Myndigheten för samhällsskydd och beredskap

Risk- och sårbarhets-analyser för ett säkrare och mer resilient samhälle

En populärvetenskaplig sammanfattning

FORSKNING

MSB:s kontaktpersoner:
Ulrika Postgård, 010-240 50 33

Publikationsnummer MSB1080 - februari 2017

Förord

LUCRAM (Lunds universitets centrum för riskanalys och riskhantering) har under perioden juli 2011 till december 2015 genomfört ett ramforsknings-program, PRIVAD (Program for RIsk and Vulnerability Analsysis Development) finansierat av MSB (Myndigheten för Samhällsskydd och Beredskap). Syftet med ramforskningsprogrammet var att utveckla metoder för risk- och sårbarhetsanalys på alla nivåer av samhället, dvs. lokal (kommuner), regional (länsstyrelser, landsting) och nationell nivå (MSB, regeringskansliet, andra centrala myndigheter). Avsikten är att bättre kunna förutse, förebygga och hantera alla typer av risker och hot i samhället. I längden är tanken att forskningen ska bidra till utvecklingen av ett mer resilient samhälle. Detta är en populärvetenskaplig sammanfattning av ramforskningsprogrammet. Mer information, vetenskapliga publikationer, etc. finns på:

http://www.lucram.lu.se/research/privad.

Innehållsförteckning

Sammanfattning

I takt med att samhället blir mer komplext och sammankopplat ökar även behovet att arbete systematisk och proaktivt med risk- och sårbarhetsanalyser. Det ställs nya krav på de metoder som används för detta arbete där många av de metoder som traditionellt sett använts inte längre är så lämpliga. Ramforskningsprogrammet PRIVAD har arbetat med att utveckla metoder för risk- och sårbarhetsanalys med ett antal olika inriktningar. Speciellt har arbetet riktats in på fyra olika områden: 1) Samlade riskbilder, 2) Föremågebedömningar, 3) Kritiska samhällsfunktioner och 4) IT-system.

Det första området handlar om hur riskinformation kan och bör aggregeras för att skapa en samlad riskbild på olika nivåer av samhället. För att t.ex. åstadkomma detta är det fördelaktigt om aktörer använder samma metoder och/eller samma bedömningsskalor för t.ex. beskrivning av sannolikhet och konsekvens. Samtidigt är det viktigt att vara medveten om att det även finns andra syften med att genomföra risk- och sårbarhetsanalys som kan påverkas negativt av en ökad grad av standardisering.

Det andra området handlar om hur föremågebedömningar kan utvecklas så att de ger bättre beslutsunderlag. Genom experiment har det visat sig att erfarna personer upplever att förmågebedömningar som baseras på tillgängliga resurser är mest användbara. För mindre erfarna personer, å andra sidan, är det viktigt att det även framgår vilka uppgifter en aktör kan lösa med dessa resurser. Med andra ord beror lämpligheten i en förmågebedömning delvis på vem mottagaren är.

Det tredje området handlar om hur samhällskonsekvenser och återhämtningsförmåga i kritiska samhällsfunktioner kan analyseras. Kritiska samhällsfunktioner utgör sådant som alltid måste fungera för att samhället ska fungera, såsom fungerande elförsörjning, hälsa och sjukvård samt transporter. I projektet har bl.a. en simuleringsmodell utvecklas där återställningstiden kan uppskattas som en funktion av tillgängliga resurser och omfattningen av ett avbrott.

Det fjärde området handlar om hur metoder för risk- och sårbarhet av IT-system kan förbättras. IT-system har de senaste decennierna kraftigt förändrat förutsättningarna för hur vi administrerar och driver våra verksamheter. Men eftersom IT-system har en annan karaktär jämfört med många andra system krävs nya arbetssätt. I projektet har bl.a. en riskanalys som utgår från olika perspektiv (designerns, testarnas, användarnas, etc.) utvecklats i syfte att förbättra identifieringen av risker i IT-system.

