KBM:S TEMASERIE | 2003:5

IT och sårbarhet

KRITISKA BEROENDEFÖRHÅLLANDEN I DEN NATIONELLA IT-INFRASTRUKTUREN

Andreas Malm, Jan Softa,
Jan Joel Andersson,
Klas Lindström

KRISBEREDSKAPS
MYNDIGHETEN

KBM:S TEMASERIE | 2003:5

IT och sårbarhet

KRITISKA BEROENDEFÖRHÅLLANDEN I DEN NATIONELLA IT-INFRASTRUKTUREN

Andreas Malm, Jan Softa,
Jan Joel Andersson, Klas Lindström

KBM:S TEMASERIE

2003:1 Bagdad-Bob, menige Jessica Lynch och Cirkus Saddam
Irakkriget iscensatt i svenska medier

2003:2 Irakkrigets andra dag
En jämförelse mellan SVT och tidningspressen den 21 mars 2003

2003:3 Krisberedskap i omvärlden
Samordningsstrukturer i fem länder

2003:4 Från osäker källa
Bevakningen av Irakkriget i svenska medier

2003:5 IT och sårbarhet
Kritiska beroendeförhållanden i den nationella IT-infrastrukturen

Titel: IT och sårbarhet – Kritiska beroendeförhållanden i den nationella IT-infrastrukturen
Utgiven av Krisberedskapsmyndigheten (KBM)
Omslagsfoto: Jack Mikrut/Prb
Övriga bilder: sid 12 Creative Collection, sidan 17;1,2 Future image bank, 17;3 PhotoDisc, 17;4 Edelpix
Upplaga: 2 000 exemplar

ISBN: 91-85053-27-9
KBM:s dnr: 0907/2003
Grafisk form: AB Typoform

Tryck: Edita Ljunglöfs, Stockholm 2003

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

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

KBM:s temaserie 2003:5

Innehåll

Förord

Pilotprojektet *Kritiska beroendeförhållanden – i den nationella IT-infrastrukturen* utfördes under sommaren och hösten 2003 av Krisberedskapsmyndigheten. Syftet med pilotprojektet var att pröva och utvärdera scenarioplanering som metod för att identifiera kritiska beroendeförhållanden mellan olika aktörer i den nationella IT-infrastrukturen i Sverige.[1]

I denna skrift beskriver vi hur insikten om beroendeförhållanden utgör en nödvändig del i säkerhetsarbetet kring den allt mer kritiska nationella IT-infrastrukturen. I skriften ger vi exempel på olika beroendeförhållanden och diskuterar hur dessa kan hanteras för att minska sårbarheten i det totala systemet. Vi visar även på behovet av att analysera beroendeförhållanden som en integrerad del i arbetet med att reducera samhällets sårbarhet i IT-infrastrukturen. Vi drar en skiljelinje mellan sårbarheter i och hot mot IT-infrastrukturen och kopplar dessa till det övergripande nationella arbetet med informations- och IT-säkerhet.

Utan de deltagande parternas engagemang i detta pilotprojekt hade det inte varit möjligt för oss att genomföra detta arbete. Vi vill därför rikta ett stort tack till alla deltagande och bidragande parter och hoppas att vårt gemensamma arbete skall bära frukt i form av säkerhetsförbättringar inom den nationella IT-infrastrukturen som kommer näringslivet, staten och den enskilde medborgaren till godo.

Konsultfirman 4C Strategies AB har på uppdrag av Krisberedskapsmyndigheten utfört pilotprojektet.

Krisberedskapsmyndigheten

[1] I denna skrift definierar vi kritiska beroendeförhållanden i infrastrukturer som en koppling mellan aktörer i infrastrukturer som innebär att funktionen i en infrastruktur påverkas av funktionen och agerandet i en annan infrastruktur. Om en kritisk infrastruktur inte kan användas kan det: Hota statens överlevnad; Ha allvarliga nedsättande konsekvenser för nationen i sin helhet; Negativt påverka stora delar av befolkningen; Kräva brådskande, om inte omedelbara, åtgärder.

