att det finns övervakningskameror.

Det läggs stora resurser på forskning kring automatiserad bildanalys för övervakningssystem. Samtidigt finns det en oro för att den ökande användningen av kameraövervakning kommer att leda till ökande missbruk av övervakningsbilder och information från övervakningssystem. Både missbruk där enskilda personer sprider bilder och information på ett otillåtet sätt och en systematisk ändamålsglidning där myndigheter och organisationer använder bilder och information i allt fler sammanhang, som inte har direkt med det ursprungliga syftet att göra. Genom framstegen inom automatisk bildanalys kommer det att kunna byggas övervakningssystem med kameror som har en betydligt mer specifik funktion än att visa och spela in video från ett visst område.

När övervakningssystem med kameror kommer att kunna kallas falldetektor, överfallslarm, överträdelsedetektor, trafikbeteendeövervakning, och som inte kommer kunna användas som något annat, så minskar risken för kränkning av oskyldigas personliga integritet. Figur 2 visar schematiskt motsättningen mellan integritet och säkerhet som kameraövervakningssystem för med sig och hur förhållande mellan integritet och säkerhet kan förbättras med automatisk bildanalys.



Figur 2. Figuren visar schematiskt avvägningen som man måste göra mellan integritet och säkerhet.

Med aktiva, manuella system kan man uppnå en relativt hög grad av säkerhet, men det kan samtidigt vara svårt att skydda personers integritet. Med passiva system finns det bättre möjligheter att värna personers integritet, men säkerheten minskar eftersom det inte finns någon bevakningsoperatör som kan slå larm. Aktiva system med automatisk bildanalys gör att man kan uppnå både bättre säkerhet och bättre skydd av integriteten.

Ansvaret för säkerhet och skyddet av individers integritet

Det ingår ofta som en del i forskningen att undersöka vilka etiska och juridiska krav som ställs på övervakningssystemen och ta reda på vilka möjligheter som finns att leva upp till kraven. När det gäller tillämpad forskning så är det väsentligt att systemen som utvecklas uppfyller långtgående etiska och juridiska krav så att systemen har förutsättningar att kunna användas. Forskning om tekniska system kan inte lämna svar på hur olika intressen ska vägas mot varandra men den kan lämna svar på vilka valmöjligheter som finns. Övervakningssystem ska så långt möjligt ge både säkerhet och integritet. Sedan är det upp till lagstiftare och de som ska använda övervakningssystemen hur man vill kompromissa mellan olika intressen.

Vidare läsning

- Andersson, M., Gustafsson, F. and St-Laurent, L., Recognition of anomalous motion patterns in urban surveillance, IEEE Journal of Selected Topics in Signal Processing, vol. 7, nummer 1, 2013.
- Andersson, M., Rydell, J., St-Laurent, L., Prévost, D. and Gustafsson, F., Crowd Analysis with Target Tracking, K-means Clustering and Hidden Markov Models, 15th International Conference on Information Fusion, Singapore, 2012-07-09 - 2012-07-12, s.1903-1910.
- www.adabts-fp7.eu

12 Trygghetssystem med inbyggt integritetsskydd för falldetektion

Steven J Savage, Henrik Allberg, Erika Emilsson, Joakim Rydell och Björn Larsson

Idag sker en snabb demografisk förändring i Sverige, med en ökande andel äldre personer. I takt med befolkningens ökade livslängd ställs större krav på samhället när det gäller vård och omsorg. Det uppstår ett behov av självständiga och trygga boendealternativ för äldre, där den personliga integriteten och livskvalitén kan säkerställas. I takt med att befolkningen åldras ökar dock även antalet olyckor som de är inblandade i. Av dessa olyckor är fallolyckor det kanske största problemet, vilket tydligt syns i statistiken. Fallolyckor är ett samhällsproblem som orsakar stor smärta och lidande för såväl de direkt drabbade som deras anhöriga. Dessa olyckor kostar samhället stora belopp varje år, i form av sjukhusvistelser och rehabilitering.

Det finns således behov av en trygghetslösning som kan ge äldre personer det stöd de behöver utan att göra intrång i deras privatliv. Helst ska lösningen kunna användas både i en normal bostad såväl som i ett boende anpassat för äldre personer. Redan idag finns det teknik utvecklad som skulle kunna anpassas för dessa behov. Teknikutvecklingen för sensorer[8] och datorprocessorer har lett fram till en miniatyrisering som kan vara särskilt intressant i detta sammanhang.

FOI studerar hur sensorer, som automatiskt detekterar fallolyckor, kan användas som trygghetssystem utan att inkräkta på integriteten hos den person som är i

[8] En sensor är ett tekniskt eller biologiskt system som samlar in, konverterar och i vissa fall sänder någon form av signal, stimuli eller data. Människans fem sinnen är exempel på olika biologiska sensorer.

behov av hjälp och stöd. Bland annat har FOI tagit fram en tekniklösning som använder enkla, billiga och kommersiellt tillgängliga sensorer som visar att man kan göra stora förbättringar med små medel. Resultaten skulle kunna användas i hemmiljö eller integreras i större system.

Fallolyckor och deras konsekvenser

Fall är den typ av olyckor som äldre är mest utsatta för. Varje år vårdas över 70 000 personer på sjukhus på grund av att de har varit med om fallolyckor. I sjukvården är denna grupp överrepresenterad med nästan fem gånger så många personskador än de som sker till följd av olyckor i trafiken. Vidare är det omkring tre gånger så många som omkommer på grund av fallolyckor i jämförelse med antalet som dör vid olyckor i trafiken. Omkring 90 % av de som avlider på grund av fallolyckor är 65 år eller äldre.

Konsekvenserna av dessa olyckor drabbar även samhället hårt. Detta har varit drivkraften för att med utgångspunkt från system som tagits fram för militära tillämpningar, utveckla och tillämpa sensorteknik för falldetektion med civila syften. Verksamheten har haft som mål att utveckla ett system som kan detektera och larma tidigt för inträffade olyckor eller varna för förstadier till olyckor, innan situationen utvecklats till ett akut läge. Som exempel kan här nämnas att om en person ramlar men lyckas resa sig igen, så tyder detta på att olycksfallet troligtvis kommer att få begränsade konsekvenser. Däremot om personen blir liggande, och eventuellt skadad i timmar utan att kunna kommunicera med omvärlden, kan situationen få allvarligare konsekvenser med livshotande skador som följd. Genom tidig detektion av olycksfall kopplat till ett beslutsstödsystem skulle mer kvalificerade larm med sammanvägd information om situationen kunna skickas, vilket skulle stödja hjälpinstanser med beslut om åtgärder.

Vilket krav kan man ställa på en falldetektor?

I dag finns det ett par vanliga lösningar som används för att påkalla hjälp i samband med att en olycka sker i hemmet. Bland annat finns personburna trygghetslarm, som kan bäras runt handleden eller kring halsen. I viss utsträckning används även rörelsesensorer, som ger ett larm så fort en person rör sig. Personburna larm kräver dock att de just finns inom räckhåll vid behov. Många äldre glömmer eller väljer av olika anledningar (avsiktligt) att inte använda larm. Den sensor som reagerar på rörelse är istället överkänslig och larmar vid minsta rörelse (då personen går till toaletten, hämtar ett glas vatten, etc.), och alltså inte enbart vid fall. Denna sensors överkänslighet leder till många falsklarm.

För att minimera den tid en person blir liggande i samband med ett fall så skulle det vara önskvärt att använda en detektor som inte är personburen, men som ändå

bara larmar i samband med att en person faktiskt har ramlat. En sådan falldetektor ska ge larm när en person har legat orörlig på golvet en viss tid. Den ska fungera i såväl ljus som mörker. Av integritetsskäl bör systemet inte vidarebefordra visuella bilder. I händelse av en olycka ska systemet till exempel kunna skicka larm till en anhörig eller personalen vid ett vårdboende.

Systemet ska även kunna vara till hjälp för att förbättra hemmiljöer så att risken för fallolyckor minskar. Detta skulle kunna göras om falldetektorn kan användas för att ta reda på vissa orsaker till fall, till exempel tröskel, mattkant, längre tids balansproblem.

Beskrivning av en falldetektor

Många sensorer används i dag i diverse konsumentprodukter. Detta leder ofta till en ökad efterfrågan med en snabbare teknikutveckling och billigare enheter som resultat. En relativt billig sensor, en så kallad avståndsmätande kamera, finns bland annat i TV-speltillbehöret Kinect, som är avsedd att fungera som styrenhet till Microsofts spelkonsol Xbox 360.

Den avståndsmätande kameran är en sensor som, med hjälp av en osynlig och ofarlig infraröd laser, *mäter avstånd* till de objekt, till exempel en person eller möbler som finns inom synfältet. Detta skiljer avståndskameran från en vanlig kamera (visuell kamera), som mäter *infallande ljus* från objekten inom synfältet. Avståndsmätningen genererar djupbilder, som den som visas till vänster i Bild 1 nedan. En motsvarande visuell bild visas till höger. I djupbilder kan människor förhållandevis lätt segmenteras ut (det vill säga hittas och avgränsas) från omgivningen med hjälp av bildanalysteknik. Tekniken i den avståndsmätande kameran har alltså den fördelen att den inte gör samma intrång i individens privatliv som en visuell kamera.

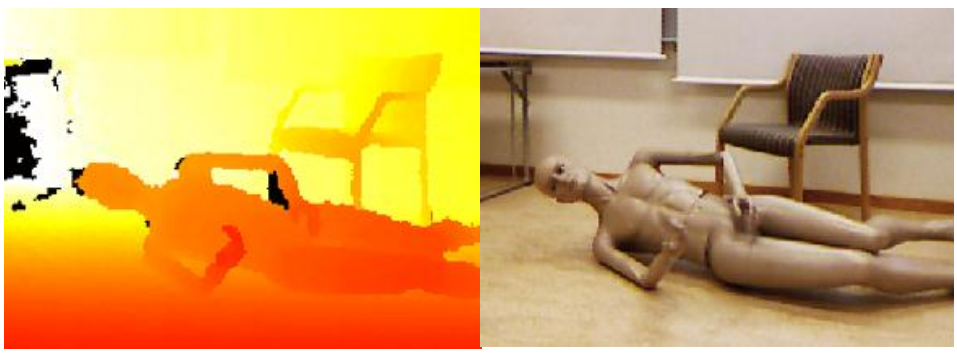


Bild 1: Bilden från avståndkameran (vänster) som används i falldetektorn och motsvarande från en visuell kamera (höger).

Utifrån djupbilderna segmenteras även positionen för ett antal kroppsdelar (arm, ben, huvud, etc.) som sedan följs i syfte att upptäcka när en person faller. Bild 2 visar ett datorproducerat ”skelett” som har anpassats till de följda kroppsdelarna, överlagrat på en visuell bild. (Den visuella bilden är inte nödvändig för att följa kroppsdelar, utan används enbart för att illustrera metoden.) Eftersom en avståndsmätande kamera baseras på aktiv belysning (en Kinect sänder ut ljus i en våglängd där det inte förekommer något annat ljus inomhus, och har en kamera som bara ser ljus i just den våglängden) fungerar detta även i mörker.

För att detektera fall följs hela tiden huvudets position. Om huvudet under en längre tid befinner sig under en viss höjd anses detta vara ett tecken på att personen har fallit. Om huvudet är på väg nedåt och därefter försvinner ut ur synfältet, betraktas även det som ett misstänkt fall. En sådan situation uppstår till exempel då en person faller ner bakom möbler som skymmer sikten för den avståndsmätande kameran. När ett fall eller ett misstänkt fall har detekterats, kan ett larm utlösas.

Bild 2: Visuell bild med ett överlagrat skelett, baserat på mätningar från avståndsbilden.

Tekniken har visat sig fungera bra för att detektera fall i flera olika miljöer. Sensorn i Kinect är dock i första hand anpassad för användning i spel, och har därför ett smalare synfält än det som skulle ha varit optimalt för falldetektion. Tekniken har även testats i miljöer som vanligtvis ger falsklarm, till exempel där det finns husdjur, och har då visat sig fungera tillfredsställande. De erfarenheter som gjorts med systemet visar, att i ett praktiskt användbart system baserat på samma teknik bör en liknande sensor, men med delvis andra egenskaper, användas.

När flera personer finns inom synfältet samtidigt kan detektorn avaktiveras. Detta görs eftersom den person som inte har fallit förväntas kunna hjälpa den andra, alternativt påkalla hjälp. Detta är ytterligare ett sätt att bevara integriteten hos personen som monitoreras. Avaktivering görs automatiskt genom att tekniken räknar antalet personer i synfältet.

Användarens perspektiv

Det finns tre grupper som skulle kunna dra nytta av ett trygghetssystem som kan detektera fall. Dels den äldre person som har systemet installerat hos sig, dels anhöriga och vänner till den som använder systemet, och dels organisationer med ansvar för de äldres välfärd. De som har nytta av systemet kan således indelas i primära, sekundära och tertiära användare.

Primära användare
En primär användare är en som har direkt nytta av systemet, till exempel en äldre person med någon form av rörelsehinder. En sådan användare kan leva ett mer eller mindre självständigt liv ensam eller tillsammans med någon, men skulle ha nytta av ytterligare stöd för att förhindra att en mindre olycka (till exempel ett fall) utvecklas till en allvarligare händelse. Det primära syftet med systemet är att skapa trygghet hos den enskilde personen. Ett sekundärt syfte är att förlänga ett aktivt och självständigt liv genom att denna trygghet behövs för att fortsätta leva ett aktivt liv både fysiskt och psykiskt.

För de primära användarna fungerar inte alltid befintliga larm i alla situationer. Till exempel kan en person med dagens larmsystem ta av sig en larmknapp och lägga den ifrån sig, eller falla så olyckligt att larmknappen hamnar under kroppen och bli oåtkomlig. Personen kan också bli chockad och helt enkelt inte komma ihåg att larmknappen finns. Snabbare och mer noggranna larm som är specifikt framtagna för att detektera fall är önskvärda då många av dagens larm bara bygger på enkel rörelsedetektion.

Sekundära användare
En sekundär användare är en som indirekt har nytta av systemet, exempelvis en vän eller anhörig till en primär användare, eller någon som är oroad för en äldre persons säkerhet och välbefinnande. En sekundär användare kommer också att dra nytta av systemet genom att en tryggare kontakt möjliggörs, genom att anpassa besöken efter rådande behov. Ett sådant exempel kan vara när en äldre person vaknar mitt i natten och blir förvirrad och desorienterad. Ett tillstånd som kan leda till potentiellt farliga situationer såsom att personen går ut mitt i natten, ibland otillräckligt klädd, eller orsakar störning och olägenhet både för sig själv och närboende.

Tertiära användare
Denna grupp av användare är mindre väldefinierad, men består huvudsakligen av användare som till exempel organisationer med ansvar för de äldres välfärd. Exempel är vårdhem (offentliga och privata), vårdcentraler, försäkringsbolag, transportsystemansvariga samt lokala och statliga skyddsorganisationer.

En genomförd behovsanalys visar vidare att fallprevention måste ses i ett större perspektiv. I första hand identifieras idag på vilka platser fallen sker i störst utsträckning, denna information sparas sedan i ett nationellt register, Senior Alert, där de arbetar med prevention av olyckor. Där analyserar man i första hand var riskerna finns och anpassar därefter åtgärderna efter den boendes behov, som till exempel att ta bort mattor från golvet och anpassa höjden på en fåtölj. Till detta blir nya tekniklösningar ett komplement som ytterligare skall stärka den äldres trygghet.

Flera grupper av äldre skulle vara behjälpta av systemet. Det kan bland annat vara de som har problem med yrsel eller de med lågt eller högt blodtryck, vilket kan göra personen ostadig på benen.

På grund av komplexiteten i situationen med flera olika användare och avsaknad av en tydlig huvudman/problemägare är det svårt att utveckla ett komplett system eller egentligen ett system av system som motsvarar behoven. Det som sker i dag är att olika aktörer (oftast forskarlag eller små företag med begränsade resurser) utvecklar och marknadsför en mindre del eller komponent av ett system. Visserligen kan komponenten användas fristående men komponenterna kan sällan användas tillsammans i ett större system.

Beslutsstöd

Ett enda system har svårt att erbjuda fullständig tillförlitlighet i alla situationer. Vardagens alla situationer och människors normala beteenden är alldeles för unika för detta. Därför krävs beslutsstödsystem som kan använda information från ett flertal olika källor. Ett beslutstödssystem skulle kunna minska osäkerheten om en situation genom att tillhandahålla så bra underlag som möjligt med hänsyn tagen till sjukdomshistoria, symptom och sensordata.

Bättre beslutsunderlag skulle i förlängningen leda till mer konsekventa beslut och att situationer som liknar varandra hanteras på samma sätt varje gång de inträffar. Standardiserade lösningar skulle således möjliggöras. Målet med beslutstödssystemet är alltså att uppnå konsekventa bedömningar av situationer för att säkrare, snabbare och effektivare möjliggöra beslut som på bästa sätt åtgärdar en uppkommen situation.

För att beslutsfattaren ska acceptera och få förtroende för beslutstödssystemet är det viktigt att det förser operatören med tillförlitlig information, som till exempel att antalet falsklarm hålls på en acceptabelt låg nivå. Mängden av information och typ av information måste dessutom vara hanterbar för att inte överbelasta larmoperatören/sjuksköterskan. Det är också viktigt att systemet är lätt att hantera och att det är transparent, det vill säga att det är möjligt för beslutsfattaren att göra en rimlighetsbedömning av det som systemet varnar för.

Etik och integritet

Det är vanligt med övervakning av allmänna platser, till exempel flygplatser, i handeln och utomhus i stadsmiljö med visuella kameror, etc. I dessa fall görs bedömningen att nyttan (oftast förbättrad säkerhet) väger tyngre än intrånget i den personliga integriteten. Om liknande teknik införs i en mycket mer integritetskänslig miljö (det egna hemmet, sovrummet, badrummet, etc.) finns det stora risker att systemet inte kommer att accepteras. Av denna anledning bör systemet integrerats med ”*privacy by design*”-begreppet, det vill säga inbyggd integritet i systemet som koncept.

Den avståndsmätande kameran i en Kinect levererar avståndsbilder av den typ som visas till vänster i figur 1. Man bör ta ställning till om den typen av bilder är integritetskränkande, och i vilken utsträckning de behöver skyddas. Kinect har även en visuell kamera, som tar vanliga färgbilder. Om en falldetektor även borde ha en visuell kamera är en öppen fråga som måste utredas. I så fall är det också viktigt att utreda hur man ska skydda bilder, så att de bara kommer rätt personer till del. Det bör även kontrolleras om den typen av bilder ska skickas vidare. Tekniken kan vidareutvecklas för att ytterligare slå vakt om personlig integritet. Om visuella bilder ändå är nödvändiga kan integritetsintrånget minimeras genom uppdelning av den information som bilden innehåller. Genom att dela upp informationen i olika flöden/kanaler som hanteras separat kan man separera personen från sammanhanget (vad personen gör), datumet och klockslag (när aktiviteten görs) och positionen (var aktiviteten sker). De flesta av dessa begränsningar är inte applicerbara på dagens monitoreringssystem, men är värt att notera i ”*privacy by design”* – konceptet för framtiden. (Ytterligare resonemang om integritetsproblemet med kamreaövervakning finns i artikel 11).