1. Fyra forskningsteman

Samhället blir alltmer komplext och sammankopplat och olika sorters samhällsförändringar sker i allt snabbare takt. Risker och kriser kan idag snabbt spridas både över stora geografiska områden och mellan många olika samhällssektorer. Eftersom konsekvenserna av sådana händelser kan bli väldigt allvarliga kan vi inte vänta tills de inträffar för att lära oss av dem och sedan bygga bättre system. Vi måste även försöka befinna oss steget före och analysera vilka potentiella händelser och risker som kan ge upphov till allvarliga skador på liv och hälsa, samhällets funktionalitet och andra värden som vi människor bryr oss om.

Risk- och sårbarhetsanalyser är ett viktigt verktyg för att skapa en nödvändig framåtblick och möjlighet att förebygga eller förbereda sig inför kriser. Forskningen inom PRIVAD har inriktats mot en rad olika teman som alla på ett eller annat sätt har med risk- och sårbarhetsanalys att göra. I denna populärvetenskapliga sammanfattning kommer fyra av dessa teman att beröras:

1. *Samlade riskbilder* – hur kan och bör riskinformation aggregeras för att skapa en samlad riskbild på lokal, regional eller nationell nivå?
2. *Föremågebedömningar* – hur kan föremågebedömningar som ger bättre beslutsunderlag utvecklas?
3. *Kritiska samhällsfunktioner* – hur kan återhämtningsförmåga och samhällskonsekvenser analyseras?
4. *IT-system* – hur kan metoder för risk- och sårbarhet för IT-system förbättras?

”Risker och kriser kan idag snabbt spridas både över stora geografiska områden och mellan många olika samhällssektorer”

2. Samlade riskbilder

Ett av målen med de risk- och sårbarhetsanalyser som görs av kommuner och myndigheter är att ta fram en samlad riskbild på lokal, regional eller nationell nivå. Myndigheten för samhällsskydd och beredskap (MSB), som har ansvaret för den nationella analysen, använder sig av RSA:er från andra centrala myndigheter samt de regionala analyserna. Dessa förlitar sig i sin tur på kommuners analyser i sitt arbete. Att skapa sådana samlade riskbilder är inte en enkel uppgift och den görs än svårare av att det är upp till varje kommun eller myndighet hur de väljer att genomföra sin risk- och sårbarhetsanalys och presentera sin riskbild.

Inom PRIVAD har frågan om hur aggregering av dessa risk- och sårbarhetsanalyser går till idag undersökts genom att studera hundratals dokument och genom intervjuer med personer som arbetar med analyserna. Det visade sig finnas stora variationer i hur risker presenteras och att de senaste ändringarna i MSB:s föreskrifter har haft ganska stor genomslagskraft. Problemet med variationer i beskrivning av riskbilden är att det blir svårt att jämföra analyser med varandra. Om en kommun väljer att beskriva sin risk för exempelvis översvämningar som ”hög” och en annan som ”en gång vart 50:e år”, blir det problematiskt att beskriva översvämningsrisken för området i sin helhet. Ofta saknas det också en motivering till varför en risk placeras i en viss kategori, något som är värdefull information för en utomstående som vill förstå hur författaren av rapporten har resonerat. När studenter från riskrelaterade studier på LTH och Mittuniversitetet samt utexaminerade risk- och brandingenjörer fick bedöma olika sätt att presentera risker visade det sig att de var ganska överens oavsett bakgrund. Åsikten var att en så kallad kvantitativ beskrivning, dvs. en beskrivning som använder siffror (t.ex. 1 gång på 10 år), ansågs vara mer användbar än en kvalitativ beskrivning, dvs. en beskrivning som endast använder ord (t.ex. ”låg risk”).

”Ett problem som kan uppstå är att aktörer är ovilliga att dela med sig av information på grund av sekretess eller upplevd sekretess”

Exempelbild workshop. Foto Gunnar Menander.