Inledning

Det svenska samhället har under de senaste årtiondena successivt övergått från ett industrisamhälle till ett informationssamhälle. I dagens samhälle påverkar möjligheterna att sammanställa och använda information vårt sätt att göra affärer, vårt sätt att styra landet och vårt sätt att hantera kriser. Denna samhällsomvandling har möjliggjorts tack vare utvecklingen inom informationsteknologin (IT). Vissa forskare anser att utvecklingen av informationsteknologin på sätt och vis är en ”tyst revolution” men att det är mycket troligt att denna ”tysta revolution” kommer att påverka och förändra det internationella systemet och människors livsvillkor minst lika mycket som det kalla krigets slut gjorde.[1]

Förvandlingen från industrisamhälle till informationssamhälle har inte enbart medfört optimism och förväntningar utan även ovisshet och ängslan. Dessa motstridiga uppfattningar är inte helt förvånande med tanke på den oerhört snabba och stora strukturomvandling som den nya informationsteknologin innebär för myndigheter, näringsliv, beslutsfattare och medborgare.

En del forskare menar även att det kalla krigets slut medfört en förskjutning från en värld av fiender till en värld av faror och risker.[2] IT-revolutionen har utmålats som en sådan fara då den trots sina många fördelar även lett till en ökad sårbarhet i samhället på grund av beroendet av komplexa datoriserade system.[3] Redan 1978 påtalade en statlig utredning att det datoriserade svenska samhället blivit oacceptabelt sårbart, men utredningen ledde då inte till några större åtgärder.[4] Sedan mitten av 1990-talet har dock statsmakterna ägnat allt större uppmärksamhet åt informationsteknologin (IT) som en källa för allvarliga risker i samhället.[5]

---

1 Alberts & Papp, 1997. Sid. xiv.
2 Beck, 1999. Sid. 3.
3 Castells, 1996. Sid. 4.
4 Karlsson & Sturesson, 1995, Sid. 221.
5 Den första proposition som uppmärksammar IT som hot mot säkerheten är Prop. 1995/96:12.

Som en följd av denna förändring i synsätt har informations- och IT-säkerheten kommit att bli allt viktigare.

Tills för ett par år sedan berörde dock informationssäkerhet primärt statsmakternas hantering av klassificerad information. När vi idag diskuterar informationssäkerhet menar vi inte bara säkerheten kring statshemligheter utan även kring information som blivit kritisk för såväl näringslivet som samhället i stort. Säkerheten i bemärkelsen robustheten, tillförlitligheten och uthålligheten i den nationella IT-infrastrukturen har därför kommit att bli en fråga inte enbart för staten och näringslivet, utan för alla!

Säkerhet, sårbarhet och hot

Säkerhet är idag ett centralt begrepp inom IT och kan betecknas som ett tillstånd som innebär skydd mot okontrollerad insyn, förlust eller påverkan, oftast i samband med medvetna försök att utnyttja eventuella svagheter. Ett system är säkert i den utsträckning man anser sig kunna lita på att det fungerar (eller kommer att fungera) på avsett sätt. Bedömningen av detta kopplas som regel till en uppskattning av existerande eller potentiella hot.[1] Både teoretiker och praktiker har funderat över vilka sårbarheter och hot den informationsteknologiska utvecklingen medför för individ, samhälle och stat. Ofta fokuserar tekniker på tekniska brister i IT-produkter och system, medan samhällsvetare ofta fokuserar på vilka konsekvenser störningar kan få för individ, samhälle och stat. Att olika grupper har olika betoning på vad informations- och IT-säkerhet utgör kan vara bra och nödvändigt, men det kan även innebära att såväl förståelsen som analysen av sårbarheter och hot inte blir heltäckande.