Relevansen för individen och samhället

Fallolyckor är bara en anledning, även om den är en uppenbar sådan, till varför vi måste betrakta säkerhet ur ett brett perspektiv. Oftast ses säkerhet som en fråga som berör samhället i stort, men för att säkerställa en bra livskvalité för människor i högre ålder och samtidigt slippa tvinga allt fler äldre flytta till speciella (och dyra) boenden måste vi påbörja utveckling av större och mer sammanhängande system, det vill säga system av system.

Det är inte överdrivet att konstatera att ”samhällssäkerheten flyttar in i vardagsrummet och skapar trygghet för alla”. Ny teknik som bygger på modern och billig konsumentelektronik öppnar nya möjligheter för ökad tryggheten i hemmet genom att automatiskt detektera fallolyckor. Dessa falldetektorer behöver dock inte offra den personliga integriteten om ”privacy by design”-principer tillämpas vid utformandet av sådana system, vilket är nödvändigt om det ska kunna accepteras i hemmet. Fallolyckor är dock bara en mindre del av ett komplext problem som samhället måste hantera. För att kunna närma sig en lösning krävs mer än bara de delsystem som finns idag, det krävs utveckling och implementering av beslutsstödsystem där varningssignaler från olika delsystem kan tas emot, bearbetas och valideras. Då flera olika användare inom olika verksamheter skulle använda sig av ett sådant system är finansiering och uppbyggnad av sådana system ytterst komplex.

Vidare läsning

- Savage, S.J., Allberg, H., Emilsson, E., Larsson, B., Nilsson, T., Peolsson, M., Rydell, J. och Stenborg, K.-G. Ett proaktivt trygghetssystem – slutrapport, FOI-R--3515--SE, nov 2012.

13 Behovet av bättre CBRN-krisberedskap

Ann Göransson Nyberg

Scanpix: Jeppe Gustafsson

Vid en oväntad exponering av kemiska (C) biologiska (B), radiologiska (R) eller nukleära (N) ämnen kan många individer skadas. Politiska mål i Europeiska unionen (EU) anger att krisberedskapen mot avsiktliga eller oavsiktliga kemiska och radiologiska katastrofer ska stärkas. Sådana händelser torde kunna utveckla sig över landsgränserna varför en gemensam planering och hantering bör eftersträvas. Men hur implementeras målen i medlemsstaterna?

Bakgrund

I stora delar av samhället, inom industri, forskning, energiproduktion, sjukvård med mera, används omfattande mängder med CBRN-ämnen (se vidare artikel *Farligt avfall – återvinna eller deponera*). För att minska risken för att människor, djur och miljö ska exponeras för dessa ämnen finns olika lagar och föreskrifter för hantering. Ändå sker ibland oavsiktlig spridning av farliga ämnen genom till exempel olyckor med farligt godstransporter, läckage vid

anläggningar eller stora utbrott av smitta. Det finns dessutom risk för någon form av avsiktlig användning av CBRN-ämnen i syfte att skada människor, miljö eller egendom.

Våra möjligheter att möta CBRN-hot eller -olyckor kommer att bero på hur väl förberedda vi är. Det är därför viktigt att formulera tydliga och konkreta risk- och hotbildsbedömningar inom CBRN-området som kan ge underlag till bland annat myndigheternas risk- och sårbarhetsanalyser och vidare beslut om åtgärder på olika samhällsnivåer. Det är också av central betydelse att det finns förmåga i Sverige och EU att tekniskt och medicinskt kunna bedöma olika ämnens egenskaper och verkan samt möjligheter att detektera, analysera och skydda oss mot CBRN-ämnen.

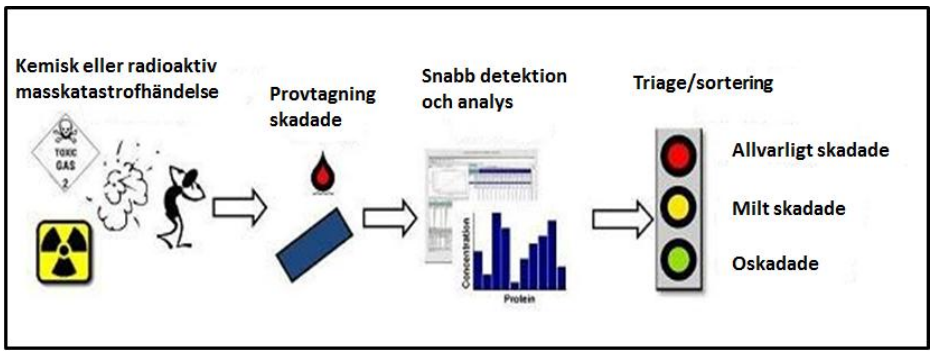
En akut masskadehändelse efter exponering av giftiga kemikalier och/eller radioaktiva ämnen kan utvecklas mycket snabbt och nå en magnitud tillräcklig för att leda till en katastrofal krissituation i samhället. En sådan händelse skulle Sverige ha svårt att hantera utan stöd från andra länder. Enligt EU är en för medlemsstaterna allmän beredskapsplanering och förmåga att fungera effektivt tillsammans viktiga nycklar för att minska effekterna av till exempel en kemikalieolycka. Kemikalier kan med stor sannolikhet också spridas till angränsande land/länder.

Vad gäller hälso- och sjukvård finns inom området inga formella överenskommelser på EU-nivå för att samordna insatserna vid kemiska händelser. Hittills har utgångspunkten varit överenskommelser från fall till fall som tydligt har visat på behovet av en strukturerad process för riskbedömning och samordning av offentliga sjuk- och hälsovårdsmyndigheters agerande på EU-nivå.

När viktiga hörnstenar i samhällets beredskap för och skydd mot CBRN-ämnen bygger på riskbedömningar, planering och skyddsåtgärder som samhället har vidtagit på en rad olika organisatoriska nivåer, blir kunskap och utbildning av största vikt för att ett väl fungerande skyddskoncept ska lyckas i praktiken. En förutsättning är att berörda parter vet hur man agerar i en CBRN-miljö, att nödvändig utrustning finns tillgänglig och att man vet hur den används. I det av EU-kommissionen sanktionerade projektet MASH (Mass-Casualties and Health Care following the release of toxic chemicals or radioactive materials) genomfördes en bedömning av den katastrofmedicinska beredskapen hos EU:s 27 medlemsstater inför kemiska och radiologiska händelser. Projektet kom att bli avstampet för Sveriges deltagande i en rad nätverk och projekt på EU-nivå inom området.

En bedömning av den katastrofmedicinska beredskapen inom EU:s 27 medlemsstater

Under tre år genomförde FOI tillsammans med sex andra medlemsstater i EU, projektet MASH. Projektet, som i huvudsak leddes av European CBRNE Center (en centrumbildning vid Umeå universitet som arbetar med forskning inom områdena för säkerhet och sårbarhet med avseende på incidenter med CBRN och explosiva (E) ämnen) och FOI, syftade till att bedöma nivån på katastrofmedicinsk beredskap hos EU:s medlemsländer. Hur skulle projektet gå till väga? Utgångspunkten blev att använda sig av en uppsättning realistiska scenarier som innefattar giftiga kemiska eller radioaktiva ämnen. Via ett webbaserat formulär fick sedan specialister inom CBRN-området svara på frågor rörande deras länders beredskap för katastrofmedicinska situationer vid dessa händelser.



Figur 1. En kemisk eller radioaktiv masskatastrof kan komma att innebära en överväldigande börda för hälso- och sjukvårdssystemet. Schematiskt flödesschema för bedömning av masskadeoffer vid exponering för farliga ämnen.

Större utsläpp av giftiga kemikalier eller skadliga radiologiska ämnen kan komma att innebära en överväldigande börda för hälso-och sjukvårdssystemet. Projektet identifierade flera områden som måste förbättras. För att höja kapaciteten hos medlemsstaterna att handskas med en masskada orsakad av kemiska eller radioaktiva substanser visade det sig finnas behov av bättre samspel genom utvecklade metoder för information och kommunikation. Ett annat utvecklingsområde visade sig avse effektiva metoder för möjlighet till diagnostik och omhändertagande av skadade (se vidare artikel *Biomarkörer för att identifiera kemisk lungskada*). En central slutsats av projektet visade att kompetens och engagemang vad gäller krisberedskap hos katastrofmedicinsk personal saknas eller är otillfredsställande låg.

Resultaten från projektet visade också att Sverige inte är unikt i fråga om brist på kunskap och samspel mellan olika aktörer inom katastrofmedicin. Ska EU:s

medlemsstater kunna bistå varandra vid gränsöverskridande olyckor, avsiktliga såväl som oavsiktliga, är det en förutsättning att varje land i första hand har fungerande beredskap som i sin tur kan länkas ihop med andra länders beredskap.

Projektet rekommenderade på lång sikt att insatserna koncentreras till den katastrofmedicinska personalen. Former måste utvecklas för kommunikation och aktiviteter som stimulerar till ökad kapacitet att hantera masskadehändelser till följd av kemiska eller radiologiska utsläpp. För att motivera berörda aktörer att engagera sig i och bidra till en ökad krisberedskap inom EU inför sådana händelser måste processer möjligöras och definieras. Den katastrofmedicinska personalen är den primära målgruppen, men på längre sikt är hälsovårdsmyndigheterna, som arbetar nära regeringen, den viktigaste målgruppen som ansvariga för genomförandet av politiska ambitioner som berör krisberedskapen vid masskadehändelser. Att nå bortom de politiska ambitionerna och aktivera intresse och motivation där skadeinsatserna ska ske är en av stora utmaningarna på området.

Den allmänna rekommendationen från MASH-projektet är att öka krisberedskapen bland EU:s medlemsstater vid katastrofmedicinska situationer, särskilt de som rör kemiska och radiologiska ämnen. Detta måste göras på ett sätt som innebär att "komplettera, stödja och ge ett mervärde till medlemsstaternas politik och bidra till ökad solidaritet och välfärd i Europeiska unionen" (Commission decision, Co D, 2009/964/EU). Det långsiktiga målet är att mildra effekterna av masskadehändelser på sjukvården i medlemsstaterna. Sådana åtgärder ligger väl i linje med EU-kommissionens ansträngningar att göra vårt samhälle mer motståndskraftigt och därför säkrare.

Ett exempel på hur arbetet går vidare

Projektet MASH innebar ett avstamp för Sveriges deltagande i en rad nätverk och projekt på EU-nivå. Ett exempel på ett nystartat sådant projekt inom CBRN-området där arbetet bedrivs vidare, är det som FOI nu tillsammans med forskare från flera andra EU-länder ska genomföra. Projektet inriktar sig på samverkan och samordning av hälso- och sjukvårdsinsatser vid gränsöverskridande händelser och syftar till att säkra en på EU-nivån effektiv och sammanhållen reaktionsförmåga vid allvarliga gränsöverskridande händelser som orsakas av kemiska ämnen.

Detta ska bland annat åstadkommas genom att ett pilotnätverk på EU-nivå inrättas. Nätverket ska ha förbindelser med alla befintliga EU-mekanismer och -strukturer som har utvecklats och införts, till exempel ”Lessons Learned”-programmet under EU:s Civilskyddsmekanism som rör större katastrofer, inbegripet kemiska händelser, då mekanismen aktiveras. Nätverket förväntas i detta sammanhang bidra till en viktig erfarenhetsåterföring mellan

medlemsstaterna. Detta är särskilt värdefullt för stater med en lägre grad av kapacitet och expertis att hantera kemiska händelser. Vidare ska nätverket ge en uppfattning kring om det är nödvändigt att vidta ytterligare åtgärder och hur omfattande dessa i så fall ska vara. Projektet ska också utveckla ”verktyg”, som till exempel gemensamma riktlinjer och metoder för kommunikation, så att nätverkets förmåga kan breddas samt kompetensen och kapaciteten inom hälso- och sjukvårdsområdet ökas.

Avslutning

Svensk krisberedskap är djupt invävd i den europeiska, inte minst vad gäller hanteringen av kemiska och radiologiska händelser. I EU finns såväl intentioner och mål som ett starkt behov av att förbättra nuvarande insatsförmåga mot avsiktliga och oavsiktliga kemiska och radiologiska händelser och i det sammanhanget förbättra skyddet av de europeiska medborgarna. EU:s ambitioner för hantering av sådana risker implementeras inte i tillräcklig omfattning hos berörda aktörer i medlemsstaterna. Arbetet fortgår på EU-nivå men skillnaden mellan politiska mål för akuta masskadesituationer å ena sidan och relativa brister på medverkan kring sådan krisberedskap av katastrofmedicinsk personal å andra sidan, utgör ett av de stora problemen på området. Motivationshöjande insatser och tydliga riktlinjer kan avsevärt förbättra Sveriges och EU:s krisberedskap för att hantera kemiska och radiologiska masskadehändelser.

Vidare läsning

- Göransson Nyberg, A., Stricklin, D. and Sellström, Å. 2011. Mass Casualties and Health Care Following the Release of Toxic Chemicals or Radioactive Material - Contribution of Modern Biotechnology. Int. J. Environ. Res. Public Health 2011, 8(12), 4521-4549 FOI-S--3883--SE. http://www.mdpi.com/1660-4601/8/12/4521

- Göransson Nyberg, A., Baker, D., Watson, S., Holmes, S., Mobbs, S. and Murray, V. 2011. Foresight into Needs, Possibilities and Information Requirements for the Future. MASH EAHC Project 2007/209. FOI-S--3748--SE. http://ec.europa.eu/eahc/projects/database.html

- Sellström, Å. MASs-casualties and Health-care following the release of toxic chemicals or radioactive materials - MASH. Chemical Hazards and Poisons Report From the Chemical Hazards and Poisons Division, April 2009, Issue 14, p. 34. http://www.hpa.org.uk/webc/HPAwebFile/HPAweb_C/1242717232594

INTERVJU

14 Simuleringsstöd för samhällssäkerhet

Intervju med Christian Carling

***Christian Carling** är forskningsledare och har arbetat med utveckling av ledning och samordning i civil och militär krishantering sedan 1995. De senaste åren har han främst ägnat åt flera stora projekt inom Europeiska unionens (EU:s) säkerhetsforskningsprogram, om havsövervakning, hamnskydd, CBRN-olyckor och säkerhetshot i stora kollektivtrafiksystem.*

– Utvecklingen i våra större städer skapar och omformar ständigt en redan komplex och svårbedömd riskbild. Samtidigt är de verktyg som idag används för bedömningar av fysiska olyckor ytterst förenklade, förklarar Christian Carling, forskningsledare vid FOI. Därför, förklarar Christian vidare, har FOI sedan 2011 bedrivit ett forskningsprojekt som har involverat ett tjugotal FOI-forskare, för att utveckla verktyg för att stödja samhällets hantering av kriser kopplade till större olyckor. Genom att samla FOI:s kompetens inom många områden, från modellering och simulering till spridningsberäkningar och toxikologi, har man kunnat skapa en plattform för att flexibelt kunna sätta samman situationsanpassade simuleringsverktyg. Tekniken bygger på att man kombinerar beprövade modeller, som var och en simulerar en del i händelseutvecklingen. Modellerna kan återanvändas och bytas ut efter behov, för att på bästa sätt skapa en sammansatt modell för varje given situation. På så vis blir det möjligt att studera invecklade händelsekedjor, från olycka eller attack, till effekt på människor och omgivning, utan att bygga en ny modell för varje typ av händelse, betonar Christian Carling.

Som en första tillämpning för att demonstrera tekniken, förklarar Christian Carling, har vi undersökt hur simuleringsplattformen kan stödja arbetet med insatsplanering vid gasutsläpp i en stor tätort. Arbetet har förankrats i den praktiska verkligheten genom samverkan med personer från den kommunala räddningstjänsten. I demonstrationen ingår modeller som simulerar utsläpp och spridning av gasen, befolkningens rörelser i tätorten och hur de påverkas av gasexponeringen. Till skillnad från traditionella modeller som bara simulerar spridningen över en fri yta har vi använt en 3D-modell över tätorten i Norrköping, där varje hus och gata är noggrant modellerad. Den högupplösta gasspridningsmodellen visar många effekter som inte ses i enklare simuleringar;

bland annat ser man uppkomsten av kraftiga virvelbildningar och flöden mot vindriktningen, som skapas av den komplicerade stadsmiljön. Redan detta ger anledning att se över var man väljer att gruppera räddningstjänsten för insats i området. I området simuleras också en befolkning på 20 000 individer som självständigt tar sig mellan bostäder och arbete, men reagerar på gasen, beroende på vilken exponering man fått. Resultatet från simuleringen är framförallt ett bedömt skadeutfall, vilket indikerar det akuta vårdbehovet, förklarar Christian Carling.

Figur 1. Framtagen 3D-modell över Norrköping.

– Vi har också använt simuleringsplattformen i ett EU-projekt där vi studerat effekten av gasspridning i tunnelbanemiljö, där risken för omfattande skadeutfall är stor, förklarar Christian Carling. I den fortsatta utvecklingen av projektet kommer vi att studera modeller för att simulera andra typer av händelser, till exempel explosioner, lokal smittspridning, utsläpp av farliga ämnen i vatten- och avloppssystem med mera. Vi vill även undersöka om simuleringsplattformen kan användas för att skapa trovärdiga inspel och händelseutveckling under övningar, förklarar Christian Carling. En annan intressant möjlighet är att undersöka hur informationsspridning och alarmering vid olyckor beror på olika tekniker och framförallt, befolkningens agerande påpekar Christian Carling.

– Simuleringsplattformen är på detta sätt en öppen spelplan för att laborera med olika händelser och åtgärder för att bemöta dem avslutar Christian Carling sin redogörelse för hur arbetet med simuleringsplattformen kan stödja samhällets säkerhet.

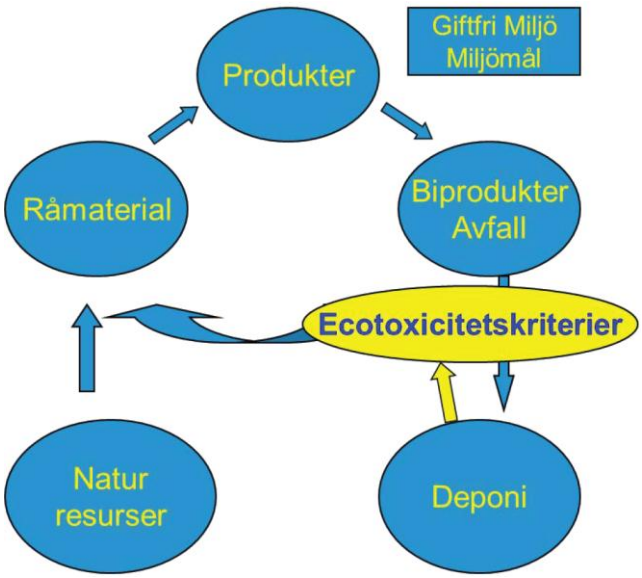
15 Farligt avfall- återvinna eller deponera?