En grundläggande utmaning för att aggregera riskinformation är att veta var det går att hitta den information som behövs. För att veta detta är det viktigt att man inom den egna verksamheten har insikt i vilka aktörer man är beroende av, även inom den egna verksamheten, samt hur samhällsviktiga funktioner hänger ihop. Denna helhetsbild är något som till stor del saknas inom arbetet med risk- och sårbarhetsanalyser idag.

När man väl vet vilka aktörer som är viktiga för sin verksamhet behövs effektiva kanaler för informationsutbyte. En av svårigheterna med detta är att många av aktörerna är privata företag som ofta saknar bra incitament för att dela med sig av informationen. Det finns ingen lagstiftning som ”tvingar” dem att samarbeta, så allt beror på deras välvilja, tid och intresse. Tiden är den faktor som oftast benämns som den begränsande faktorn, eftersom tid dels kostar, dels finns i en begränsad mängd. Ett problem som kan uppstå är att aktörer är ovilliga att dela med sig av information på grund av sekretess eller upplevd sekretess. Många handläggare är också osäkra på hur de ska hantera sekretessbelagt material och föredrar därför att inte ens ta del av det.

För att få bästa möjliga förutsättningar för att kunna skapa samlade riskbilder borde samtliga aktörer använda samma metod för att analysera risker. Det kan dock vara problematiskt eftersom olika metoder passar olika bra beroende på vad som ska analyseras. Exempelvis är en metod för att analysera elproduktion troligtvis inte lika lämpad att hantera miljörisker. Risk- och sårbarhets-analyserna har också andra syften än att ge underlag till en samlad riskbild. För att underlätta aggregering föreslås dock att myndigheter bör enas om att använda sig av gemensamma skalor för presentation av viktiga begrepp såsom sannolikhet och konsekvenser.

3. Förmågebedömningar

Om någon gav dig en handbrandsläckare och frågade: ”Vad är din förmåga att släcka en brand?”, vad hade du svarat? Det är inte en helt enkel fråga och svaret kommer exempelvis bero på vilken storlek på branden du föreställer dig och din erfarenhet av att använda handbrandsläckare. Dessutom kommer svaret att innehålla en viss osäkerhet. Myndigheter som inom ramen för risk- och sårbarhetsanalyser ska bedöma sin förmåga att hantera kriser står inför liknande problem, fast kanske ännu svårare eftersom det handlar om betydligt mer komplicerade situationer.

Många av dagens metoder för förmågebedömning bygger på olika former av indikatorer, det vill säga listor som anger variabler som anses viktiga för utfallet av en kris. Ofta handlar det om vilka resurser som finns att tillgå vid en eventuell kris. I en del metoder är indikatorerna vidareutvecklade till ett index. Då tilldelas varje variabel en siffra och med hjälp av en ekvation beräknas ett slutgiltigt förmågeindex. Sådana metoder är relativt enkla att använda och gör det lätt att jämföra från år till år hur förmågan har utvecklats eftersom det är enkelt att jämföra hur indexet förändras.

När en kris inträffar behöver nästan alltid flera aktörer samarbeta. Även vid en vardaglig händelse som en bilolycka samarbetar SOS Alarm, räddningstjänst, polis och ambulans för att hantera händelsen. Vid större händelser behövs ofta samarbete mellan fler aktörer och då måste flera aktörers sammanvägda förmåga bedömas, och detta kan vara svårt att göra med indikator- och indexmetoder.

För att utveckla metoder för förmågebedömning som bättre tar hänsyn till exempelvis beroenden mellan aktörer är det första viktiga steget att definiera vad man menar med ”förmåga”. Speciellt är det viktigt att definiera begreppet i ett krishanteringssammanhang och koppla det till andra centrala begrepp såsom risk och sårbarhet. Vanliga definitioner av förmåga idag likställer förmåga med resurser och saknar koppling till exempelvis risk, scenario, sannolikhet och konsekvens. Inom PRIVAD föreslås istället en definition som utgår från att en aktör genomför en uppgift med ett visst syfte under en kris. Förmågan speglar effekten av att genomföra uppgiften, det vill säga om förmågan är hög så blir konsekvenserna låga, och tvärtom. Vilka resurser som finns tillgängliga är en viktig aspekt i detta, men inte den enda som utgör förmågan.