Med *informationssäkerhet* menar vi säkerhet vid hantering av information avseende önskad tillgänglighet, (informations-) kvalitet, sekretess och spårbarhet.[2]

- *Tillgänglighet*: möjligheten att utnyttja resurser efter behov i förväntad utsträckning och inom önskad tid.
- *(Informations-) kvalitet*: att en informationsmängd inte avsiktligt eller oavsiktligt förändras eller förstörs.
- *Sekretess*: att information (eller ibland även dess existens) inte får göras tillgängligt eller avslöjas för obehöriga.
- *Spårbarhet*: att en verksamhet och tillhörande system skall innehålla funktioner som gör det möjligt att entydigt härleda utförda operationer till enskilda individer.

[1] Källa för denna begreppsbildning och terminologi, se Rapport ITS 6.
[2] PTS-ER-2002:24. Sid. 9.

Med *IT-säkerhet* avser vi de delar av begreppet informationssäkerhet som avser säkerheten i den tekniska hanteringen av information som bearbetas, lagras och kommuniceras elektroniskt samt administrationen kring denna.[1]

För att kunna diskutera och analysera informations- och IT-säkerhet är det också viktigt att tydliggöra skillnaden mellan sårbarheter och hot. Dessa begrepp blandas ofta ihop men vi har funnit det lämpligt att analytiskt skilja på begreppen. I denna skrift betecknar vi *sårbarheter* som härstammande från interna svagheter och brister i system och infrastrukturer betraktade såväl separata som sammansatta i en större helhet. *Hot*, å andra sidan, har sitt ursprung i en vid systemkonstruktionen oförutsedd eller riskmedvetet accepterad extern händelse eller påverkan. I den följande analysen av kritiska beroendeförhållanden i den nationella IT-infrastrukturen utgår vi från dessa två centrala begrepp.

[1] KBM, 2003:5.

Vilka är hoten?

Hoten mot den nationella IT-infrastrukturen kan delas upp i två huvudtyper – *aktörshot* och *icke-aktörshot*.