Rune Berglind och Per Leffler

Källa: Silje Bergum Kinsten/norden.org

Produktionen av avfall utgör ett växande miljöhot i Sverige och övriga länder i världen. En mindre del av avfallet är farligt för miljön. Avfall som innehåller miljöfarliga ämnen, ekotoxiskt avfall, kan komma från industrin och från byggsektorn, men också vara aska från förbränning av hushållssopor. Avfallets farlighet för miljö och hälsa avgör om det ska läggas på särskilda deponier för farligt avfall, eller om det kan återbrukas, till exempel som konstruktionsmaterial i vägar. Det vanliga sättet att ta reda på det idag är kemisk analys, vilket rekommenderas av Naturvårdsverket. Den metoden ger tillräcklig information om de ämnen man vet finns i avfallet. Kemisk analys ger dock inte information om det kan finnas kända eller okända ämnen i avfallet som är ekotoxiska. Kemisk analys ger inte heller information om ämnena kommer att tas upp av levande organismer eller om de är bundna i avfallet. Det finns alltså behov av mer effektiva sätt att ta reda på om avfallet är farligt för miljön. Forskningsinstitut inom Europeiska unionen (EU) däribland FOI förespråkar ekotoxikologisk testning kompletterat med kemisk analys av ekotoxiskt avfall inför faroklassificering. Den metoden ger information om alla biologiskt

tillgängliga ämnen och ger därmed ett samlat biologiskt svar på avfallets farlighet. Med hjälp av metoden kan man snabbt avgöra om ett avfall är biologiskt ofarligt och som därmed kan bli en användbar råvara istället för ett avfallsproblem.



Figur 1. Modifierad från Fällman och Svensson, 2006. Kriterier för återvinning av avfall i anläggningsarbeten. Statens Naturvårdsverk (SNV) Förlag

Bakgrund

Varuproduktion har i alla tider genererat biprodukter, ett avfall som antingen har lagts synligt på hög, dumpats under vatten eller grävts ned i deponier. Vår nya tid ser ett alternativ växa fram – återbruk, recycling. Avfall är något som för tillfället är oanvändbart och blivit över. En rest som behöver tas om hand för att inte skapa skräpig otrivsel, orsaka mänsklig ohälsa eller förgiftning av vår miljö, vårt ekosystem och livsrum på jorden. Sett ur ett miljöperspektiv är genereringen av avfall ett exempel på ineffektivitet och bör minimeras i ett resurssnålt samhälle. Avfall som ändå uppstår kan ses som en ny naturresurs att använda i varuproduktion under förutsättning att inga nya farligheter uppstår. EU-lagstiftningen definierar avfall som ett ”ämne eller föremål som innehavaren gör sig av med eller avser eller är skyldig att göra sig av med”. Detta avfall skall återanvändas, återvinnas eller i sämsta fall läggas på deponi för säker förvaring. Deponerat avfall klassificeras i tre kategorier enligt förordning, SFS 2001:512:

- Farligt avfall (som har hög inneboende giftighet) till exempel kreosotförorenad jord
- Icke-farligt avfall (som saknar inneboende giftighet)
- Inert (Icke-reaktivt) avfall till exempel betong

Fortsättningsvis fokuserar denna artikel på farligt avfall och metoder att fastställa ekotoxiskt avfall, sådant avfall som sätter ekosystemet i obalans. Farligt avfall kan vara en blandning av flera kemiska ämnen, varav några är giftiga eller mycket giftiga, andra är explosiva, frätande eller brandfarliga, och ibland även smittspridande. Ämnesblandningen som sådan kan förändra de enskilda ämnenas exponerings- och gifteffektrelaterade egenskaper. I EU:s ”Directive on Waste 2008/98/EC”, beskrivs de inneboende faroegenskaperna hos avfall i 15 huvudtyper av farokoder H1 – H15 (H = Hazard). Farokod H14 ”Ekotoxiskt avfall”, definieras som ”avfall som omedelbart eller på sikt innebär risk för en eller flera miljösektorer”. EU-direktivet har införlivats i den svenska Avfallsförordningen (2011:927) och de myndigheter som särskilt förknippas med farobedömningen av avfall är Naturvårdsverket och Kemikalieinspektionen. Från 2008 till 2011 var FOI en av parterna i Marksaneringscentrum Norr tillsammans med Umeå Universitet, ett EU-projekt med fokus på sanering av förorenad mark. FOI ledde delprojektet ”Recycling and disposition of waste (REDIWASTE)”. Syftet var att genom intervjuer och litteraturstudier sammanfatta kunskapsläget beträffande användning av kemisk analys respektive toxikologisk testning för faroanalys av sådant avfall som specificerats under farokod H14. Intervjuer av representanter för myndigheter, konsulter, forskare och representanter för industri gav en bild av synen på frågan om hur miljöfarligheten hos avfall effektivast och säkrast bör mätas. Hypotesen var att genom en tillräckligt rättvisande metodik bör stora kvantiteter avfall kunna frias för återbruk och en minskad andel avfall avskiljas till deponering om kvarstående ekotoxicitet kunnat fastställas.

Faroklassificering – Svårigheter, Metoder och Bedömningsgrunder

Farligt avfall indelas alltså i 15 faroklasser enligt EU efter egenskaper som till exempel frätande, mutagent (skadar generna), brandfarligt eller reproduktionstoxiskt (skadar fortplantnigen). Klassificeringen följer i stort indelningen av de faroegenskaper som anges för ”kemiska ämnen och produkter” med fokus på hälsorisker för människa. Egenskapen ekotoxiskt (H14) fokuserar på skydd av ekosystemet det vill säga miljön i dagligt tal. Ekotoxiskt avfall är vanligen en blandning av ämnen, både ofarliga och farliga. Varje enskilt ämnes miljöfarliga egenskaper är i många fall kända (till exempel bly, zink, miljögifterna DDT eller PCB). Ett avfall innehåller också ett flertal kända och okända ämnen vars miljöfarliga egenskaper inte har hunnit undersökas

toxikologiskt. För att kunna klassificera avfall som ekotoxiskt, måste en stabil kunskapsbas om dess miljöskadande egenskaper skapas. Klassificeringen kan antingen göras genom mätning av avfallets innehåll av på förhand utvalda ämnen eller genom att testa dess toxicitet i ett eller flera biologiska testsystem. Enligt Naturvårdsverket ska avfallet betraktas som farligt om koncentrationen av ett känt giftigt ämne (angivet som vikt %) är så högt att avfallet uppvisar en eller flera av de egenskaper som anges i bilaga till avfallsförordningen till exempel ekotoxiskt (H14). Vid klassificering av avfall förordar Naturvårdsverket kemisk analys av avfallet och jämförelse med gränsvärden som grund vid bedömning av dess farlighet. Mot denna ståndpunkt står mätning av den samlade giftigheten i avfallet i toxikologiska modellsystem. Direkt mätning av giftighet är fullt möjlig i miniatyriserade modellsystem som har kapacitet att klara av många mätprover på kort tid.

Farlighetsbestämning med kemisk analys

Kemisk analys bygger på att avfallets ursprung är känt, helt eller delvis. Huvuddelarnas kända innehåll av farliga ämnen kan då uppskattas och vilka farliga ämnen som ska identifieras och kvantifieras kan väljas ut som bas för farlighetsklassificeringen. Om avfallet antas innehålla ett flertal farliga ämnen ska koncentrationerna av alla dessa ämnen bestämmas. Prov på avfallet, alternativt vattenextrakt av avfallet, skickas till certifierat laboratorium för kemisk analys och identifiering och kvantifiering enligt vissa standardiserade mätmetoder. Med utgångspunkt från koncentrationerna av valda farliga ämnen i provet, görs en jämförelse med gränsvärden för dessa ämnen och en bedömning om avfallet ska klassificeras som ekotoxiskt. Om koncentrationerna av enskilda farliga ämnen resulterar i att avfallet inte klassificeras som farligt, görs en sammanvägning av dessa enligt anvisningar av Naturvårdsverket. En svaghet med kemisk analys är att det är enbart de ämnen som har valts ut och analyserats som kommer med i bedömningen. Samverkanseffekter mellan ämnen kan inte beräknas utifrån enbart kemisk analys.

Farlighetsbestämning med toxikologisk analys

Kunskap om ett avfalls ursprung är inte avgörande vid en toxikologisk analys av avfall. Prov av ett avfall kan istället tas blint och beredas så att det går att testa på den organism eller de organismer som ska användas i undersökningen. Mätning av ett ämnes effekter (toxicitet) på biologiska testsystem som bakterier, svampar, växter och djur, ger ett mått på dess farlighet vid kortare och längre exponering. Om testet skall göras på en vattenlevande organism, till exempel vattenloppa eller alg, extraheras avfallet med en vattenlösning till ett extrakt under 14 till 24 timmar, varefter organismerna kan exponeras för extraktet. Hur mycket provet behöver spädas för att inte påverka den organism som används i testet utgör ett

mått på farligheten hos provet. Ju mer provet måste spädas ut desto giftigare (farligare) för människan/miljön är provet (avfallet). En bedömningsgrund som flera forskargrupper föreslagit vid farlighetsbedömning är NOEL (No Observed Effect Level) vilket är den högsta testnivå som inte ger någon observerbar effekt på den testorganism som använts. Om provet behöver spädas mer än 10 ggr för att inte ge gifteffekt, bedöms det som farligt. Krävs mer än 100 ggr spädning bedöms det som mycket giftigt. Alla prov som förorsakar genetiska skador bedöms som mycket giftiga.

Uppfattning om bedömningsgrunder hos företrädare för myndigheter, industri och forskare om kriteriet H14

Mot bakgrund av att avfallets farlighet kan bestämmas genom kemisk och/eller toxikologisk analys undersökte forskargruppen vid FOI hur tre olika grupper av aktörer inom avfallssektorn, myndigheter, forskare/konsulter samt stora producenter av avfall, såg på metoder för klassificering av farligt avfall. På den centrala frågan ”Tror du att toxikologiska tester kommer att accepteras som metod för klassificering av farligt avfall?” skilde sig de tre grupperna åt. Företrädare för myndigheterna var tveksamma medan företrädare för konsulter och forskare var positiva till användning av toxikologiska testmetoder (testsystem) för att bestämma farligheten hos avfall. Industriföreträdarna visade en splittrad uppfattning i denna fråga. Forskargruppens tolkning av resultatet är att myndigheter förlitar sig i hög grad på gränsvärden och traditionella analyser. Intervjuade forskare visade, kanske av ren nyfikenhet, en öppnare och flexiblare syn på hur farobedömning av avfall bör ske med bibehållen säkerhet. Vanligt var att forskare ville kombinera toxikologiska test på avfallet med kemisk analys för att kunna spåra troliga orsaker till ett utfall. Industrin har sannolikt större intresse i att få saken avdömd än valet av metod vid bestämning av avfallets farlighet.

Forskares uppfattning om farlighetsbestämning av avfall

I Sverige och internationellt anser forskare som är verksamma inom miljöforskningen att miljöfarlighetsbedömning av avfall och förorenad mark, sediment och vatten samt av varor och kemiska produkter bör ske med hjälp av biologiska testmetoder. Internationella organisationer som Organisationen för ekonomiskt samarbete och utveckling (OECD), Europeiska Unionen (EU) och Internationella Standardiseringsorganisationen (ISO) samt nationella organisationer som Standardiseringskommissionen i Sverige (SIS) och naturvårdsverket i USA (US-EPA) har givit ut riktlinjer som kan användas för att undersöka miljöfarligheten hos avfall. Dessa testmetoder omfattar land- och

vattenmiljöer, prokaryota (organismer utan cellkärna till exempel bakterier) och eukaryota organismer (med cellkärna – svampar, växter och djur), djur och växter, samt rutiner för hantering av prover och beredning av extrakt från fasta prover. Fördelen med att använda biologiska testmetoder (testsystem) vid bestämning av ett avfalls miljöfarlighet anges vara:

- Provets hela effektegenskaper undersöks – det vill säga alla ämnen kommer med, kända ämnen, okända ämnen, ej påvisade ämnen, och kända ämnen med okänd giftighet, inklusive interaktioner mellan ämnena
- Koncentrationsnivåer av extrakt för akuta respektive kroniska effekter kan bestämmas
- Lägsta koncentrationer för uppkomst av olika typer av effekter som tillväxt- och reproduktionsstörningar, hormonstörningar eller uppkomst av kromosomskador

Användningen av biologiska testsystem vid bedömning av farligt avfall (H14) varierar mellan olika länder inom EU. Till skillnad från till exempel Frankrike och Finland, har Sverige inte någon rekommendation eller uttalad rutin för att använda biologiska testmetoder för att bedöma miljöfarligheten hos avfall av kategorin H14. Bland de länder som använder biologiska testmetoder använder några länder kombinationer av olika testmetoder, medan andra länder använder endast enstaka testmetoder. Som en reaktion på den bristande harmoniseringen av vilka metoder som används har upprättats förslag på kombinationer av olika testsystem i testbatterier som är anpassade för att täcka de flesta ämnens toxikologiska egenskaper. I ett ekotoxikologiskt testbatteri bör testsystem som representerar land-och vattenmiljöer, bakterier, växter och djur ingå.

Undersökningar har gjorts angående samstämmigheten mellan toxikologisk test och kemisk analys vid bedömning av farligheten hos avfall. För majoriteten av undersökta avfall fanns ingen korrelation mellan utvalda analyserade giftiga ämnen och utfallen i toxicitetstesterna. Den kemiska analysen av utvalda ämnen i undersökta avfall kunde därmed inte ge tillräcklig information för att rangordna avfallens miljöfarlighet. Toxikologisk testning med en kombination av 3-5 olika ekotoxikologiska testmetoder (testbatteri) av samma avfall gav resultat som möjliggjorde en rangordning av avfallen. Avfall och därmed också extrakten av avfall har komplex sammansättning och innehåller många icke förutsägbara och ej analyserade organiska föreningar med okända egenskaper. Forskarnas slutsats var att toxikologisk testning av avfall beskriver avfallets farliga egenskaper i sin helhet. Kemisk analys gav en fragmenterad bild och fokuserade enbart på de ämnen som hade valts ut på förhand mot bakgrund av avfallets ursprung och valda ämnens kända farliga egenskaper.

Avslutning

En framtida avfallshantering kan med ett förändrat synsätt generera en ökad råvarubas för flera industriella produktlinjer. Pappersåtervinning och elektronikåtervinning är två goda exempel på hur avfall blivit återvinningsbara restprodukter. Friklassning av farligt avfall baserat på toxikologisk screening enligt föreslagna modeller kan dessutom innebära en reducering i uttaget av naturresurser från ekosystemen. En ökad återanvändning av friklassat (ofarligt) avfall innebär en reducerad mängd deponerat avfall, en minskad övervakningsplikt av farliga avfall och ett säkrare samhälle.

16 Biomarkörer för att identifiera kemisk lungskada

Elisabeth Wigenstam

Stora volymer giftiga industrikemikalier transporteras på våra vägar idag, främst med tåg men även med lastbilar. Trots att säkerhetsrutinerna kring dessa är rigorösa finns ändå risken för att en allvarlig olycka sker. Ett snabbt och korrekt omhändertagande av skadade är av yttersta vikt för att så många som möjligt ska klara sig utan allvarliga skador. På en olycksplats kan flera hundra personer vara i riskzonen för allvarliga skador. Hur avgör man vilka som kräver behandling och vilka som kan gå hem utan medicinering? Det finns även personer som inte har några synliga symptom, men ändå har exponerats för den giftiga gasen. Dessa individer är lätta att missa om man bara söker synliga tecken på skada. Författaren vill med den här artikeln belysa vikten av att få fram så kallade biomarkörer, små proteiner som meddelar om det finns förhöjd risk för skada vid en exponering.

Farliga industrikemikalier

De vanligaste förekommande toxiska industrigaserna (klorgas, ammoniak och svaveldioxid) är några exempel på lungskadande ämnen som ger upphov till

akuta vävnadsskador i övre luftrör och bronker. Vid höga koncentrationer utvecklas skadorna till en svårartad inflammation och vätskeansamling i luftvägarna som i värsta fall kan vara livshotande. Mycket allvarlig förgiftning ger förutom andningssvårigheter även medvetslöshet och cirkulationskollaps.

Klor är en av de viktigaste kemikalierna inom den kemiska industrin och framställs i industriell skala. Klor används vid tillverkning av polyvinylklorid (PVC) som är en av de vanligaste plasterna och tidigare användes för blekning av pappersmassa. Även i dricksvatten, simbassänger och som desinfektionsmedel används klor. Klorgas är starkt giftigt. Det är irriterande på ögon, andningsorgan och hud vid relativt låga koncentrationer. Redan vid halter på två-tre gram per kubikmeter luft kan den vara dödlig.

Ammoniak har många användningsområden; som rengöringsmedel, i hårfärg, för ugnsrengöring och rengöring av guld samt vid tillverkning av gödsel, salpetersyra och plaster. Ämnet används även som köldmedium i köldmaskinerier. Vid exponering för ammoniak är det främst hudskador och inhalationsskador som uppstår men explosionsrisken är också stor vid olycka.

Svaveldioxid används främst för tillverkning av svavelsyra. Eftersom svaveldioxid kondenserar vid -10 °C så kan gasen lätt göras flytande med till exempel torris och fraktas lätt. Svaveldioxid används även i matindustrin som konserveringsmedel (nummer E 220) och i pappers- och massaindustrin i sulfitprocessen för tillverkning av kemisk pappersmassa. Vid en olycka uppstår huvudsakliga skador i luftvägar och andningsorgan. Symptomen kan i stigande skala vara irritation i andningsvägar och ögon – hosta – andnöd – medvetslöshet – andningsstillestånd. Vätskeexponering eller exponering för extremt höga gaskoncentrationer kan dessutom ge frätskador på huden.

När olyckan är framme

Natten till den 3 december 1984 inträffade den största kemiska katastrofolyckan någonsin till följd av ett massivt utsläpp av metylisocyanat från en pesticidfabrik i Bhopal, Indien. En tredjedel av stadens invånare (ca 800 000) utsattes för utsläppet och dödssiffran uppskattades till minst 20 000 offer. Ytterligare tusental fick kronisk lungskada och lider än idag av men efter olyckan.

Den 6 januari 2005 kolliderade två godståg i Graniteville, South Carolina, USA (bild 1). Uppskattningsvis frigjordes 11 500 liter klorgas, vilket orsakade nio dödsoffer och minst 529 personer sökte medicinsk behandling för eventuell klorexponering. Flera tusen invånare var tvungna att evakuera sina hem under två veckors tid medan sanering pågick.

Bild 1: Granitville, USA, 2005 Bild från Wikimedia Commons

I Sverige har vi hittills varit förskonade från någon allvarligare kemisk olyckssituation med allvarliga personskador, men i Kungsbacka var det nära. Måndagen den 28 februari 2005 spårade ett godståg ur norr om Kungsbacka. Tåget var lastat med drygt 700 ton kondenserad klorgas. Inget av den giftiga klorgasen läckte ut och ingen person kom till skada vid olyckan, men bärgningsarbetet tog tre veckor och kostade mångmiljonbelopp.