För att undersöka vad personer inom det svenska krishanteringssystemet tycker om den här formen av beskrivning av förmåga, genomfördes en studie där beslutsfattare från räddningstjänsten fick se en av fyra versioner av en förmågebedömning om skogsbränder. De fick sedan svara på frågor om hur användbar de tyckte att bedömningen var som underlag för beslut kring förmågehöjande åtgärder. Versionerna skiljde sig åt genom att (1) enbart innehålla beskrivningar av tillgängliga resurser, (2) enbart innehålla beskrivningar av de uppgifter som kan genomföras och med vilken effekt, (3)

innehålla beskrivningar av *både* resurser och uppgifter, eller (4) varken innehålla beskrivningar av resurser eller uppgifter, utan bara slutsatsen att ”förmågan är god men med vissa brister”. Resultatet visade att erfarna personer föredrog att endast få en lista med tillgängliga resurser, medan de som var relativt oerfarna föredrog versionen med beskrivning av både resurser och uppgifter. Anledningen är antagligen att erfarna personer själva kan avgöra vad som kan utföras med en viss uppsättning resurser och om dessa är tillräckliga, något som är mer problematiskt för en oerfaren person.

Denna slutsats är viktig att ta i beaktande om man vill bedöma den samlade förmågan hos flera aktörer, eftersom aktörerna inte är experter på varandras områden och därför kan behöva mer information än en resurslista för att förstå varandras förmågor.

”Resultatet visade att erfarna personer föredrog att endast få en lista med tillgängliga resurser, medan de som var relativt oerfarna föredrog versionen med beskrivning av både resurser och uppgifter”

4. Kritiska samhällsfunktioner

För att skapa ett mer resilient samhälle är det viktigt att se till att kritiska samhällsfunktioner, såsom el- och vattendistribution, transporter, hälsa och sjukvård, etc. är robusta och klarar av att hantera och återhämta sig från såväl små som stora störningar. Att uppnå detta är komplicerat med tanke på den stora mängd både offentliga och privata aktörer samt den uppsjö lagar och regleringar som utgör och påverkar samhällsfunktionerna. Komplikationsgraden ökar då kritiska samhällsfunktioner även blir allt mer sammankopplade med varandra, t.ex. är elsystem beroende av elektronisk kommunikation för att fungera. PRIVAD har bland annat undersökt vilka konsekvenser störningar i kritiska samhällsfunktioner kan ge för samhället samt utvecklat modeller och metoder för att analysera hur lång tid det tar att återställa systemen. Fokus har varit på tekniska system, framförallt eldistributionssystemet, troligen den mest kritiska samhällsfunktionen i ett modernt samhälle.

(MdE, 2004)

Hur snabbt återhämtar sig elsystem efter en störning? I Sverige är det ett lagkrav (funktionskravet i Ellagen) att elavbrott inte får vara längre än 24 timmar (med vissa inskränkningar). Men hur snabbt t.ex. ett eldistributionssystem kan återställas beror på flera parametrar, framför allt på påfrestningsgraden, vilka resurser som finns tillgängliga och hur snabbt dessa kan mobiliseras. Vid större störningar lånar aktörer resurser från andra aktörer inom samma område genom så kallade samverkansgrupper. Hur ovan nämnda parametrar och betingelser påverkar förmågan för elnätsbolag att återhämta sig från störningar var en av de centrala frågeställningarna.