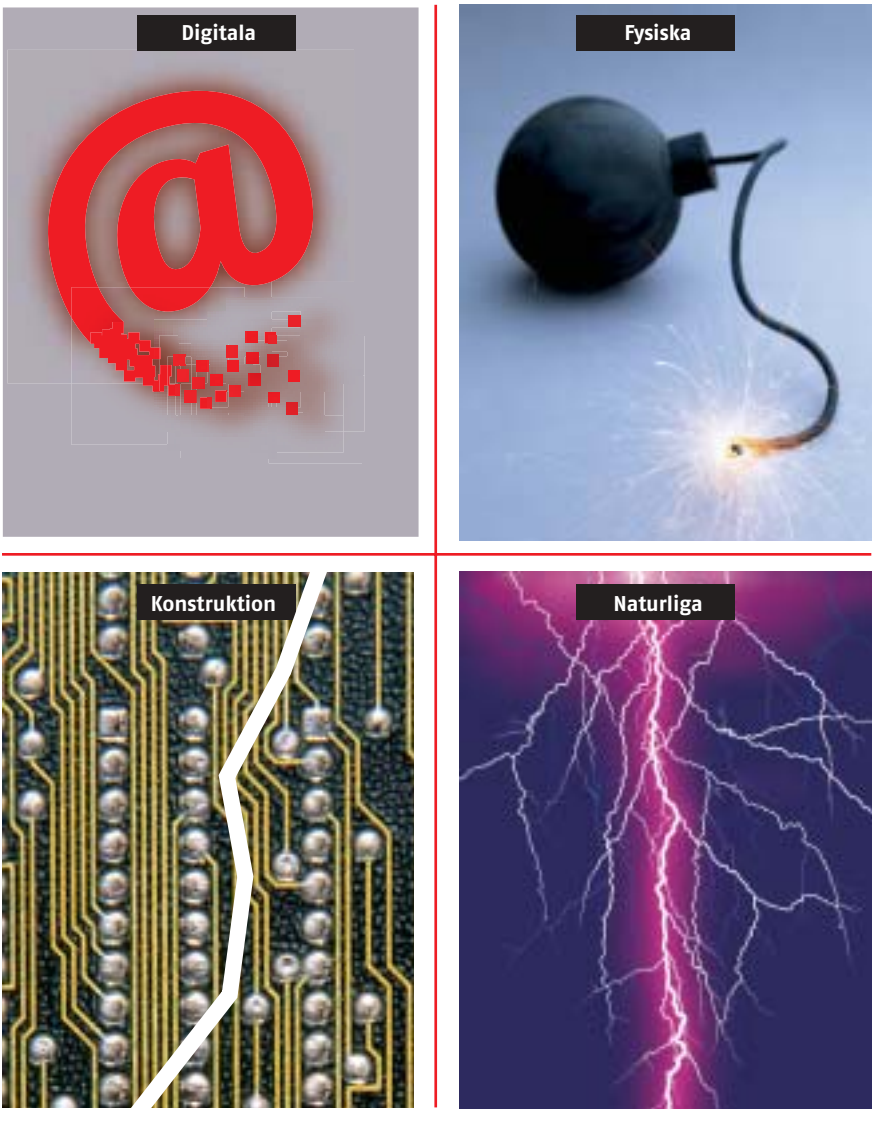
Utgångspunkten för *aktörshot* är att det är en aktör som är hotet. Aktörer kan vara unga ”hackare” eller ”crackare” som drivs av nyfikenhet, men kan även vara andra stater, konkurrerande företag, industrispioner, terrorister eller till och med egna medarbetare.[1] Dessa aktörer kan sedan *avsiktligt* eller *oavsiktligt* använda sig av *digitala* eller *fysiska* medel för att hota den nationella IT-infrastrukturen. Cyberattacker riktade mot företags eller myndigheters hemsidor, e-post eller IP-adresser är exempel på aktörshot utförda med *digitala* medel. Motivet för dessa attacker kan vara att aktörer ser en möjlighet att stjäla, manipulera eller förstöra data för att till exempel kunna påverka beslutsprocesser eller få tillgång till information i företag och myndigheter.[2]

Aktörer kan även använda sig av *fysiska* medel för att hota den nationella IT-infrastrukturen. Aktörshot med fysiska medel kan vara både oavsiktliga och avsiktliga. Ett exempel på ett oavsiktligt aktörshot med fysiska medel är dåliga säkerhetsrutiner som kan leda till olyckor och fysiska skador på IT-infrastrukturen i samband med montering eller underhåll av utrustning. Även om oavsiktliga hot fortfarande kan anses utgöra den större delen av aktörshoten har de avsiktliga aktörshoten mot den nationella IT-infrastrukturen ökat i antal, bland annat till följd av den nya typ av internationell terrorism som vi sett sedan det kalla krigets slut.[3] Det går inte att utesluta att icke-statliga aktörer med fysiska medel kan vara beredda att åstadkomma avsiktlig och omfattande skada mot viktiga samhällsintressen, något 11-septemberattackerna i New York och Washington DC i USA år 2001 tydligt visade. Även

[1] Hackare – en individ som finner glädje i att ha en djup förståelse av interna arbetssystem, speciellt datorer och datanätverk. Crackare – en individ som försöker att få tillgång till datasystem utan tillåtelse.
[2] Softa, 2003.
[3] KBM: 0753/2003, 2003.