I maj 1976 körde en långtradare lastad med över 30 kubikmeter ammoniak av vägen och kraschade ner på Southwest Freeway i Houston, USA. Kraschen orsakade ett utsläpp av ett stort moln av ammoniak och gav upphov till allvarliga lungskador hos de som andades in röken. Sju personer dog, 78 personer blev svårt skadade och ytterligare ett hundratal behövde läkarvård. Många av dessa utvecklade kroniska skador och lider än idag av nedsatt lungfunktion.

Biomarkörer

En biomarkör är en substans i människokroppen som kan användas för att identifiera ett biologiskt tillstånd. Kliniskt användbara biomarkörer kan hjälpa till att bestämma sjukdomsrisk, sjukdomens förekomst eller sjukdomens svårighetsgrad. För att kunna identifiera en kliniskt användbar biomarkör måste forskarna bestämma vilka substanser i kroppen som har samband med den aktuella sjukdomen och sedan utveckla en metod för att ta prov och testa.

En ideal biomarkör i detta sammanhang bör vara lungspecifik och gå lätt att mäta hos ett stort antal människor. Vid en skada kan lungspecifika proteiner läcka ut i blodet när cellerna i lungan förstörs. Kan man då detektera dessa proteiner i ett blodprov, urinprov eller i utandningsluft finns bevis på att personen är skadad och behöver vård.

Vid exponering för en kemikale av typen klorgas eller ammoniak är det mycket troligt att lungorna påverkas. Inandning av dessa gaser kan orsaka allvarliga skador såväl akut som på längre sikt. Det är därför viktigt att snabbt kunna hitta exponerade personer och bestämma hur allvarlig skadan är för att sedan sätta in bästa möjliga behandling.

Vad gör forskarna?

En bättre förståelse för hur den kemiska lungskadan uppstår ökar möjligheten att utveckla och förfina nya behandlingsmetoder. Konceptet att använda inflammatoriska förändringar som biomarkörer har inte tidigare studerats vid exponeringar för högtoxiska kemiska ämnen, men har prövats för diagnostik av andra miljörelaterade lungsjukdomar såsom astma och kroniskt obstruktiv lungsjukdom (KOL).

Individer utsatta för bland annat klorgas riskerar att få bestående luftvägsskador. Genom att använda tidiga inflammatoriska förändringar som biomarkörer för lungskada skapas utvecklingsmöjligheter för såväl diagnostik som prognosbedömning samt förståelse för hur den kemiska lungskadan uppstår. Detta kan i sin tur leda till utveckling av nya behandlingsmetoder.

På FOI bedrivs ett arbete med målsättningen att 1) identifiera biomarkörer som kan hjälpa oss att hitta skadade individer utan uppenbart synliga symptom och 2) utveckla verktyg för klinisk diagnostik som kan förutsäga risken för långtidsverkande och kvarstående skador. Genom laborativt arbete har i detalj undersökts vad som händer i lungorna vid en engångsexponering för ett starkt lungskadande ämne. Genom analys av lungsköljvätska och serum finns idag kunskap om vilka proteiner som får ett högre uttryck, det vill säga förekommer i större mängder i exponerade lungor, jämfört med friska lungor. Utmaningen ligger nu i att kunna detektera dessa proteiner även i utandningsluft och urin. Vid en olycka som kräver snabbt omhändertagande hinner vårdpersonal inte ta blodprover för analys, utan för att dessa biomarkörer ska fungera vid allvarliga händelser måste ett snabbprov genom exempelvis utandningsluft kunna tas fram.

Att forskning inom detta område är viktigt framgår inte minst av de kemiska katastrofer som inträffat den senaste tiden, till exempel explosionen av en konstgödselfabrik i april 2013 i Texas, USA, som krävde flera dödsoffer och flera hundra skadade, många till följd av de giftiga ångor som spreds.

Vilken är relevansen för Sverige och Europeiska unionen (EU)?

Toxiska industrigaser produceras och distribueras i stora mängder i Sverige, Om det skulle ske en kemisk katastrofsituation med extremt hög belastning på

vårdkedjan skulle möjligheter till snabb diagnostik av kemiska olycksoffer ge förbättrade möjligheter till riktat och fokuserat omhändertagande av de individer som är i störst behov av vård, och därmed skulle omfattande insatser på icke skadade eller lindrigt skadade individer kunna undvikas.

Vidare kan en olycka ske var som helst, ibland även över nationsgränser. I dessa fall blir det oerhört viktigt att olika länders räddningssystem kan synkroniseras och att inte fördröjningar i omhändertagande sker på grund av brister i kommunikation. FOI är partner i flera olika EU-projekt med syftet att främja gränsöverskridande samarbete (se vidare artikel *Behovet av bättre CBRN-krisberedskap*). I dessa projekt arbetar flera europeiska länder tillsammans för en lösning. Inom projekten försöker man, förutom protokoll och mallar, ta fram verktyg som går att använda ute i fält. En viktig del i detta arbete är att ta fram biomarkörer specifika för lungskadande ämnen.

Slutord

En kemisk katastrofsituation kan uppstå när som helst, var som helst. Även om det inte sker frekvent måste ändå beredskapen finnas och ambulanspersonal och räddningstjänst vara beredda på hur de ska agera i olika situationer. Genom att ta fram nya biomarkörer och hitta snabba och korrekta metoder för analys av dessa hoppas forskarna på FOI kunna bistå med en viktig del i omhändertagandet av patienter efter en kemisk olycka.

Vidare läsning

- Göransson Nyberg, A. ”Klorgaskatastrofen i South Carolina 2005 - medicinska konsekvenser.” FOI MEMO 3512
- Wigenstam, E. och Bucht, A. ”Sammanställning av långtidseffekter av senapsgas efter Iran-Irak-kriget, 1980-1988.” FOI MEMO 3657
- Eriksson, H. och Östlund, H. ”Insatsplan för olycka med svaveldioxid i Umeå.” Räddningsverket FOU-rapport

17 Hemmagjorda bomber – det trygga samhällets fiende

Malin Kölhed, Patrik Krumlinde, Hans Önnerud och Henric Östmark

Viktiga utgångsämnen för tillverkning av hemmagjorda bomber är lätta att komma över. FOI bedriver forskning för att försvåra otillåten användning av vissa av dessa utgångsämnen och därigenom minska det totala hotet från hemmagjorda bomber.

Bakgrund

Hemmagjorda sprängmedel, HME (HomeMade Explosives), är ett hot mot samhällets och medborgarnas trygghet av några enkla skäl; det finns terroristgrupper som hotar samhället, det är lätt för allmänheten att komma över grundläggande utgångsämnen, utrustning för tillverkning av sprängmedel och bomber kan inhandlas i många vanliga butiker och det finns rikliga möjligheter att skaffa sig information om hur sådan tillverkning sker, både från öppna källor som internetforum eller via direkt kunskapsöverföring inom terroristgrupper.

Men hur enkelt är det egentligen att tillverka en bomb, hur pålitliga är recepten och hur lätt är det att få tag på de nödvändiga ingredienserna?

Dessa frågor är alla grundläggande och i all väsentlighet fortfarande obesvarade av sprängämnesexperter och forskare, eftersom kunskaperna om de tillhörande grundläggande fysikaliska och kemiska processerna är otillräckliga. Anledningen är att hemmagjorda bomber inte har någon naturlig plats i samhället eftersom sprängämnen är väldigt instabila och därmed känsliga, vilket gör dem mycket farliga.

Otillåten tillverkning av sprängämnen

I kampen för att förebygga att bombattentat sker är det väsentligt att arbeta i alla steg för motåtgärder. Det handlar om att försvåra tillverkning av sprängämnen, lokalisera illegala bombfabriker samt detektera bomber för att på ett tidigt skede öka möjligheten att finna terrorister och stoppa en planerad attack. En bombfabrik kan rymmas i en lägenhet i en storstad eller vara placerad på en enslig plats långt ifrån städer. Utrustningen som används är ofta det som finns enkelt tillgängligt för alla konsumenter. Var de än är placerade så är det mycket svårt att hitta dessa bombfabriker. Europeiska kommissionen lämnar idag bidrag till flera forskningsprojekt med just detta syfte.

För att vara maximalt proaktiv i kampen mot terrorismen måste man beakta hela kedjan av terroristhandlingar som föregår själva verkställandet av en terroristattack. När bomben väl är utplacerad i samhället är tiden väldigt knapp för att motverka attacken. FOI bedriver innovativ forskning för att förhindra eller åtminstone göra det betydligt svårare att överhuvudtaget tillverka hemmagjorda bomber. Denna forskning går ut på att finna ämnen att tillsätta till vanliga vardagskemikalier, vilka terrorister använder för bombtillverkning, för att därigenom på kemisk väg försvåra eller förhindra själva produktionen av sprängmedel. När det tar längre tid att tillverka bomben kan spaningspersonal få mer tid på sig vid sökningen efter bombfabriken. Det kan också tvinga terroristerna att välja andra typer av hemmagjorda sprängmedel, vilket ytterligare ökar den tid som spanarna har på sig att förebygga en planerad terroristattack.

Bombattentat urholkar trygghetskänslan hos oskyldiga människor

I juli 2005 sprängdes fyra bomber på kort tid i morgonrusningen i centrala London i England. Denna koordinerade terroristattack tydde på noggrann och detaljerad planering av ett terroristnätverk. Senare visade de kriminaltekniska undersökningarna att en viss typ av HME hade använts, antingen som så kallade initiatorsystem eller som huvudladdning och att bombfabriken hade funnits i en lägenhet i staden Leeds i England.

Bild 1: Bombningarna i London 2005. Scanpix: Peter Macdiarmid

Den 22 juli 2011 drabbades Europa återigen av en förfärlig terroristattack, när Anders Behring Breivik efter noggrann planering sprängde en lastbil fylld med HME utanför regeringsbyggnaden i Oslo. Detta HME bestod, enligt den kriminaltekniska undersökningen, av närmare 1000 kg konstgödsel, vilket hade inhandlats i Norge och omvandlats till HME efter omsorgsfulla förberedelser och ett omfattande kemiskt arbete. Vid attacken dog åtta personer, men antalet skadade och döda kunde blivit mycket större om inte bilen med HME hade ställts direkt ovanför ett parkeringsgarage, samtidigt som många personer som arbetade i eller i närheten av regeringsbyggnaden befann sig på annan plats när explosionen inträffade. (Ett stort antal människor mördades senare samma dag i en annan terroristhandling utförd av samma gärningsman). Förstörelsen på de närliggande byggnaderna var omfattande, till följd av den stora mängden sprängmedel och de omfattande splittereffekterna.

Polisutredningen visade senare att terroristen provat sprängmedlet för att vara säker på att hans bomb skulle fungera. (En analys av fönsterkross spelade en betydande roll i den kriminaltekniska undersökningen med målet att bedöma hur stor laddningen hade varit. Läs mer om fönsterkrossanalys i artikel *Glas – vackert men farligt*.) Det är dock inte alltid så att allt sprängmedel i en terroristattack verkligen detonerar. Exempelvis skedde en självmordsbombning på Bryggargatan i Stockholm 2010 där bara en del av sprängmedlen detonerade, vilket gjorde att det endast var självmordsbombaren själv som dog i attacken. Ett annat exempel där alla bomber inte detonerade är tågsprängningen i Madrid 2004 då tio bomber visserligen sprängdes med stor skadeverkan och många offer, men där polisen senare hittade flera bomber vilka aldrig hade detonerat.

Bild 2: Gatan efter bombningen i centrala Oslo 2011. Scanpix: Karl Melander/Sydsvenskan

Behovet av säkerhetsforskning är enormt

För specialisten är det naturligtvis enkelt att under kontrollerade förhållanden tillverka en bomb, men vid improviserad tillverkning kan det lyckligtvis inträffa många saker som gör att bomben inte detonerar vid den planerade attacken. Detta ger möjligheter att vidta motåtgärder i form av forskning för ett säkrare samhälle. Det är viktigt att identifiera de steg i en improviserad bombtillverkningsprocess där motåtgärder ger störst effekt för att förhindra uppkomst av ett explosivt ämne. Det kan till exempel handla om att förändra de kemiska eller fysikaliska förhållandena. När man planerar lämpliga motåtgärder måste man ta hänsyn till både den utlösande primärladdningen och huvuddelen av bomben, sekundärladdningen.

Inhibitorkemikalier– en möjlighet att motverka bombangrepp

Improviserad tillverkning av sprängmedel är lätt att genomföra, men det är svårare att avgöra om sprängmedlet kommer att fungera. Terrorister använder material, utrustning och kunskaper som de skaffar sig via kriminella nätverk och eftersom recepten och procedurerna varierar kraftigt får detta stor effekt på slutresultatet. Inte desto mindre måste forskning om motåtgärder vara flexibel

nog för att hitta alla steg som kan förhindra att en HME exploderar, så att ett utgångsämne inte längre kan omvandlas till ett sprängmedel.

Genom att allt fler av utgångsämnena för HME "modifieras" så att de inte längre kan användas för tillverkning av HME, eller att det åtminstone blir mycket svårare att använda dem i detta syfte, så ökar möjligheterna att begränsa antalet terroristattacker i form av bombsprängningar. Därigenom ökar säkerheten för medborgarna och samhällsordningen får ett starkare skydd. En sekundär effekt av att antalet terroristattacker reduceras är att skadorna på och förstörelsen av kritisk infrastruktur minskar. Därmed minskar även de ekonomiska effekterna av sådana infrastrukturella skador med efterföljande behov av återuppbyggnad.

FOI bedriver forskning för att hitta substanser som kan göra att vissa utgångsämnen inte längre kan omvandlas till sprängmedel, med målet att därigenom *minska* vissa stora hot mot de europeiska samhällena. Detta innebär att de europeiska samhällena kan bli mer *proaktiva* i kampen mot terrorismen. Målet för forskningen är att minska hoten från terroristattacker och därigenom öka säkerheten för medborgarna i Sverige och Europa.

Forskningsbehovet inom området explosivämnessäkerhet är enormt, nya terroristattacker inträffar överallt i världen. Den 15 april 2013, detonerade två bomber i anslutning till Bostons maratonlopp i USA. De fulla konsekvenserna från dådet är ännu inte helt klara, men med flera dödade och hundratals skadade belyser detta återigen samhällets sårbarhet och svårigheten för polisiära myndigheter att stoppa bombattentat.

Vidare läsning

- För mer information om den forskning på hämmande substanser i utgångsämnen som bedrivs vid FOI, besök: www.prevail-fp7.eu .
- För mer information om den forskning på sökning efter HME-fabriker som bedrivs vid FOI, besök: www.lotusfp7.eu eller www.emphasis-fp7.eu .
- Andra relevanta projekt på området säkerhet och sprängmedel som samordnas av FOI är: www.hyperion-fp7.eu och www.encounter-fp7.eu .

INTERVJU

18 EU:s handlingsplan för bättre sprängämnessäkerhet

Intervju med Sara Wallin

***Sara Wallin** är fil. dr i fysik och forskningsledare inom explosivämnesdetektion. Hennes expertområden är explosivämnesdetektion och Security of Explosives. Sara har många års erfarenhet av att driva forskningsprojekt, särskilt mot Europeiska unionens (EU:s) 7:e ramprogram. Hon medverkar också i expertgruppen NaG-ExpSec.*

Explosiva ämnen som används vid terrorattacker runtom i världen skördar många människoliv. I vår omedelbara närhet minns vi händelserna i Oslo 2011 och sprängningen på Bryggargatan i Stockholm 2010. Efter bombdåden i Madrid initierade Europeiska unionen (EU) ett arbete kring hur nationer kan förebygga och hantera sådan användning av hemmagjorda bomber. I en handlingsplan har ett antal åtgärder identifierats för förbättring av medlemsstaternas sprängämnessäkerhet (security of explosives).

Hur har handlingsplanen utarbetats?

– År 2007 formaliserades arbetet på EU-nivån i *Explosives Security Experts Task Force*, en expertgrupp där FOI har varit representerade från starten. Expertgruppen presenterade 50 rekommendationer för att förbättra säkerheten i fråga om sprängämnen och därigenom förhindra att explosivämnen används mot samhället. Arbetet utmynnade i att EU-kommissionen senare samma år lade fram denna handlingsplan.

Vad innebär handlingsplanen?

– Den bygger på principerna om förebyggande, detektion och respons och förtecknar sammantaget 47 konkreta åtgärder vilka alla rör det som på engelska heter ”security” och alltså inte handlar om ”safety” – en distinktion som strular till det för oss svenskar som har samma ord för båda. Planen inbegriper såväl medlemsstaterna som EU:s institutioner och den privata sektorn. EU-kommissionen ber medlemsstaterna att minst årligen rapportera om hur långt man kommit med genomförandet.

Hur genomförs handlingsplanen i Sverige?

– Myndigheten för samhällsskydd och beredskap (MSB) och Rikspolisstyrelsen (RPS) har utifrån regeringsuppdrag ett gemensamt ansvar för att tillsätta en nationell arbetsgrupp vars uppgift är att genomföra åtgärder för implementeringen av handlingsplanen i Sverige. Expertgruppen har representation från FOI och ett antal andra berörda myndigheter. För FOI:s del genomförs en del av handlingsplanens åtgärder genom forskningsprojekt, framför allt inom EU:s sjunde ramprogram, där FOI bland annat koordinerar projektet PREVAIL som handlar om att förhindra tillverkning av hemmagjorda sprängämnen.

Vilka är några av utmaningarna på området?

– Generellt är det en utmaning att få så många aktörer att enas kring gemensamma ståndpunkter, i stort och smått, nationellt och internationellt. En del åtgärder kan vara lätta att genomföra medan andra kräver mycket samordning innan de kan genomföras.

– Ett konkret exempel på stora utmaningar finns kring arbetet med begränsning av prekursorer, det vill säga ämnen för framställning av explosiva ämnen. Ett exempel på prekursorer är ammoniumnitrat som till exempel fanns i de kylpåsar som användes som startmaterial vid sprängningen på Bryggargatan och som används som gödningsmedel i stora kvantiteter. Det är ett ämne som lätt ersätts med andra i kylpåsar, men som är svårare att ersätta som gödningsmedel. En utmaning är att begränsa rätt ämnen och så få som möjligt eftersom de flesta utgör viktiga hushålls- och industrikemikalier. Man kan till exempel inte förbjuda socker, men man kan begränsa koncentrationen på den väteperoxid som är lätt tillgänglig för allmänheten. Det kan också handla om information till kemikaliebranschen om att rapportera onormala köp av vissa substanser. Att begränsa antalet prekursorer och tillgängligheten till dem genom lagstiftning som leder till en ökad samhällssäkerhet och samtidigt inte inverkar menligt på produktion och konsumtion är oerhört komplicerat. Det är många intressen som ska komma överens. En viktig utmaning för forskningen i till exempel projektet PREVAIL är därför att hitta ämnen som kan förhindra illegal produktion av explosivämnen från prekursorer, men som inte är farligt eller menligt för prekursorns normala användning. Detta ser ändå ut att kunna vara möjligt i vissa fall, vilket är en enorm vetenskaplig bedrift.