I en studie på en kommun i Sverige med cirka 100 000 invånare har detta undersökts. Metoden kräver både en modell av själva den tekniska infrastrukturen, här ett eldistributionssystem, och en modell av återställningssystemet, dvs. resurser och manskap och hur nyttjandet av dessa prioriteras för att återställa systemet. Med modellerna kunde sedan systemets förmåga analyseras genom datorsimuleringar. Bland annat framgick det av resultaten hur återställningstiden påverkas av påfrestningsgrad på elnätet och tillgängliga resurser. Det simuleringsbaserade angreppssättet medför att många olika kombinationer av påfrestningar och resurser kan analyseras (miljontals olika scenarion). Genom att analysera resultaten kan olika slutsatser dras, t.ex. för vilken grad av påfrestningar som man uppfyller 24h kravet och vilka resurser eller sårbarheter i elnätet som är kritiska. En

övergripande slutsats för det studerade elnätsbolaget var att vid normala störningar (vardagsstörningar) kunde elförsörjningen snabbt återställas medan för omfattande störningar eller bortfall av särskilt kritiska anläggningsdelar kunde inte elleveransen återställas inom 24h. En liknande studie med samma angreppssätt för IT-system har även genomförts för att utreda dess applicerbarhet på tekniska infrastrukturer generellt, med lovande resultat.

I en annan studie var fokus på att jämföra olika mått för att beskriva de samhälleliga konsekvenserna som uppstår vid elavbrott. Två mått användes: avbrottsersättning som elbolagen måste betala ut vid avbrott (elnätbolagets ekonomiska konsekvenser) samt vilka samhällsviktiga verksamheter som påverkas utifrån Styrel (samhällskonsekvenser). I Sverige måste elbolag betala ut ersättning till kunder som har varit utan el i minst 12 timmar och ersättningen ökar ju längre avbrottet varar. Det finns även ett system i Sverige, Styrel, som bestämmer vilka kunder som har högst prioritet utifrån samhällets perspektiv om det råder brist på el av någon anledning. Simuleringar för tidigare nämnda eldistributionssystem genomfördes och det visade sig att de avbrottsscenarier som gav upphov till stora samhällskonsekvenser (dvs. drabbade de prioriterade verksamheterna enligt Styrel) även var kostsamma för elnätsbolaget (dvs. i form av avbrottsersättning att betala ut). Dock fanns det även scenarier där viktiga samhällsfunktioner drabbades men som inte ledde till höga avbrottsersättningar för elnätsbolaget, vilket leder till slutsatsen att avbrottsersättningen till viss del styr rätt, dvs. ger incitament för robust elförsörjning till samhällsviktiga funktioner, medan det i vissa fall krävs andra incitament.

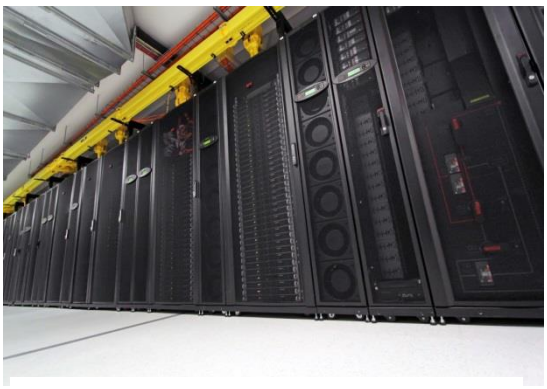
Det finns dock fortfarande mycket forskning som återstår kring hur störningar i teknisk infrastruktur påverkar samhället, hur dessa störningar kan sprida sig mellan infrastrukturer och viktiga samhällsfunktioner, förmågan att återställa dessa system vid storskaliga störningar, samt hur incitament kan utformas för robust försörjning av samhällsviktiga funktioner. Detta är spännande utmaningar som kommer kräva studier och utveckling av modeller och metoder från en mängd olika perspektiv för att kunna besvaras.

”Vid större störningar lånar aktörer resurser från andra aktörer inom samma område genom så kallade samverkansgrupper”

5. IT-system

En annan trend som har vuxit fram under de senaste 50 åren, men framför allt de senaste 20, är användandet av datorer och IT-system inom, i princip, alla verksamheter. IT-system har lett till stora förändringar för hur vi administrerar, kommunicerar, socialiserar, producerar varor, sköter bankärenden, etc. I början var det mest lokala, slutna system, det vill säga inom en organisation. Men sedan internets uppkomst har systemen blivit större i omfattning och därmed också mer komplexa. Med internet har också möjligheten att medvetet attackera IT-system ökat, eftersom alla som på något sätt är anslutna i någon mån är sårbara för attacker. Som ett resultat av denna utveckling används IT-system också i stor utsträckning inom samhällsviktig verksamhet och kan även betraktas som ett eget system på en större skala, dvs. nätverksinfrastrukturen. Exempelvis styrs el-systemen med hjälp av IT, flygplatser och tågtrafiken är beroende av sina ledningssystem, samtidigt som det finns ett behov av att kommunicera mellan myndigheter och organisationer, vilket även det sker till stor del med hjälp av IT-system.