MATRIS ÖVER HOT MOT IT-INFRASTRUKTUREN

Aktörshot



Icke aktörshot

”elektronisk” störning av kommunikationer och aktörers begagnande av elektromagnetiska vapen hör till denna kategori av hot då de renderar en yttre påverkan på elektronik/elektronisk utrustning.[1]

Icke-aktörshot, å andra sidan, utgörs av konstruktionsbrister och naturkatastrofer. *Konstruktionsbrister* uppkommer när ett system har otillräcklig säkerhetsnivå eller funktionalitet. Det kan exempelvis röra sig om funktionsfel (buggar) i för samhället kritiska IT-system. Y2K-buggen (också känd som millenniebuggen) är kanske det mest kända exemplet på en konstruktionsbrist som gestaltades som ett hot mot hela samhällen och stater.[2] *Naturkatastrofer* i form av oväder, jordbävningar, vulkanutbrott och laviner utgör också hot mot den nationella IT-infrastrukturen då dessa kan skapa avbrott i elförsörjningen och telekommunikationer vilka är en förutsättning för att Internet och e-post med mera skall kunna fungera. Naturkatastrofer som hot mot IT-infrastrukturen är något som betonas olika mycket från stat till stat. På Island till exempel betonas den unika naturen och de extrema väderförhållandena som ett hot mot öns IT-infrastruktur.[3]

[1] Elektronisk störning – En elektromagnetisk störning som avbryter, hämmar eller på annat sätt försämrar eller begränsar ett effektivt användande av elektronik/elektronisk utrustning. En sådan störning kan ske avsiktlig, som i vissa former av elektronisk krigföring, eller oavsiktlig, som ett resultat av bristfällig funktion i hård- eller mjukvara.

[2] Holmgren & Softa, 2001.

[3] Gunnarsson, 2002.

Vilka är sårbarheterna?

För att nå hög säkerhet och robusthet i IT-infrastrukturen är det nödvändigt att inte bara känna till de yttre hoten mot IT-infrastrukturen. Det är även nödvändigt att veta vilka de inre sårbarheterna är. Dessa kan påverka funktionen av IT-infrastrukturen samt påvisa möjliga konsekvenser av förverkligade hot. Som framgått vid flera tillfällen under senare tid kan inre sårbarheter genom förverkligade hot orsaka spontant inträffade sammanbrott i olika tekniska system. Dessa sammanbrott är särskilt allvarliga om de drabbar elförsörjningen, telekommunikationerna, vissa IT-system samt distributionen av radio- och TV-program.[1]

RISKANALYSMATRIS
KONSEKVENS & ÅRLIG SANNOLIKHET (ÅS)

	Frekvent Ås ≥ 1.0	Mycket möjligt Ås 0,1 ≥<1,0	Då och Då Ås 0,01 ≥< 0,1	Avlägset Ås 0,0001 ≥< 0,01	Ytterst avlägset Ås 0,000001 ≥< 0,0001	Omöjligt Ås <0,000001
Katastrofal	🔴🔴🔴	🔴🔴🔴	🔴🔴🔴	🟠🟠	🟡	🟢
Kritisk	🔴🔴🔴	🔴🔴🔴	🟠🟠	🟡	🟡	🟢
Marginell	🟠🟠	🟠🟠	🟡	🟢	🟢	🟢
Försumbar	🟢	🟢	🟢	🟢	🟢	🟢