19 Logistiksäkerhet – en grund för vårt välstånd

Sören Jägerhök, Pontus Svenson, Maria Andersson, Christian Carling, Anneli Ehlerding, Anders Elfving, Micael Granström och Anna Pettersson

Den exempellöst snabba välståndsökningen i det moderna samhället vilar till stor del på förmågan att snabbt, effektivt och säkert kunna transportera varor och människor. Allt fler människor pendlar och måste kunna anlända säkert och tillförlitligt. Såväl samhällets mat- och medicinförsörjning som industrier och övrigt näringsliv bygger sin existens på ”just in time”-leveranser (inget tillverkas innan kunden lagt sin beställning för att hålla nere lagerkostnader och ledtider). Störningar och avbrott i transportkedjorna kan därför snabbt skada såväl den enskilda människan som näringsliv och andra viktiga samhällsfunktioner. Kopplat till transportsektorns enorma volym och betydelse finns några speciella hot mot samhällets säkerhet.

1. Den effektiva transportapparaten utnyttjas samhällsskadligt för smuggling av alltifrån illegala ämnen såsom farliga sprängmedel, narkotika och kemikalier till piratkopierade varor, stöldgods och traffickingoffer.

2. Koncentrationen av människor och värdefulla varor i transportsystemen attraherar kriminella organisationer och terrorister.
3. Olyckor, naturkatastrofer, pandemier med mera kan påverka logistikkedjan på ett sätt som ger indirekta skador långt värre än de direkta.

Hoten kan således delas in i hot mot själva logistikkedjan, till exempel stölder, samt hot mot samhället i vidare mening, till exempel smuggling av illegala ämnen. Smuggling och stöld/bedrägeri utgör några av de allvarligaste hoten inom varutransportkedjan i Sverige. Årligen stjäls till exempel stora mängder gods från lastbilar, inte sällan då lastbilarna står parkerade på rastplatser. Stölderna är ofta organiserade av kriminella ligor. För att säkerställa transportfunktionen i det moderna samhället behövs både skydd av själva transportkedjorna (transportgodset och transportinfrastrukturen) och skydd mot smuggling och annat skadligt utnyttjande av transportkedjorna. Ett sätt att skydda samhället är tidig upptäckt och varning vid försök till illegal införsel eller utförsel av varor, till exempel stöldgods. Vad gäller terrordåd inom transportsektorn har Sverige varit förskonat. I anslutning till Behring-Breiviks attentat i Norge 2011 höjdes ändå säkerhetsnivån för delar av transportapparaten, till exempel i Göteborgs hamn. Däremot har den svenska beredskapen mot besvärliga väderförhållanden inom transportsektorn prövats vid många tillfällen. Störningar i gods- och persontrafiken på järnväg har under flera vintrar kostat många aktörer mycket pengar. Säkerhetsresurserna behöver sättas in där de gör störst nytta och där de möter de viktigaste hoten.

Artikeln beskriver inledningsvis hur man, för att avgöra vilka dessa hot är, kan använda riskanalyser. Därefter beskriver författarna olika metoder för att upptäcka hoten och vidare för att hantera/åtgärda dem. Artikeln avslutas med några reflektioner om hur svensk logistiksäkerhet kan förbättras.

Att analysera hot och risker

En förutsättning för att på ett välavvägt sätt kunna bemöta hot mot samhällets säkerhet är givetvis en relevant kännedom om vilka hot som finns och vilka risker de medför för en verksamhet. Utan en balanserad uppfattning om detta riskerar vi inte bara att överraskas av oförutsedda hot utan även att i onödan lägga resurser på skydd mot överdrivna hot.

Riskhanteringen i logistikkedjan försvåras av det stora antalet inblandade aktörer som alla har egna värderingar och preferenser när det gäller att bedöma risker och välja åtgärder. Resultatet blir ofta att risker förskjuts från en plats i kedjan till en annan, från en aktörs ansvar till en annans. Gemensamma metoder för riskanalys och riskvärdering ökar chansen att uppnå en totalt sett bättre

risksituation i logistikkedjan, men försvåras främst genom komplexiteten i systemet.

Risker för kriminalitet i logistikkedjan finns i huvudsak inom fem hotområden; stöld, bedrägeri, smuggling, kapade transporter och korruption. Olyckor och naturkatastrofer kan naturligtvis också få synnerligen allvarliga konsekvenser för varuförsörjning och transportväsen. Även om den allmänna uppfattningen är att naturkatastrofer och korruption är mindre frekventa i vårt land så måste alla hot beaktas när det gäller Sveriges sårbarhet. Logistikkedjans betydelse för världsekonomin och välståndet innebär att också terroristhotet måste beaktas, även om de faktiska förlusterna på grund av direkta terrorhandlingar inte är av samma storleksordning som de för andra hot. Indirekta konsekvenser av terroraktioner är sannolikt större än direkta, till exempel leder förändrade resemönster efter flygplanskapningar till kännbara problem för flygbolagen. Kostnaderna för säkerhetskontroller på världens flygplatser överstiger också de direkta kostnaderna orsakade av terrorhandlingar mot flygtransporter.

Riskanalys är ett moget område, med en etablerad praxis, men också många variationer. I de flesta fall bygger analysen på någon kvantitativ modell för värdering av sannolikheter och konsekvenser för olika händelser. Det uppstår dock ett metodproblem när man försöker använda dessa modeller, väsentligen utvecklade för olyckor, för brottsliga handlingar. Händelserna är ofta så ovanliga att pålitlig statistik saknas. Hoten är i dessa fall dessutom avsiktliga, planerade av en aktör som snabbt kommer att anpassa sig till de nya skyddsåtgärder som utvecklas. Detta skapar en återkoppling mellan hot-risk-åtgärd-hot som den traditionella kvantitativa riskanalysen har svårt att hantera. Därför måste den kvantitativa analysen i dessa fall kompletteras med kvalitativa metoder, exempelvis scenariometodik och spel, för att på ett kreativt sätt fånga upp oväntade risker och resonera om lämpliga åtgärder.

Att detektera hot

När ett hot mot logistikkedjan håller på att realiseras är det viktigt att det kan upptäckas, detekteras. FOI har behandlat problemet med att identifiera de avvikelser i sensorsignaler och informationsflöden som tyder på att något anmärkningsvärt eller avvikande håller på att inträffa. Det är för detta ändamål viktigt att utnyttja all tillgänglig information (från till exempel administrativa system, inpasseringssystem och sensorer). Vid val mellan olika sensorsystemlösningar är det avgörande att känna till både sensorernas prestanda och tillämpningens krav. Ofta kan olika tekniker, metoder och källor komplettera varandra så att säkerhetssystemet blir mer effektivt.

Som tidigare nämnts kan hoten delas in i hot mot samhället i vidare mening då logistikkedjan utnyttjas för skadliga ändamål och hot mot själva logistikkedjan.

Nedan exemplifieras hotdetektion vad gäller smuggling, farliga ämnen och farliga aktörer.

Att detektera smuggling och farliga ämnen

För att upptäcka smuggling behövs detektionsmetoder som kan upptäcka smuggelgods i till exempel containrar. Oftast är det av ekonomiska och praktiska skäl dock inte möjligt att scanna eller inspektera alla containrar, utan det krävs ett urval av containrar att inspektera. För att hantera detta problem utvecklas i ett projekt metoder för att beräkna riskindex för containrar och annan frakt. Riskindexberäkningarna är av nödvändighet dynamiska och använder all tillgänglig information för att försöka sortera ut containrar med störst risk för otillåtet innehåll.

Farliga ämnen gömda i bagage eller fraktgods riskerar att utgöra hot både under och efter transporter såväl på land som på fartyg och i flygplan. Ansamlingen av människor på exempelvis järnvägsstationer, tunnelbanor och flygplatser gör dem också till lockande mål för terrorister. En utplacerad bomb, spridning av giftiga gaser eller radioaktivitet kan få stora konsekvenser inte bara för det land som i första hand drabbas.

Ett allvarligt hot mot luftfarten utgörs av farliga ämnen gömda i handbagage, i kläder eller på passagerare. En stor skillnad jämfört med kontrollen av fraktgods är att flygplatser och säkerhetskontroller måste hantera ett dynamiskt varierande flöde av resenärer, varför det blir viktigt att genomföra snabba kontroller med minimal störning för de resande. Utökade och ändrade kontroller på senare år, efter att flera incidenter har inträffat, har lett till en ökad säkerhet men också till mer krångel för resenärerna. Regelverket kring medförda vätskor skärptes bland annat på grund av ett dåd 2006, där en grupp terrorister försökte detonera hemmagjorda, flytande explosivämnen på flera flygplan från Storbritannien till USA och Kanada. Nuvarande krav att passagerare endast får bära med sig små volymer vätska (100 ml per förpackning) ombord, beror på att dagens utrustning inte anses tillräckligt tillförlitlig för att skilja explosiva vätskor från ofarliga vätskor. Resultaten är särskilt svåra att utvärdera då vätskan ligger inuti bagaget, vilket förklarar att passagerarna måste ta upp de små vätskemängderna ur handbagaget. FOI arbetar i detta sammanhang med att utveckla snabbare och mer selektiva detektionsmetoder baserade på Ramanspektroskopi, en teknik för att identifiera spår av explosivämnen på handbagage som rör sig på transportband. Tekniken är både känslig och snabb samt möjliggör scanning av allt handbagage, vilket inte utförs i dag. Liknande teknik utvecklas också för kontroll av personer och fordon vid gränskontroller.

Med flygfrakt skickas årligen ca 400 000 ton gods till och från Sverige och det är svårt att identifiera sådana transporter med farliga (explosiva eller radioaktiva) ämnen. Stickprovskontroller mot explosivämnen görs med bland annat

spårhundar eller röntgenutrusning, men det saknas effektiva metoder och verktyg för att på ett bra sätt undersöka allt gods som hanteras.

Även vad gäller gömda radioaktiva källor finns idag mycket begränsad detektionskapacitet i Sverige och Europa. Endast ett fåtal system är i bruk, samtidigt som antalet incidenter med strålkällor har ökat sedan slutet av 1990-talet. Radioaktiva ämnen som har gömts luktar inte, syns inte och hörs inte. För att detektera ämnena krävs därför speciella instrument. FOI arbetar bland annat för att förbättra tekniken att hitta explosivämnen och radioaktiva ämnen i transportkedjan och få tekniken tillräckligt billig och snabb.

De detektionsmetoder som nämnts för explosivämnen och radioaktiva ämnen appliceras också på andra håll inom logistikkedjan, till exempel inom posthantering där FOI utvecklar metoder för att kunna genomsöka all post och alla paket. Systemen skulle i framtiden kunna vidareutvecklas till att även hitta spår av droger eller biologiska hotsubstanser när post och paket sorteras.

Att detektera farliga aktörer

För att upptäcka hot mot själva logistikkedjan krävs en annan sorts riskindex. Information från till exempel videoövervakningssystem för att upptäcka intrång eller avvikande beteenden blir väsentlig. Övervakningssystemen bör präglas av en helhetssyn och beakta såväl kostnader som personlig integritet och andra etiska aspekter. En viktig del vid automatisk sensoranalys i övervakningssystem är att minimera antalet falsklarm med bibehållen säker detektion av kritiska händelser. Att korrekt analysera sensordata och automatiskt tolka situationer kan ofta försvåras av variationer i väder- och ljusförhållanden. För att få en god överblick över ett område så är det fördelaktigt att utnyttja mer än en sensor och gärna sensorer av olika typ, till exempel en kombination av optiska och akustiska sensorer samt radar. Felaktiga tolkningar av sensordata uppträder sällan samtidigt i flera sensorer och genom att fusionera data från flera sensorer, samt analysera mönster i data över tiden, så kan viktiga och kritiska händelser lättare urskiljas från det som är ointressant eller har tolkats på ett felaktigt sätt i en enskild sensor. Vanligtvis vill man låta systemet lära in en ”normalbild” över området och sedan larma för avvikelser från denna. Ofta är olika avvikelser olika svåra att upptäcka och man måste därför utgå från den riskanalys som gjorts för att välja vad övervakningssystemen ska vara inställda för.

Videoövervakning är i dessa sammanhang det vanligaste systemet, men information från exempelvis rörelsedetektorer och inbrottslarm kan också ge värdefull information. För att utveckla sensorsystem till låg kostnad kan det ibland vara en fördel att använda till exempel ”billiga” videokameror och istället fokusera på metodik för att enkelt integrera dem i ett sensor- och informationsnätverk. För att med automatiska beslutsstödsfunktioner avlasta operatörerna från rutinmässigt stirrande på sensorbildskärmar behöver

sensorinformationen omvandlas och representeras mer systematiskt så att datorer kan dra slutsatser om den. Två personer nära varandra där armarna rör sig snabbt kan exempelvis vara tecken på slagsmål medan en person där armarna rör sig snabbt istället kan tyda på en åkarbrasa. Lämnar någon aktör ett föremål som kan vara en bomb efter sig? Rör sig någon aktör på ett ovanligt sätt – mot eller tvärs folkströmmen eller dröjer någon sig kvar i ett område där alla brukar hasta förbi? Genom att representera informationen på en högre nivå kan sensorinformation enklare slås samman med annan information och slutsatser dras om några aktörer i området är förknippade med högre risker än vanligt. FOI forskar bland annat kring upptäckt av avvikande beteende hos individer och grupper dels i och omkring folksamlingar, dels på parkeringsplatser för lastbilar.

All information där människors identitet kan fastställas omgärdas av regler för att hindra intrång i den personliga integriteten. Ett antal olika sätt har prövats för att skydda identiteten på personer som rör sig i sensorövervakade områden. En möjlighet är att sensorsystemet kräver en auktoriserad order (som sedan arkiveras) varje gång personidentifierande information visas/förmedlas. Ett problem med att rutinmässigt skydda identiteten på personer i bevakningsområdet är om det just är vissa individer som utgör de största hoten. Då måste larm ges om dessa individer identifieras inom området. Många gånger kan det dessutom vara önskvärt att genomföra identifiering av individer i gamla sensordata efter säkerhetsincidenter. Ny teknik provas för att möjliggöra avbildning genom tonade bilrutor och MC-hjälmvisir och tyg framför ansiktet. Automatisk igenkänning av människors rörelsemönster och att genom lager av tyg kunna se dolda vapen och sprängmedel är andra teknikområden som har utvecklats under senare år, bland annat med sikte på säkerhetskontroller av passagerare på flygplatser. Teknik utvecklas också för att det ska bli möjligt att upptäcka människor bakom väggar eller dörrar.

Att vidta åtgärder mot detekterade hot

För att aktörerna i logistikkedjan effektivt ska kunna minska hot, risker och förluster, och därmed bidra till kontinuiteten i viktiga samhällsfunktioner krävs inte bara att hoten upptäcks och identifieras. De måste också kunna stävjas på något sätt. Det räcker inte att upptäcka hoten tidigt, aktören måste också ha en planering för åtgärder som är juridiskt, ekonomiskt och etiskt försvarbara. För ändamålet kan åtgärdslistor sammanställas. Om till exempel säkerhetssystemet i en terminal upptäcker att ett par personer håller på att klättra över staketet runt området, kan det vara lämpligt att rikta fler kameror mot inkräktarna och att skicka ut en säkerhetspatrull för att avvisa dem. Ofta är det välbetänkt att dessutom kalla på polis för att ha beredskap mot en eskalerande våldsnivå och eventuellt identifiera inkräktarna för en framtida lagsökning. En god beredskap mot hot och risker förutsätter ofta att det finns en plan för vilka åtgärder som ska vidtas på vilka indikationer. Alla tänkbara åtgärder som kan vidtas på någon

indikation kan sammanställas i åtgärdslistor. När ett hot är identifierat kan åtgärdsplaneringen sedan användas för att hjälpa beslutsfattaren att välja rätt handling. För att stödja beslutsfattaren i valet utvecklar FOI stödverktyg för att resonera kring hoten. Målet är att beslutsfattarna inte bara ska få en relevant bild av hur läget är (”situationsförståelse”) utan också att händelseutvecklingen blir begriplig och att tänkbara alternativ för incidenters utveckling lätt ska kunna förutses.

Lika viktigt som att det inte finns hål i stängslet runt en terminal som behöver skydd mot intrång är det att organisationerna genomsyras av relevant säkerhets-medvetande mot till exempel korruption. Frågeställningar som rör organisationens säkerhetsmedvetande är bland annat bakgrundskontroller av anställda, tillträdeskontroll till anläggningar, inspektioner av väskor och fordon vid tillträdeskontrollerna, träning/utbildning och organisationens tålighet mot personförluster. Ett väsentligt element i korruptionsbekämpning är att attester och in/utpasseringstillstånd inte hanteras av olika befattningshavare var för sig utan att dokument kontrasigneras.

Som i andra fall är informationsutbyte mellan de olika aktörerna i logistikkedjan centralt. Både administrativ information och sensorinformation måste analyseras för att upptäcka hot av såväl indirekt karaktär, till exempel smuggling, som direkta hot, till exempel från terrorister. Informationsutbytet har både tekniska och organisatoriska aspekter. Teknikmässigt gäller det att se till att systemen kan kommunicera med varandra och att rätt nivå av säkerhet kan upprätthållas. Semantisk interoperabilitet, det vill säga att en organisation och dess informationssystem kan förstå vad ett annat menar, är ett nyckelbegrepp.

Det är slutligen viktigt att säkerhetstänkandet integreras i de tekniska systemen redan på konstruktionsstadiet. En systemlösning som är helt fokuserad på högsta effektivitet under normala förhållanden kan visa sig bli sårbar mot terrorister och brottslingar liksom mot sällsynta olyckor och naturkatastrofer. Det ger ofta bättre motståndskraft att ha fler tekniska system och en viss överkapacitet för en uppgift även om ett enda slimmat system per uppgift ter sig effektivare i normalfallet. En säkerhetsåtgärd som har visat sig mycket effektiv kan i ett slag bli överspelad av förändringar i hotens uppträdande.

Hur kan svensk logistiksäkerhet förbättras?

Det är tydligt att effektiva sensorer, informationsfusion med beslutsstödssystem och en viss redundans ger ökad tillförlitlighet för logistiksystem. Ofta ger samma åtgärder förbättringar av säkerheten i fler än ett problemperspektiv. Ett exempel på detta är att efter attentatet mot World Trade Centre 2001 höjdes säkerhetsmedvetandet inom flera områden. Det fick till följd att Internationella Sjöfartsorganisationen 2002 tog fram en ny internationell kod för skydd av sjöfart och hamnanläggningar mot terrorism. När den infördes reducerades

stölderna inom hamnområdena i ett slag. Det är därför viktigt att på något sätt i förväg värdera säkerhetsåtgärders effekter mot olika hot och risker för att möjliggöra systematisk optimering av säkerhetsåtgärderna hos olika aktörer.

Beredvilligheten att öka säkerheten i logistikkedjan varierar dock liksom inom andra sektorer med upplevd hotnivå och mellan olika organisationer. Kraven på ökad säkerhet behöver balanseras. För att få perspektiv på området behövs också insikten att alla säkerhetsåtgärder som vidtas utan att det finns relevanta hot är slöseri med pengar och urholkar konkurrenskraften för organisationer och nationer. Medan till exempel smuggling är ett omfattande problem för samhället i stort och tullen i synnerhet är det inte av så stor betydelse för fraktbolagen som mer akut oroas av svinn och avbrott i leveranskedjan.