IT-system skiljer sig från andra tekniska system eftersom väldigt små fel kan leda till stora konsekvenser väldigt fort. En rad kod i en rutinmässig uppdatering av ett system kan göra hela systemet obrukbart en längre tid, exempelvis var bankkunder hos Swedbank utan bank- eller korttjänster i tio timmar efter en intern uppdatering av systemen sommaren 2015 (DN, 2015). Naturligtvis vill vi ha pålitliga IT-system, men eftersom de beter sig lite annorlunda från andra tekniska system som elkraft behövs också andra metoder för att analysera risker och sårbarheter.



(CSIRO, 2016)

Efter att inom projektet undersökt olika metoder för att analysera IT-system från ett riskperspektiv, kunde det konstateras att det fanns väldigt få utvärderingar av sådana riskanalysmetoder. Därför valdes den av dem som ansågs mest lämplig ut och vidareutvecklades inom projektet. Ett resultat blev en så kallad ”Perspektivbaserad riskanalys” (PBRA). Grundtanken med denna metod är att man under riskanalysarbetet tittar på systemet från olika personers perspektiv, i det här fallet systemdesignern, systemtestarna, användarna med mera.

Metoden introducerades sedan till ett fyrtiotal försökspersoner som fick använda sig av PBRA eller en mer traditionell metod för riskanalys. Deras uppgift var att hitta risker i ett IT-system som styrde öppningen av dörrar på

tåg. De personer som använde sig av PBRA hittade fler relevanta risker än resten och upplevdes också som enklare att använda i jämförelse.

Projektet har även utvecklat en mjukvaruprototyp som automatiskt söker igenom texter online som har med IT-incidenter att göra, såsom nyhetsartiklar eller felrapporter. Programmet fick först en del test-texter för att lära sig vilka texter som innehöll relevant information, sedan fick det arbeta med att samla in data. Cirka 60 procent av texterna som programmet ansåg innehålla relevant information, gjorde det vid kontroll. Tanken med ett sådant program är att använda sig av en databas med inträffade händelser som stöd för personer som arbetar med riskanalyser inom IT, eftersom de då kan dra lärdom av tidigare fall.

I framtiden kommer fler metoder för riskanalyser testas i liknande studier, för att dra ytterligare lärdomar som kan användas för att förbättra PBRA. Ambitionen är att i slutändan ha utvecklat en riskanalysmetod som är specifikt anpassad för att hantera risker relaterade till IT-system inom svenska myndigheter och kommuner. För att det skall vara möjligt behöver den vara enklare att använda och mindre tidkrävande än existerande metoder, det vill säga den behöver vara mindre teknisk, mer översiktlig och fokusera på de mest kritiska funktionerna i verksamheten.

Referenslista

DN (Dagens Nyheter), 2015. Elektronisk källa. Hämtad från: www.dn.se/ekonomi/teknikproblem-for-swedbank-losta/ (2016-04-07)

CSIRO, 2016. Elektronisk källa. Hämtad från: http://www.scienceimage.csiro.au/image/2042 (2016-04-07)

MdE, 2004. Elektronisk källa. Hämtad från: https://commons.wikimedia.org/wiki/File:Umspannwerk_Abspannportal_Schalter.jpg (2016-04-08)

”Grundtanken med denna metod är att man under riskanalysarbetet tittar på systemet från olika personers perspektiv, i det här fallet systemdesignern, systemtestarna, användarna med mera”

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1080- februari 2017