En viktig aspekt för kommersiella aktörer är kostnaden för säkerhetssystemet. Det anses dock självklart att säkerhetsåtgärder som direkt kan avräknas mot minskat svinn, lägre försäkringspremier eller ökad marknadsandel bör genomföras. Kan ökad säkerhet och ökad effektivitet uppnås samtidigt är det heller inte svårt att övertyga beslutsfattarna att satsa på säkerhetsåtgärder. Ökad säkerhet mot mycket sällsynta händelser medför dock ofta en ökad kostnad utan någon tydlig ekonomisk fördel. Tvingande direktiv från någon myndighet om att vissa säkerhetsrutiner/åtgärder måste vidtas över hela Europa torde underlätta acceptansen för sådana åtgärder bland transportsektorns kommersiella aktörer och göra åtgärderna konkurrensneutrala över hela den inre marknaden.

Ett annat exempel på drivkrafter inom transportsäkerhetsområdet gäller frågan om flygpassagerares medförande av vätskor i handbagaget, tänkbara hotscenarior med flytande explosivämnen har ovan belysts. Säkerhetskraven i kombination med avsaknaden av en säker och billig teknik för klassificering av vätskor i plast- och glasflaskor gör att tusentals liter dryck och konserver kasseras varje år vid säkerhetskontrollerna i världens flygplatser. Det ekonomiska trycket från affärsidkarna på flygplatserna att ta bort vätskebegränsningarna är också mycket stort. När en tillräckligt säker och billig teknik finns tillgänglig kommer därför bestämmelserna att förändras. Några flygplatser i Australien har redan infört teknik som klassificerar vätskor och därmed lättat på bestämmelserna om att passagerare endast får medföra mycket små vätskemängder i handbagaget.

I de projekt inom Europeiska unionen (EU) som författarna deltar i och som denna artikel beskriver resultat ifrån, medverkar flera svenska aktörer, både som projektpartners och som medlemmar i referensgrupper och liknande. De får naturligtvis god insyn och kännedom om möjligheterna till förbättrad logistiksäkerhet. Projekten är dessutom aktiva i att sprida information. De brukar bland annat ordna demonstrationer där landvinningarna konkret visas upp. Detta gör det möjligt för aktörerna i den svenska försörjningskedjan att dra nytta av forskningen. Det är alltså en kombination av tekniska möjligheter, politiska beslut och kommersiella drivkrafter som ger samhället de säkerhetssystem det har inom logistikområdet. Det är viktigt att hela tiden låta de olika

hotperspektiven vara levande så att alla aktörer strävar efter att med sina begränsade resurser vidta de säkerhetsåtgärder som motverkar flest hot istället för att enbart fokusera på nyupptäckta akuta säkerhetsbrister.

Vidare läsning

- Franke, U., Johansson, R., Mårtenson, C. och Svenson, P. ”Fusion av information från heterogena källor”, FOI-R--3453--SE, 2012.
- Fensel, A., Rogger, M., Gustavi, T., Horndahol, A. and Mårtenson, C. ”Semantic data management: sensor-based port security use case”, EISIC 2013.
- Gustavi, T. and Svenson, P. “Taxonomy for port security systems”, SecOnT 2013.

20 Glas – vackert men farligt

Annika Lööf

Den moderna citykärnan idag består av mängder av glasade fasader - vackra men sårbara. Fönsterglas är den svagaste länken i en fasad vid en explosion och resulterar i många sekundära skador både inuti och utanför byggnaden. Internationell terrorism har ökat behovet av kunskap kring effekten på glasfasader utsatta för explosiva laster. Grupper av terrorister skapar uppmärksamhet för sina åsikter genom att orsaka ekonomiska förluster, kaos och politiska bryderier. Ett sätt att åstadkomma detta är att placera och detonera en bomb i ett utsatt område så som ett industriellt eller kommersiellt centrum. Verkan från explosioner i anslutning till byggnader ger på grund av glassplitter omfattande skador på både personer och materiel, i och utanför de påverkade byggnaderna.

FOI har i ett samarbete inom Europeiska unionen (EU) fått möjligheten att jämföra resultat och nå längre i slutsatserna kring just dödligheten av fönsterglas. Inom projektet har funderingarna kretsat kring hur befintliga miljöer kan förbättras, vad som bör betänkas inför nybyggnation och tillvägagångssätt vid en önskad höjning av säkerhetsnivån i befintliga miljöer.

Glaset i vårt samhälle

Vad är glas? Glasets grundläggande funktion är att släppa in ljus, vilket visat sig spela en betydande roll för vårt välbefinnande. Vanligt glas tillverkas av sand, soda och kalk med små tillsatser av magnesium, aluminium och järn. Glas är ett gammalt material och det betraktades länge som en lyxvara, mellan åren 1743 och 1809 fick man i Sverige till och med betala skatt för det. Under 1920-talet började maskinglas tillverkas. Därmed kunde glasformaten varieras mer än tidigare och antalet användningsområden öka. Glasrutor har förändrats mycket under årens lopp och varje tidsperiod har haft ”sina” fönster. Arkitekturen runt om oss har påverkats i en riktning för att spegla vår självbild av ett öppet och överskådligt samhälle, vilket har gjort att just glas har blivit ett favoritmaterial i alla delar av byggnadskonstruktionerna. Fasader, dörrar, räcken, golv och hissar är exempel på idag vanliga användningsområden, se till exempel New World Trade Building i New York och Europeiska Centralbanken i Frankfurt. Detta innebär att kraven på glasets egenskaper har skärpts för tillämpningar inom bland annat brandskydd, bullerdämpning, energisparande samt skydd mot personskador och inbrott. Var och en av dessa tillämpningar kräver specifika egenskaper. Dessa och ytterligare några egenskaper går att bygga in i en enda glaskonstruktion genom en väl definierad kravprofil på den önskade slutprodukten. En väl fungerande glaskonstruktion består ofta av flera rutor, och ibland i konstruktion med en tilläggslösning i form av en skyddsfilm, bombgardin eller försänkt infästning.

Farligt glas

Tryckvågen från en terroristbomb, IED (Improvised Explosive Device), vilken skulle kunna innehålla det hemmagjorda sprängmedlet (HME) (se vidare artikel *Hemmagjorda bomber – det trygga samhällets fiende*) eller en olycka med transport av farligt material är mycket kraftigare och ger ett snabbare skadeförlopp än till exempel väderfenomen. Det finns dock vissa extrema naturliga förhållanden vilka kan generera liknande effekter, så som meteoritnedslag och vulkanutbrott. En anordning med explosivämne som detonerar genererar ett tryck som beror av massan hos laddningen. Det tryck som uppkommer beror självklart på hur bomben är tillverkad och vad den består av, men generellt bedöms emellertid att en klassificering av hot bör ske efter laddningsvikten. Detta ger i sin tur en uppdelning beroende på hur bomben förmodas transporteras, såsom i en väska, bil eller lastbil. Viktigt att veta är att vid en detonation blir det inte bara en tryckvåg, utan området kan också utsättas för undertryck som kan resultera i stora skador på så att säga ”fel sida” om fasaden. Denna form av terrorhot har tvingat oss att omdefiniera begreppet ”skyddsvärda byggnader”, vilket tyvärr belysts åter igen, senast vid Marathon 2013 i Boston. Hotet mot och definitionen av en skyddsvärd byggnad är idag ett

svårbemästrat problem, framförallt då den aktuella byggnaden kanske är belägen i ett stort affärscentrum och hotet då är angeläget även för omkringliggande byggnader. Vid bombdådet i Oklahoma City 1995 var det ett flertal byggnader vars fönster påverkades. På upp till 1,6 km avstånd orsakade glassplitter skador till följd av explosionen. Så mycket som 85 % av alla skador i en urban miljö kan orsakas av glassplitter i olika former. Att utvärdera en risk kan vara ganska enkelt i sig, men att förutspå var hotet kommer att presentera sig är inte helt enkelt. Det är en grundförutsättning att veta vilka byggnader som är önskvärda att skydda och till vilken nivå, innan de faktiska konstruktionslösningarna ska installeras.

Vad gör forskningen?

Vid bland annat FOI har kompletterande och överlappande försök gjorts på olika kvaliteter av glas, främst fönsterglas. Dessa har sedan kopplats vidare till skaderisker och dödlighet. Vid institut i andra EU-länder har dessa försök främst kopplats till simuleringar, för att ge korrekta ingångsvärden och för att bekräfta institutens egna beräkningsmodeller. Vid FOI har praktiska försök gjorts. En rumsmodell i full skala byggdes enligt en brittisk modell för att utsättas för faktiska detonationer med inmonterade fönsterkonstruktioner. Rumsmodellen var indelad i 4 zoner; oskadad, minimal risk, låg risk och hög risk (risken här är risk för personskada). Hög risk är det när glassplitter flyger in i rummet och träffar väggen 3 meter in och en halv meter upp. För att detta ska kunna ske krävs endast en splitterhastighet på ca 9 m/s (ca 32 km/h). Vid dessa försök upptäcktes vidare att det inte alltid är själva glasrutan som är den svaga länken i en fönsterkonstruktion – infästning, låshakar och dekor kan också orsaka problem.

För att gå vidare med resultaten från de praktiska försöken med rumsmodellen har FOI till exempel studerat hur sjukvården definierar skador enligt en så kallad AIS-skala (Abbreviated Injury Scale) 1-6 där 1 är i princip oskadd och 6 innebär invaliditet eller avliden. Den viktigaste siffran som föll ut var att om det är 100 % sannolikhet att en fönsterkonstruktion går sönder ger det 1 % sannolikhet att någon avlider och 10 % blir svårt skadade av dem som befinner sig i rummet.

Vid institut i andra EU-länder har det också utförts forskning inom samma område. Dessa institut har dock intagit en mer heltäckande strategi och funderat mer på hur man kan göra en hel fasad mer flexibel för att kunna ta upp detonationslasterna. De har funderat över hur ett flexibelt upphängningssystem skulle klara lasterna och inkluderat detta i ett simuleringsprogram. Slutsatserna visar bland annat att deras idéer fortfarande skulle innebära stora skador på fasaden, men att konceptet avsevärt skulle minska mängden sekundära skador på omgivningen.

Under dessa arbetens gång har några institut i EU:s medlemsstater också fått möjlighet att jämföra resultat och slutsatser och även formulera synergieffekter

av respektive arbeten med gemensamma slutsatser. De mest uppenbara slutsatserna ger dock tyvärr inga enkla lösningar. Varje hotbild, byggnad och placering representerar sina egna unika förutsättningar. I många fall är det frågan om avväganden vad gäller hot-ekonomi-tid, vilket ger störst stöd till beslut. Eftersom glas är så känsligt för IED-hot och de resulterande skadorna omfattande, kan det vara rekommenderat att även lägga tid och ekonomi på så kallade perimeterskydd. Detta innebär till exempel att byggnaden står i vinkel mot förmodad attack för att sprida tryckvågen, eller att det finns hinder för att parkera en bil för nära byggnaden. På marknaden finns idag också tilläggsskydd att köpa så som ASF (Anti Shatter Film) vilken bör fästas in i karmen. Annars finns stor risk att hela rutan kommer flygande och orsakar större skada i form av blunt force trauma (trubbigt våld) istället. Ett annat tilläggsskydd är BBNC (Bomb Blast Net Curtain) vilken kan designas för att smälta in både funktionellt och estetiskt i den tänkta innemiljön.

Bild 1. Fönsterrutor med Anti Shatter Film (bild från försök i Tyskland). Fotograf: Annika Lööf.

Avslutning

Som tidigare nämnts är en del av terroristernas mål att skapa oreda genom att skapa kaos och samhällsekonomiska förluster. Dessa innefattar inte bara kostnader för infrastruktur utan även sekundära kostnader för sjukvård, sjukskrivningar, försäkringar och psykosociala aspekter. Genom ökad

medvetenhet och relativt enkla insatser kan riskanalys och förebyggande uppgraderingar, såsom hotbildsuppskattning, avståndshinder och skyddsgardiner, avsevärt minska det totala avtrycket av ett angrepp mot vårt samhälle, minska skaderiskerna och rädda liv.

Vidare läsning

- Lööf, A., FOI--2638--SE, Sammanställning och utvärdering av fönsterförsök i tunnel, 2008.
- Lööf, A., FOI Memo 1912**,** Skadeverkan av glassplitter fas 3. Bekämpning och skydd: Grindsjön. 2006.
- Lööf, A., van Doormaal, A., and Teich, M., Windows and glazing systems exposed to explosion loads: Part 1 – Lethality and Hazard Assessment, COST Action C26 "Urban Habitat Constructions under Catastrophic Events", International Conference Cost C26 – Urban habitat construction under catastrophic events, Naples, 2010.

21 Massmedia och masshysteri – hur reagerar medborgarna på information

Misse Wester

Källa: Wikimedia Commons, Patrick Furlong

Idag nås vi av information om en händelse bara sekunder efter det att den har inträffat. Detta konstanta flöde av information ställer ökande krav på hur myndigheter kommunicerar, framförallt när samhällsviktiga medelanden riskerar att hamna i skuggan av annan information. Det ställer också krav på att informationen är tillförlitlig och verifierad, och att myndigheten talar med en röst under en kris för att undvika förvirring bland allmänheten. Eller?

Viss forskning visar att det finns en rad föreställningar bland svenska myndigheter och massmedier om att befolkningen behöver lugnande information och att man ibland antar att människor kan bli oroliga om de nås av information om en potentiellt farlig situation. Annan forskning pekar på att människor är mycket aktiva i sitt informationssökande och använder sig av flera källor. Detta innebär, att medan myndigheterna och media ägnar tid åt att få sina uppgifter verifierade har medborgaren redan flyttat fokus till en annan informationskälla för att få den senaste informationen om en specifik händelse. Här blir de sociala medierna mer och mer centrala, där alla kan vara med att bidra till att nyheter skapas och rapporteras. I detta informationsflöde kan det vara svårt att veta exakt

vilken källa som har det största inflytandet på en enskild individs uppfattning om en viss situation. Snarare läggs en mosaik av den information som finns tillgänglig och skapar en sammansatt bild, där en enskild aktörs bidrag kan vara svår att spåra. Det här innebär att det krävs en ny syn på medborgaren som mottagare och producent av nyheter för att uppnå en effektiv kommunikation. Detta ställer krav på att myndigheter, länsstyrelser och kommuner ser över sina kommunikationsplaner och ifrågasätter de antaganden som ligger till grund för planernas utformning.

Myndigheters kommunikation

Att kommunicera relevant information till drabbade människor under en kris är en stor utmaning för en organsation. Att nå ut med sitt budskap även under normala förhållanden är svårt i sig, eftersom mängden information som når oss varje dag är enorm. Detta gör att kommunikation under svåra omständigheter, som i en kris, ställer ännu högre krav på effektiva kommunikationsstrategier. Givetvis är det inte bara *hur* man väljer att kommunicera som är viktigt utan också *vad* som kommuniceras. Att kommunicera under kris kan ha olika syften, vilket också speglar i vilken fas krisen är i. En enkel kronologisk uppdelning av en krishändelse kan göras med utgångspunkt från de tre faserna - före, under (den akuta fasen) och efter. Effektiv kriskommunikation bör fokusera på att det finns olika informationsbehov i de olika faserna. Det finns forskning som har visat att kriskommunikation bör inkludera information om: Vad som har hänt, Var det har hänt, När det hände, Hur det hände och Varför det har hänt.

I den fasen som föregår en kris, exempelvis vid en annalkande storm, bör informationen fokusera på vad som kommer att hända, konsekvenserna av detta och var den största påverkan kommer att vara. Givetvis måste också råd och rekommendationer kommuniceras, så att de som kommer att drabbas vet vilka de bästa handlingsalternativen är. Denna situationsanpassning måste även ske i den akuta fasen. I denna fas är det inte lika viktigt att berätta om vad som har hänt eller varför utan fokus i kriskommunikationen bör ligga på att ge konkreta råd om hur drabbade av krisen bör bete sig för att minska konsekvenserna. Ett exempel kan vara att myndigheter använder sig av TV för att nå ut med information till boende på en ort som har drabbats av ett utsläpp av en giftig gas. Det kan också handla om uppmaningar om att stanna inomhus under en storm.

Dock är kommunikation via traditionella mediekanaler, så som tv och radio, inte alltid möjliga eftersom situationen i ett krisområde kan vara så allvarlig att det inte går att nå ut till de drabbade. I sådana lägen kan personliga kontakter på plats och sociala medier på internet bli mycket viktiga. Ett bra exempel i detta sammanhang är den kommunikation som bedrevs i Östersunds kommun i samband med förekomsten av cryptosporidium (Crypto) i dricksvattnet 2010. Crypto är en bakterie som finns i de flesta dricksvattentäkter, men som i förhöjda

halter kan orsaka svår magsjuka. I Östersund upptäcktes förhöjda halter av Crypto i november 2010 i Storsjön, som förser 50 000 abonnenter med dricksvatten.

Eftersom antalet hushåll som skulle kunna drabbas av bakterien var så stort och för att förhindra ett storskaligt utbrott av magsjuka valde kommunen i ett tidigt skede att uppmana de boende att koka sitt dricksvatten. De kommunikationsvägar man använde var sociala medier på internet, så som Facebook, och kommunens hemsida. För att i så stor utsträckning som möjligt säkerställa att man nådde olika målgrupper valde man att även kommunicera via lokal press. Det något unika med denna situation var att kommunen redan innan smittan var bekräftad, både vad gäller typ av smitta och spridningsväg, valde att informera stort och brett. Den avvägning som gjordes var att det var bättre att varna i onödan än att vara för sent ute.

Även om Crypto-händelsen i Östersund 2010 är ett exempel på god kriskommunikation är det viktigt att vara medveten om, att även om de rekommendationer och uppmaningar syftar till att ge konkreta råd till hur drabbade ska agera, finns det ingen garanti att dessa råd följs. Att individer väljer att agera tvärtemot myndigheternas råd kan förefalla lite märkligt, men i krissituationer är det viktigt att förstå vilka motiv som kan ligga bakom beteende. Småbarnsföräldrar kanske åker till förskolan för att hämta sina barn mitt under ett pågående utsläpp av ett farligt ämne, för att detta känns tryggare. Det kan också vara så att ett beslut om att evakuera eller inte bygger på det förtroende individer har för myndigheterna och tidigare personliga erfarenheter av katastrofer eller kriser.

Medierna och myndigheterna

Samtidigt som viss information måste nå ut till drabbade, så finns det även ett stort informationsbehov hos de som inte är direkt drabbade. Det kan även finnas ett hårt tryck från olika regionala, nationella eller internationella massmedier på att få en samlad bild av vad som har hänt och omfattningen av krisen. I dessa situationer är det viktigt att ha en god förberedelse, så att det finns personal och rutiner för att hantera detta tryck. Dock är det viktigt att ha i åtanke att under den akuta fasen av en kris finns det inte en enskild aktör som har fullständig information om vad som sker/har hänt.

Ofta kan det vara så att representanter för massmedia söker upp en räddningsledare på plats för att få information om den aktuella händelsen, vilket ibland kallas för ”ledningscentralrapportering” (command-post reporting). Den här typen av journalistik leder till att den information som når ut i massmedia baseras på en viss källa, det vill säga den officiella räddningsledarens aktuella bild, vilket inte alltid speglar händelseutvecklingen i ett bredare perspektiv. När en kris eller katastrof har inträffat är det många aktörer som försöker reda ut

exakt vad som har hänt. Den information som då kommer fram är ofta fragmenterad och dåligt koordinerad. Det är först dagarna eller veckorna efter händelsen som en mer komplett bild av det som har inträffat kan skapas. Det är inte heller säkert att hela förloppet eller händelsens fullständiga omfång någonsin kommer att kunna sammanställas för att ge en exakt bild av det som skett. Det finns betydande skillnader mellan myndigheternas och massmediernas motiv till att kommunicera eller rapportera under en kris. Massmediernas roll är inte nödvändigtvis att ge råd och rekommendationer, utan fokuserar normalt på att ge en bild av förloppet.

Ofta är ansvariga myndigheter måna om att ge information som är verifierad. Därför finns det ibland en rädsla att släppa ifrån sig information som man inte vet är 100 % korrekt eller som motstrider tidigare fakta. Det kan visserligen finnas goda skäl att verifiera informationen, och självklart är det inte en god idé om det kommer motstridiga rekommendationer eller motsägande information ut i massmedia, men frågan är om det verkligen har en så stor effekt hos mottagaren som man kan tro.

Att gå ut med uppgifter som inte är säkra om till exempel antalet skadade kommer förmodligen inte att få förödande effekter för hanteringen av en kris. Däremot kan motsägelsefulla råd skapa viss osäkerhet – om en källa säger att drabbade ska stanna hemma, samtidigt som en annan källa uppmanar till utrymning kan det bli svårt för de drabbade att veta vilken källa de bör lyssna på. Detta behöver inte innebära att myndigheter ska vänta med att släppa ut viktig information för att den inte är helt verifierad, eller tysta ner eventuella meningsskiljaktigheter som kan finnas inom myndigheten när det gäller exempelvis information som omges av stor osäkerhet.

Medborgare söker information aktivt och förstår att information kan komma att ändras. Det kan också vara så att myndigheter där det funnits delade meningar som har tystats ner eller där man har valt att inte öppet redovisat all information man haft tillgång till, får problem med sin trovärdighet om detta framkommer efter det att krisen har ebbat ut. Att agera på ett sätt som uppfattas som oärligt i en situation kommer att försvåra möjligheterna till en effektiv kommunikation nästa gång något allvarligt sker.

”Allmänheten” – från nyhetskonsument till nyhetsproducent

Det finns studier som visar att individer idag hämtar information från en mängd olika källor och att traditionella nyhetsmedier, såsom tv, radio och tryckt media inte längre har monopol som nyhetsförmedlare. Om den information som ges ut från officiellt håll inte besvarar de frågor människor har, så söker man svar från annat håll. Detta visar att allmänheten inte är en passiv mottagare av information

utan söker aktivt information för att få en bild av vad som har hänt, varför det har inträffat och vad man kan göra både när det gäller att skydda sig men också hur man kan hjälpa till. Sammantaget visar forskning att människor hämtar in, betarbetar och agerar på information om en kris på andra sätt än det myndigheter utgår ifrån. Individer drabbas i de allra flesta fall inte av panik, blir oroliga eller agerar oöverlagt baserat på den information som når dem via massmedia.

Idag har de flesta människor tillgång till modern teknik som gör att information kan samlas och distribueras mellan en mängd olika media väldigt snabbt. Till exempel i samband med bombdåden i London 2005, fick brittiska BBC timmarna efter händelsen över 1 000 bilder, 20 videoklipp och 4 000 sms och 20 000 e-post från privatpersoner som på något sätt hade bevittnat det som hände. Detta visar att individer inte bara har en roll som konsumenter av media utan också fungerar som medproducenter av nyheter kring större händelser. Mediekanaler som Twitter, Facebook, Youtube och Instagram används för att snabbt sprida information om det som finns på plats. I samband med jordbävningen på Haiti 2010 var Twitter en av de främsta plattformarna för kommunikation som de drabbade och hjälporganisationer använde sig av. Ett annat exempel kan hämtas från explosionerna under Boston Maraton 2013 då polisen i Boston bland annat använde sig av Facebook för att samla in så mycket information om dådet som möjligt. På detta sätt kan de moderna kommunikationskanalerna användas för att samla in information om en händelse, och inte enbart för att kommunicera kring den.

Att följa traditionell nyhetsrapportering och de nyare sociala medierna kan bidra till en förstärkt omvärdsbevakning och kan på så sätt bistå i krishanteringen. Allmänhetens medproduktion av nyheter gör att myndigheter och organisationer, samt traditionella nyhetskanaler måste vara verksamma i sociala medier i mycket större utsträckning än idag. I samband med detta är det viktigt att vara medveten om att det finns en mängd aktörer på kommunikationsarenan och det kan vara svårt att nå ut med sitt meddelande till de grupper som anses vara i störst behov av information.

Med dagens teknik finns det enkla sätt att använda samma texter i olika forum. En och samma text kan läggas ut på en hemsida, skickas till en tidning, text-tv, spridas via Facebook eller Twitter. För att återvända till hur Östersunds kommun agerade under utbrottet av cryptosporidium i dricksvatten så arbetade informatörerna med att ta fram faktatexter som de la ut som dokument på sin hemsida. Dessa dokument kunde skrivas ut på exempelvis daghem, sjukhus eller på andra platser där information behövde vara tillgänglig.

Dock innebär det att när allmänheten rör sig mot att vara medproducenter snarare än enbart konsumenter av nyheter behövs en större etisk vaksamhet eller reflektion kring vad detta innebär för massmedierapporteringen vid kriser och katastrofer. De pressetiska reglerna, som de flesta traditionella nyhetsproducenter erkänner, går dessa regler inte på ett enkelt sätt att applicera på Facebook,

Twitter eller Instagram. Det material som skickas från privatpersoner till de större nyhetsförmedlarna granskas av ansvarig utgivare, även om trycket kan vara stort att vara ute först med spektakulära bilder eller flest detaljer. Denna granskning sker inte på samma sätt på de sociala medierna, där det är fritt att lägga upp bilder på drabbade utan att någon granskning sker. Hur detta bör hanteras är svårt att säga men utvecklingen tyder på att allmänhetens dubbla roll som konsument/producent får större betydelse i kommunikationen i kriser och katastrofer.

Vidare läsning

- Gustavsson, S. (2010) Sociala medier och kris. Mediateknik, Skolan för datavetenskap och kommunikation, Kungliga Tekniska högskolan.
- Lindberg, A., Lusua, J. och Nevhage, B. (2011) Cryptosporidium i Östersund vintern 2010/2011, konsekvenser och kostnader av ett stort vattenburet sjukdomsutbrott. FOI-R--3376--SE.
- Wester, M. (2011). Fight, flight or freeze: Assumed reactions of the public during a crisis. Journal of Contingencies and Crisis Management, 19(4), 207-214.

22 Innan krisen kommer - övningar som ett sätt att stärka krisberedskapen

Jenny Ingemarsdotter, Camilla Trané och Carolina Sandö

Scanpix: Nisse Schmidt

Utanför Malmö har ett oljefartyg krockat med ett lastfartyg. Stora snömängder orsakar störningar i järnvägstrafiken i norra Sverige. Ett elavbrott i Stockholm har pågått i två dygn. En kraftverksdamm i Dalarna brister.

Det finns tillfällen då vardagen rämnar. Då samhället ställs inför situationer som kräver skyndsamma och verkningsfulla åtgärder. Avgörande för hanteringen av en kris är att berörda aktörer klarar av sina uppgifter enskilt och tillsammans. Det är med andra ord nödvändigt att förbereda sig för kriser – innan de inträffar. Övningar utgör en grundläggande aktivitet för att förbereda sig, inom sin organisation såväl som tillsammans med andra.

Den här artikeln handlar om att inrikta och samordna övningar i ett samhälle där allt fler aktörer, privata såväl som offentliga, är sammanlänkade och beroende av varandra i händelse av en kris. Artikeln handlar också om vikten av att systematiskt ta tillvara och använda erfarenheter från övningar, för att nästa gång bli (ännu) bättre.

Behovet av att inrikta och samordna tvärsektoriella övningar

Lyckligtvis inträffar kriser sällan, men detta innebär också att aktörer som inte träffar varandra i vardagen kan behöva genomföra övningar tillsammans. I tvärsektoriella övningar medverkar sektormyndigheter inom två eller flera samhällssektorer/samverkansområden och myndigheter med geografiskt områdesansvar på olika nivåer – nationell, regional och lokal. Aktörerna övar sin förmåga att tillsammans hantera konsekvenserna av en händelse.

Flera tvärsektoriella övningar har genomförts under 2000-talet. Sverige deltar också i internationella övningar där samverkan över gränserna testas. För att övningar inte ska konstatera samma brister om och om igen behövs en systematik i hanteringen av utvärderingar, erfarenheter, åtgärder och övningsplanering. Utgångspunkten är kunskap om vad aktörerna har övat, vilket resultat det gav, och vad aktörerna behöver fortsätta öva.

I regeringens skrivelse *Samhällets krisberedskap – stärkt samverkan för ökad säkerhet* (2009) gjordes bedömningen att övningar i ökad utsträckning bör inriktas mot att öva identifierade brister och pröva förmågor inklusive samverkan: ”Mot bakgrund av erfarenheter från inträffade händelser, genomförda övningar och inlämnade förmågebedömningar bör det årligen tas fram en övergripande inriktning för tvärsektoriella övningar.” Detta utvecklingsarbete, som i sig kräver samverkan mellan många berörda aktörer, initierades av Myndigheten för Samhällsskydd och beredskap (MSB) under 2010.

FOI fick i början av 2012 uppdraget av MSB att identifiera och strukturera erfarenheter och förmågebrister som framkommit i dokumentationen av ett antal tvärsektoriella övningar och inträffade händelser. Målet var att utifrån underlaget identifiera och analysera mönster i erfarenheter, brister och relaterade frågeställningar.

Resultatet av ovan beskrivna uppdrag utgjorde underlag för den inriktning som angavs i februari 2013. Då fattade MSB, efter remissförfarande inom Nationellt forum för inriktning och samordning av övningar (NAFS), för första gången beslut om en övningsinriktning på nationell och regional nivå; *Övningsinriktning under 2014, 2015 och 2016 för tvärsektoriella övningar på nationell och på regional nivå.*

Hur inrikta tvärsektoriella övningar?

Det finns olika typer av underlag av betydelse för en gemensam övningsinriktning: genomförda övningar och inträffade händelser liksom MSB:s regelbundna analyser av samhällets krisberedskapsförmåga, baserade på bland

annat förmågebedömningar och risk- och sårbarhetsanalyser. Även omvärldsanalyser och analyser av beroendeförhållanden och trender, nationellt och internationellt, kan vara relevanta att beakta; nya typer av hot liksom nya skyddsvärden kan påverka vad aktörerna i framtiden behöver öva. Hur och vad som ska övas påverkas också av ramverk och förutsättningar för aktörerna. Det kan handla om resurser, organisation, lagar och regelverk, politiska beslut etc.

En grundläggande förutsättning för att ta fram en inriktning är att det finns gemensamma ”verktyg” för att beskriva den önskade riktningen. De begreppsmässiga verktyg som används vid inriktning av tvärsektoriella övningar är de generella förmågor som beskrivs i MSB:s nationella övningsplan.

Att inrikta innebär att göra en avvägning mellan generella och konkreta formuleringar. Å ena sidan riskerar allmänna formuleringar att inte peka ut någon riktning alls, medan en alltför detaljerad färdriktning kan ”låsa fast” och ge missriktade begränsningar i handlingsfrihet. En inriktning är alltså en form av prioritering både vad gäller riktning (vad är målet) och konkretionsnivå (vad ska inriktas). Vilken konkretionsnivå är då lämplig när förmågor ska anges i en övningsinriktning? Vad innebär formuleringen av förmågorna?

Ett sätt att närma sig frågan om innebörden av de generella förmågorna i MSB:s nationella övningsplan är att gå till erfarenheter av genomförda övningar. Övningsutvärderingar tar upp erfarenheter både på en mer detaljerad nivå och på en mer abstrakt nivå i förhållande till de generella förmågor som MSB formulerat i den nationella övningsplanen. Vid FOI:s analys av ett antal olika övningsutvärderingsrapporter noterades att vissa nyckelbegrepp som ansvar, ledning, kommunikation, informationshantering, samverkan och kunskap var återkommande. Analysen visade att det finns överlappande relationer mellan de nyckelbegrepp som identifierades och deras beroendeförhållanden. Om oklarheter finns gällande det egna ansvaret och ledningen blir det också svårt att samverka och förstå andras roller liksom sannolikt att kommunicera, hantera information osv.

För att kunna omsättas under övning behöver de generella förmågorna ofta konkretiseras. Även här kan ett tillvägagångssätt vara att använda sig av erfarenheter från genomförda övningar för att nå en mer konkret beskrivning av en generell förmåga.

För att genomföra en övning i praktiken behöver också en hypotetisk händelse, ett krisscenario, väljas. Krisscenariot rymmer problem att pröva sig mot. Det scenario som väljs påverkar också vilka aktörer som deltar och vilka typer av resurser som behöver finnas tillgängliga för övningen.

Att lära sig av erfarenheter från övningar

Den norska 22-julikommissionen konstaterade i sin rapport om händelserna i Oslo och Utöya att det har övats för lite och att man inte i tillräcklig grad har dragit lärdomar av erfarenheter från övningar (”Kommisjonen mener at det mange steder har vært øvet for lite, eller ikke vært tatt tilstrekkelig lærdom av erfaringer fra øvelser.”) Även på EU-nivå (Europeiska kommissionen) har det konstaterats att övning och utbildning visserligen utgör en central del av det så kallade civilskyddsamarbetet men att arbetet med erfarenhetsåterföring inte har kommit lika långt. Som FOI-rapporten *EU och krishantering – strategiska frågor för MSB* (2012) beskriver, har det ”hittills inte funnits någon struktur för att omhänderta erfarenheter”.

Att dra slutsatser från övningserfarenheter kan vara lättare sagt än gjort. Olika deltagande aktörer kan ha olika perspektiv och minnesbilder av vad som gjordes och ”hur det gick”, och det kan också finnas olika uppfattningar om huruvida övningen var ”realistisk”, det vill säga om den lyckades iscensätta reella utmaningar. Ändå är det viktigt att ta till vara erfarenheter från ofta resurskrävande och kostsamma samverkansövningar. Dessa erfarenheter kan bidra till att stärka samhällets krisberedskapsförmåga. Förutom att inrikta framtida övningar kan erfarenheter tjäna som underlag till åtgärder och spridning av kunskap.

En fungerande erfarenhetshantering bygger framför allt på att det finns ett behov av att omsätta eller ta del av erfarenheter men också på att hanteringen genomförs med systematik och med tillräckliga resurser, i synnerhet i analysfasen. Fördelen med ett mer systematiskt angreppssätt på organisationsnivå är större spårbarhet i utvecklingsarbetet och att sannolikheten ökar att kunskapen når dem som behöver den. Om erfarenhetshanteringens olika delsteg i övningssammanhang kan man läsa mer i FOI- rapporten *”Varför öva tillsammans? – mot en gemensam inriktning och samordning av tvärsektoriella övningar”*.

Övningstekniska utmaningar

Det faktum att övningar är iscensättningar av händelser kräver en särskild analys och framför allt ett hänsynstagande till övningstekniska utmaningar. Vilka slutsatser som kan dras efter en genomförd övning är beroende av såväl aktivt deltagande som övningsteknik. En övningsteknisk brist kan exempelvis vara avsaknad av den högsta beslutsfattande nivån i övningen. Likaså kan frånvaron av olika aktörer under en övning påverka resultatet negativt. Avsaknad av vissa moment, eller svårigheter att simulera tidsåtgång och resursförbrukning är andra exempel på övningstekniska utmaningar.

En övningsteknisk brist av mer teoretisk karaktär handlar om oklar begreppsanvändning. Om grundläggande begrepp, som till exempel ”förmåga”, ”samverkan” och ”lägesuppfattning”, används på olika sätt och till och med varierar från övning till övning, blir det svårare att göra jämförelser och dra slutssatser på en mer övergripande nivå. Det finns dock indikationer på att övningar som genomförts med liknande övning som förlaga har nått en högre mognadsgrad rent övningstekniskt, vilket kan tolkas som att kontinuitet, till exempel genom en övningsserie, kan ge ökad kvalitet.

Tendenser och framtida utveckling

Analyser av övningar och inträffade händelser ger en indikation på status av förmågor i krisberedskapssystemet. Denna status finns också analyserad i flera andra sammanhang, till exempel i de underlag som handlar om risk- och sårbarhetsanalyser, förmågebedömningar och beroendeförhållanden. Sammantaget kan dessa material sägas ge en nulägesbeskrivning av krisberedskapssystemet. I tillägg till denna nulägesanalys kan det också vara intressant att fundera över möjliga framtida förhållanden.

Kommer framtidens krishantering att kräva fler, eller nya, förmågor? Kommer vissa förmågor att förändras ”inifrån”, genom ny teknik eller förändrade resurser? Framtidsinriktade analyser, som till exempel trend- och omvärldsanalyser, pekar på flera övergripande och genomgripande tendenser, som till exempel effekter av klimatförändringar, den snabba teknikutvecklingen, demografiska förändringar, konsekvenser av en fortgående urbanisering, och nya hot och risker, som exempelvis antibiotikaresistenta bakterier, och mycket annat. Från ett övningsperspektiv handlar det här om att beakta tendenser som kan påverka nutida och framtida övningsbehov.

Övningar har i vissa fall redan idag visat på praktiska konsekvenser av förhållanden och tendenser som framtidsanalyserna identifierat. Innebörden av samverkan blir exempelvis alltmer komplex när drifts- och ägarstrukturer blir mer fragmenterade och diversifierade, också inom samhällsviktiga verksamheter. Den snabba teknikutvecklingen är ett annat område vars komplexitet övningar har belyst. En IT-incident kan visserligen drabba en viss kommun, men de inblandade aktörerna kan befinna sig i globala beroendekedjor som omfattar såväl statliga myndigheter som internationella tjänsteföretag med huvudkontor på en annan kontinent. I arbetet med att pröva och utveckla organisationer i en komplex värld spelar övningar en viktig roll – såväl nationellt som internationellt. EU satsar stora medel på att utveckla den gemensamma krisberedskapen och möjligheten att samverka över nationsgränserna. Både globalisering, teknikutveckling och privatisering av driftsformer och ägarförhållanden påverkar med andra ord samhällsviktig verksamhet.

Resultatet av övningar kan belysa vad som tycks fungera eller vad som inte alls verkar fungera. Vilka specifika slutsatser som kan dras är dock inte alltid självklart – för att ta till vara resultatet av övningar behövs också en systematisk erfarenhetshantering med konsekvent insamling och analys av övningserfarenheter. Erfarenhetsanalyser kan i sin tur ge anledning till olika förbättringsåtgärder, eller en ny inriktning för framtida övningar.

Vidare läsning

- Ingemarsdotter, J. och Trané, C. 2013. Varför öva tillsammans? – mot en gemensam inriktning och samordning av tvärsektoriella övningar. FOI-R--3679--SE.
- MSB. 2012. Nationell övningsplan: En strategi för tvärsektoriella övningar inom området samhällsskydd och beredskap. Dnr. 417-2012.

INTERVJU

23 Nordisk krisberedskap

Intervju med Carolina Sandö

***Carolina Sandö** är projektledare för ”Analys och utveckling av samhällets krisberedskap” och har under våren 2013 ingått i ett sekretariat för de nordiska krisberedskaps-frågorna. De nordiska länderna har ett roterande ordförandeskap vad gäller samarbetet kring krisberedskapsfrågor på ministernivå. Ministermötena förbereds av en nordisk ämbetsmannagrupp och dess sekretariat. Under våren 2013 har Sverige varit ordförande.*

Vad är nordiskt krisberedskapsarbete?

– Det nordiska samarbetet är ett av världens äldsta regionala samarbeten. Länderna samarbetar på flera områden, exempelvis inom hälso- och sjukvård, räddningstjänst och elförsörjning. Men samarbetet på en övergripande, politisk nivå vad gäller krisberedskapen formaliserades först 2009 då ansvariga ministrar samlades på Haga slott i Sverige för att anta "Haga-deklarationen". Då pekades ett antal områden ut som länderna skulle fördjupa sina samarbeten inom. Områdena var räddningstjänst, beredskap för händelser med kemiska, biologiska, radiologiska eller nukleära ämnen, kriskommunikation, frivilligmedverkan, övning, utbildning, forskning och utveckling. En uppdaterad deklaration och en strategisk utvecklingsplan har antagits i juni 2013.

Vad händer nu?

– Nu går man vidare genom att göra en utvärdering av de senaste årens arbete och analysera på vilka områden samarbetet bäst behövs. Det kan vara så att nya områden tillkommer. Prioritering ska göras på ministermötet i Norge nästa år. Den nya deklarationen har som övergripande vision ”ett robust Norden utan gränser” och det handlar då om att ta bort gränshinder som försvårar gemensamma insatser eller ömsesidigt stöd vid katastrofer. Det uttrycks också att man vill reducera sårbarheter och höja den gemensamma förmågan att hantera och återställa efter en kris. Det handlar även om att bli mer kostnadseffektiv genom att hitta gemensamma lösningar.

Utmaningar framöver för det nordiska krisberedskapsarbetet?

– Det nordiska samarbetet överlag har fått ökad uppmärksamhet de senaste åren. Många ser möjligheter och fördelar med att gå ihop i flera frågor och agera som en region, även exempelvis inom EU-samarbetet. Erfarenhetsutbyte och att lära av varandra har också fått ökat fokus, särskilt efter extrema händelser. De nordiska länderna har också antagit en solidaritetsförklaring och konsekvenserna av den är inte riktigt utredda ännu. Att vi ska bli bättre på att ge och ta emot hjälp från varandra är en del i detta.

Författare

Henrik Allberg är forskare och projektledare inom området människa-teknik-organisation. Han har en MSc. i teknisk fysik och elektroteknik och arbetar bland annat med utvärdering av staber samt hur information skall göras användbar i framtida trygghetssystem.

Maria Andersson är förste forskare inom området sensor- och telekrigssystem. Hon är också gästforskare vid avdelningen för reglerteknik vid Linköpings universitet. Hennes forskningsintressen är videoövervakning, maskininlärning, följning och anomalidetektion. Hon är (och har varit) engagerad i flera EU FP7-projekt inom olika säkerhetstillämpningar.

Rune Berglind är fil. dr i zoofysiologi och laborator i toxikologi och miljötoxikologi. Han leder EU-projektet CHEMSEA. En viktig del i nuvarande forskning är utveckling av ny miljötoxikologisk metodik för faroklassificering av komplext förorenad miljö. Rune var en av initiativtagarna till miljöforskning vid FOA i början av 1990-talet. Han har även arbetet med miljöutbildning och miljöinventeringar av förorenade områden i Estland, Lettland och Litauen. Rune är även knuten till Europeiska CBRNE-centret vid Umeå universitet.

Joel Brynielsson är tekn. dr i datalogi. Han forskar främst kring frågor som rör artificiell intelligens och IT-säkerhet. Joel är även adjungerad universitetslektor vid KTH, och har tidigare arbetat som universitets-lektor på FHS.

Christian Carling är forskningsledare och har arbetat med utveckling av ledning och samordning i civil och militär krishantering sedan 1995. De senaste åren har han främst ägnat sig åt flera stora projekt inom EU:s säkerhetsforskningsprogram, om havsövervakning, hamnskydd, CBRN-olyckor och säkerhetshot i stora kollektivtrafiksystem. Christians huvudsakliga forskningsintresse är metoder för experiment-baserad utveckling av säkerhetslösningar i komplexa system, med fokus på planering och värdering av försök.

Anneli Ehlerding är fil. dr i fysik, förste forskare samt projektledare inom området försvars- och säkerhetssystem. Anneli arbetar främst med frågor inom området *security of explosives* och leder nationella och internationella projekt inom säkerhet och beredskap. Hon bistår också med expertis inom explosivämnesdetektion inom olika EDA och NATO-grupper.

Anders Elfving är fil. dr i materiefysik och projektledare inom området försvars- och säkerhetssystem. Han arbetar med explosivämnesdetektion, främst med Raman- och masspektroskopi. Anders forskning är primärt inriktad mot förbättrad samhällssäkerhet inom bland annat internationell luftfart. Han har tidigare arbetat flera år med sensorutveckling inom halvledarindustrin.

Georg Fischer är forskningsledare med inriktning mot samhällets krisberedskap. Han har en bred erfarenhet av risk- och sårbarhetsanalyser inom olika samhällssektorer, studier av infrastrukturstörningar, metodutveckling för risk- och sårbarhetsanalyser, genomförande och utvärdering av krisövningar.

Ulrik Franke är tekn. dr i industriella informations- och styrsystem. Han är forskare och projektledare för det tvärvetenskapliga projektet Säkerhetspolitik i informationssamhället som studerar samspelet mellan samhälle och informationsteknik. Ulrik är också reservofficer med erfarenhet av såväl utlandstjänst som arbete i Högkvarteret.

Micael Granström är forskningsingenjör inom området CBRN. Han arbetar med detektion av radioaktiva ämnen, främst med inriktning på strålskyddsberedskap. Han är för närvarande involverad i ett projekt för mätning av radioaktivitet i människor. Micael är medlem av Nationell expertgrupp för sanering (NESA) som administreras av Strålsäkerhetsmyndigheten.

Tommy Gustafsson är högskoleingenjör i informationsteknik och forskare. Han är andra generationens nätverksingenjör och har jobbat med datornät och informationssäkerhet inom privat och offentlig sektor i mer än tio år. Vid FOI forskar han med inriktning på säkerhet i kommunikationsnätverk, SCADA och ICS samt objektbaserad säkerhet.

Ann Göransson Nyberg är docent i medicinsk fysiologi vid Uppsala Universitet samt laborator och projektledare inom området CBRN. Hon har bland annat deltagit i framtagande av försvarets autoinjektor och forskat kring hälsorisker vid internationella operationer. Ann har publicerat flitigt inom katastrofmedicin och gett stöd till sjukvård vid omhändertagande inom området katastroftoxikologi. Hon har även tjänstgjort som biträdande koordinator för EU-projektet MASH på European CBRNE center vid Umeå Universitet.

Jonas Hallberg är tekn. dr i datorsystem och laborator. Jonas forskar inom informationssäkerhet och är speciellt intresserad av frågor som rör värdering av informationssäkerhet och analys av informationssäkerhetsrisker. Forskningen berör såväl sociala som tekniska aspekter. Utöver forskning arbetar Jonas med strategisk inriktning och ledning av forskning inom området.

Fredrik Johansson är tekn. dr i datavetenskap och forskare inom området informations- och aerosystem. Fredrik arbetar bland annat med att utveckla tekniker och metoder för analys av stora mängder data inhämtade från internet och sociala medier. Fredriks forskningsintressen innefattar textanalys, maskininlärning och analys av sociala nätverk.

Jenny Ingemarsdotter är fil. dr i idé- och lärdomshistoria och civilingenjör i teknisk fysik. Jenny arbetar med frågor om samhällets säkerhet och krisberedskap. Hennes intresseområden innefattar strategisk analys av samhällets krisberedskap, kritiska flöden, globala trender, scenarioutveckling och metoder för strukturerad problemformulering.

Sören Jägerhök leder FOI:s arbete inom det EU-finansierade hamnsäkerhetsprojektet SUPPORT. Han arbetar inom området sensor- och telekrigssystem och har olika ledande roller i EU-projekt med tillämpningarna: detektion av onormalt beteende, hamnsäkerhet och containersäkerhet. Han medverkar i arbetsgruppen för Logistiksäkerhet inom European Organisation for Security (EOS).

Lisa Kaati är fil. dr i datavetenskap och forskare inom området bestlutsstödsystem. Lisa har arbetat med frågor som rör teknik för underrättelsearbete och beslutstöd sedan 2008. Hennes intresseområden är bland annat tekniker för analys av data från webben. Lisa har också en deltidstjänst på Uppsala universitet på institutionen för Informationsteknologi.

Patrik Krumlinde är fil. dr i organisk kemi och forskare inom området energetiska material och modellering. Patrik jobbar främst inom sprängämnessäkerhet med fokus på sprängämnesprekursorer och hemmagjorda bomber inom både nationella och EU-projekt.

Malin Kölhed är fil. dr i analytisk kemi och förste forskare inom området försvars- och säkerhetssystem. Malin driver forskningsprojekt inom områden som rör kemiska signaturer från hemmagjorda bomber och är även koordinator för EU-projektet PREVAIL.

Björn Larsson är forskningsledare och arbetar med radarsystemfrågor. Han kom till dåvarande FOA redan 1980 från Linköpings Universitet. Han har under åren arbetat med många projekt allt från isbergsspaning i arktiska farvatten till utveckling av syntetisk aperturradar (SAR) på låga frekvenser. Uppgifterna har inneburit arbete i många spännande miljöer från tropisk regnskog, öknar till arktiska isvidder och uppgifterna har inneburit systemdesign, fältförsök och projektledning. Han var chef för FOI:s institution för Radarsystem 2001 – 2009. På senare år har han även verkat som projektledare för olika EU-projekt.

Per Larsson är fil. dr i statsvetenskap och analytiker inom området samhällets krisberedskap. Han har under lång tid arbetat med krisberedskapsfrågor på lokal-, regional-, nationell- och EU-nivå, framförallt med Försvarsdepartementet som uppdragsgivare. Per arbetar för närvarande även med nationell risk- och förmågebedömning.

Per Leffler är laborator inom området toxikologi, inkluderande människa och miljö. Per har en doktorsexamen i yrkes- och miljömedicin med inriktning på metallers toxikologi och är bland annat medförfattare till skriften *Handbook on the toxikologi of metals*. Under åren 1995-1996 var han Europa-kommissionsstipendiat vid EU:s Miljöinstitut i Italien, och fick Civilingenjörsförbundets Miljöpris 1997 för ett forskningsprogram om effekter av blandningar av miljögifter i miljön.

David Lindahl är fil. mag. i datavetenskap och forskare. Han arbetar med forskning kring IT-säkerhet och datorkrigföring. Han har undervisat både militära förband, myndigheter och företag om risker och möjligheter med datorsystem. David har också deltagit i uppbyggnaden av labbet NCS3, den nationella satsningen på säkerhet i datorstyrd kritisk infrastruktur. Han är i det projektet ansvarig för kurs- och demonstrationsverksamhet för företag inom bland annat elförsörjning, dricksvattenproduktion och transporter.

Annika Lööf är bergsingenjör från KTH och forskare inom området försvars- och säkerhetssystem. Hon arbetar främst med materialfrågor med fokus på egenskaper och struktur både kopplat till snabba deformationsförlopp och skyddsegenskaper. Annika arbetar även inom civila områden där skador på byggnader, så som perrong till Citybanan, är ett exempel. Hon har tidigare jobbat på Höganäs AB i bland annat Japan.

Malin Mobjörk är fil. dr i Tema Vatten i natur och samhälle och forskningsledare. Hennes forskningsområden omfattar samhällsvetenskaplig klimat- och miljöforskning, vetenskapsstudier, tvärvetenskap och strategisk analys. På FOI har hon exempelvis analyserat vilka samband som finns mellan klimatförändringar och säkerhet, vilka utmaningar klimatförändringar ställer på samhällets krisberedskap och hur samhället kan möta dessa utmaningar.

Björn Nevhage är civilingenjör i riskhantering och analytiker med inriktning på risk- och sårbarhetsanalys och samhällets säkerhet. Hans huvudsakliga uppgifter är utveckling och implementering av metoder och verktyg för risk- och sårbarhetanalys. Björn stödjer också MSB i deras arbete med nationell risk- och förmågebedömning, som är ett relativt nytt utvecklingsarbete och som initierats av Europeiska kommissionen. Stödet omfattar både metodutveckling och genomförandet av riskbedömningen.

Anna Pettersson är förste forskare inom området försvars- och säkerhetssystem. Hon är bland annat projektledare för FOI:s deltagande i flera EU-finansierade säkerhetsforskningsprojekt. Annas främsta verksamhetsområde är *Security of explosives* som bland annat omfattar detektion av explosivämnen. Anna deltar i flera expertgrupper på EU-nivå där hon bidrar med sin expertis inom explosivämnesdetektion.

Lotta Ryghammar är analytiker med inriktning mot svensk krisberedskap. Hon arbetar sedan många år åt exempelvis Försvarsdepartementet med bland annat frågor kring styrning och uppföljning av samhällets krisberedskap.

Carolina Sandö är programansvarig för "Analys och utveckling av samhällets krisberedskap" och leder ett projekt som genomför studier om krisberedskap från lokal till internationell nivå. Sedan 2002 har hon arbetat med forskning för regeringens behov, men även på uppdrag av olika myndigheter. Periodvis har hon utgjort analysstöd på Försvarsdepartementet. Hennes studieområden innefattar krisberedskap inom EU, humanitärt arbete utanför unionen, nordiskt krisberedskaps-arbete och inriktning av nationell krisberedskap.

Steven Savage är fil. dr i tillämpad fysik och forskningschef. Han är projektledare för olika teknikprojekt och studerar bland annat hur modern säkerhets- och övervakningsteknik kan påverka och kränka medborgarens integritet och privatliv. Steven är även adjungerad professor på KTH.

Pontus Svenson är tekn. dr i teoretisk fysik och forskningsledare. Pontus har arbetat med frågor som rör informationsfusion, lägesinformation och teknikstöd för underrättelsearbete sedan 2001 och med frågor om logistiksäkerhet sedan 2010. Forskningsintressen är bland annat analys av sociala nätverk, statistiska metoder för analys av stora datamängder och bayesiansk analys.

Camilla Trané är tekn. lic. i reglerteknik och analytiker. Camillas arbetsområden spänner från utvecklingsplaner till systemanalys och rymmer erfarenheter från uppdrag hos Försvarsmakten samt olika civila myndigheter.

Ester Veibäck är civilingenjör i system i teknik och samhälle. Hon arbetar i första hand som analytiker inom områdena samhällets säkerhet och krisberedskap. Ester är projektledare för Nationell risk- och förmågebedömning och arbetar med metodutveckling inom området. Ester har också erfarenhet av frågor som rör trygg energiförsörjning.

Niclas Wadströmer är tekn. dr. i bildkodning och förste forskare. Niclas arbetar bland annat med bildanalys för övervakningstillämpningar och algoritmer för analys av multi- och hyperspektrala bilder. Han är även intresserad av etiska frågeställningar kring övervakningssystem.

Misse Wester är fil. dr i psykologi och docent i beteendevetenskaplig riskforskning. Hennes forskning fokuserar framför allt på individens roll i risk- eller krissammanhang. Misses forskningsintresse spänner över uppfattningar om risker till faktiskt beteende i större kriser.

Elisabeth Wigenstam har en PhD i ämnet lungmedicin och är forskare inom området CBRN. Hon arbetar bland annat med att ta reda på hur industrikemikalier påverkar andningsorganen och hur man bäst behandlar skadorna efter en exponering.

Hans Önnerud är tekn. dr inom pappers- och massateknik med en grund som analytisk kemist. Han är forskningsledare inom området försvars- och säkerhetssystem och leder två säkerhetsklassade EU-forskningsprojekt med FOI som koordinator. Det ena syftar till att utveckla nya system för att hitta olagliga bombfabriker och det andra har som mål att utveckla nya verktyg för forensiska analyser av ett bombattentat.

24 Så kan FOI stödja Dig och din organisation

FOI är ett av Europas ledande forskningsinstitut för tillämpad forskning. FOI är en statlig myndighet som huvudsakligen är uppdragsfinansierad. Den här skriften illustrerar FOI:s breda kompetens inom området samhällets säkerhet och trygghet. Med denna breda kompetens kan FOI även stödja dig och din organisation när det gäller frågor om säkerhet och trygghet. Exempel på uppdragsfinansierat stöd som FOI ger är:

Vi stöttar löpande verksamheter med olika typer av **expertstöd**: till exempel kravspecificering vid anskaffning och upphandling, stöttning vid myndigheters tillsynsarbete, stöd till rättsvårdande myndigheters brottsbekämpning, operativt stöd vid en inträffad olycka/kris, samt stöd vid koordinering och handläggning av forskning och användarmedverkan i forskningsprojekt.

För att förbättra långsiktiga beslut stöttar FOI arbetet **vid framtagande av strategiska beslutsunderlag**, till exempel genom sammanställningar av befintlig kunskap och -teknik, utveckling av ny kunskap och nya tekniker samt metodstöd inför och under beslutsfattande.

För att **utveckla krishanteringsförmågan** ger FOI kurser, övningar och har kunskapscentrum där kunskaper inom ett specifikt område upprätthålls.

Naturligtvis bedriver vi även forskningsprojekt och utvecklar forskningsmiljöer med främsta uppgiften att ta fram ny kunskap. FOI har även **laboratorium** till uthyrning.

Du som är intresserad av att veta mer om hur FOI kan ge stöd till din organisation – tveka inte att höra av dig till oss:

Lisa Hörnsten Friberg

Du når oss via
E-post: market@foi.se
Telefon: 08-555 030 00
www.foi.se

Eller skriv in din fråga på adressen
www.foi.se/sv/nyheter/Kontakta-oss/Marknad-och-forsaljning/

FOI är ett av Europas ledande forskningsinstitut inom områdena försvar och säkerhet. Myndigheten är uppdragsfinansierad och lyder under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling samt analyser.

FOI publicerar för första gången *fokus Samhällssäkerhet*. Det är en skrift som belyser hur FOI utvecklar samhällssäkerheten genom långsiktig kunskapsuppbyggnad och genom att direkt stödja olika samhällsaktörer i deras arbete med säkerhets- och trygghetsfrågor.

Redaktörer har varit Georg Fischer, Per Larsson,
Lotta Ryghammar och Carolina Sandö (projektledare).

fokus Samhällssäkerhet finns att ladda ner från www.foi.se.

FOI

ISSN1650-1942

www.foi.se