🔴🔴🔴 Hög Risk 🟠🟠 Moderat Risk 🟡 Låg Risk 🟢 Rutinrisk

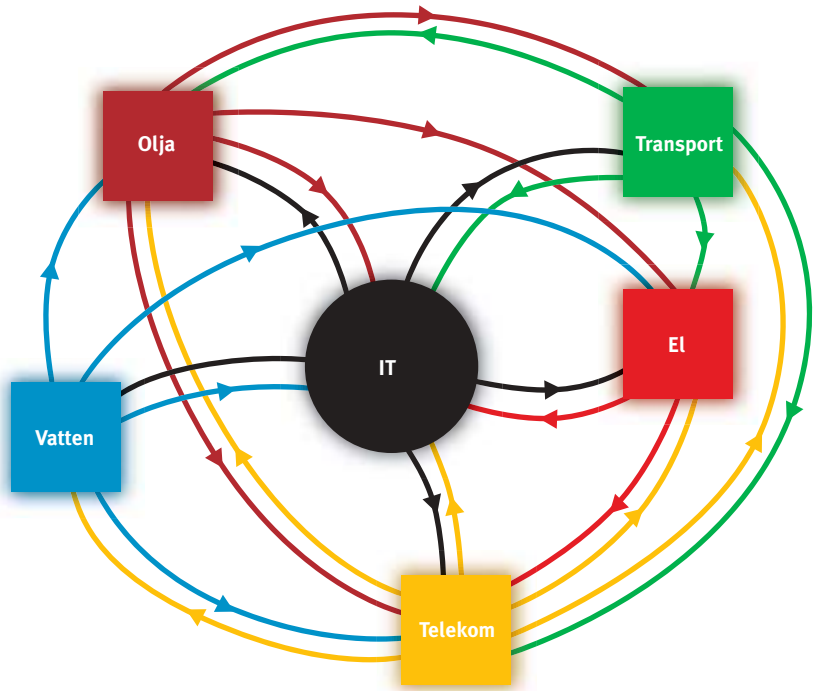
[1] KBM: 0753/2003, 2003

Robustheten i samhället i sin helhet och i IT-infrastrukturen i synnerhet kan drastiskt ökas genom att tidigt identifiera olika sårbarheter i den nationella IT-infrastrukturen. Dessa sårbarheter kan sedan åtgärdas och därmed kan konsekvenserna av eventuella realiserade hot minskas. I riskanalyssammanhang används ofta en sannolikhets- och konsekvensmatris. En sådan kan med fördel även användas i detta sammanhang. I matrisen utgör sårbarheten länken mellan hot med en viss sannolikhet och dess konsekvens om hotet realiseras.

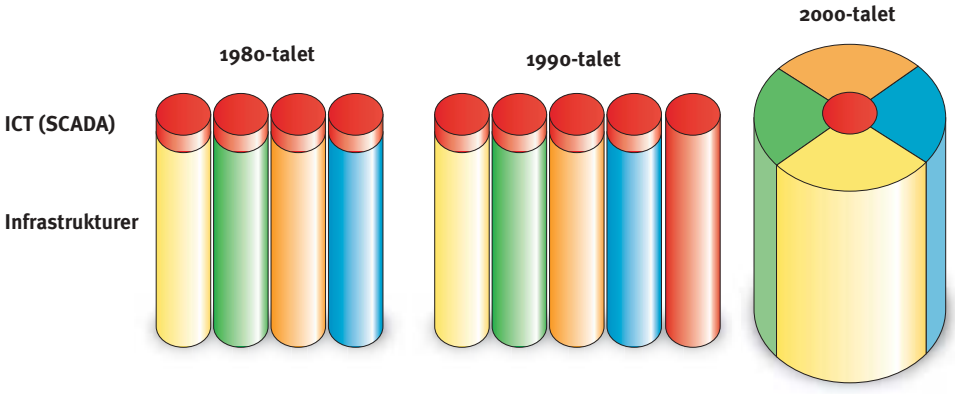
Under senare år har viktiga teknologiska, ekonomiska och juridiska förändringar dramatiskt påverkat sårbarheten i den nationella IT-infrastrukturen:

- Informationsteknologin har skapat mer sammankopplade infrastrukturer med större centralisering av kontrollfunktioner.
- Avreglering, koncentrering till färre aktörer och ökad konkurrens inom nyckelinfrastrukturer (el och tele) har kraftigt reducerat den reservkapacitet som tidigare kunde fungera som stötdämpare vid störningar.

INFRASTRUKTURELLA BEROENDEN OCH BEROENDEFÖRHÅLLANDEN



DET INFRASTRUKTURELLA LANDSKAPET



- Så kallade ”Information and Communication Technologies” (ICT), eller SCADA-lösningar, har blivit kritiska i leveransen av el, telekommunikationer, transport och hälso- och sjukvårdstjänster.
- Affärsverksamheters övergång till ”Lean Production”-principer, exempelvis övergången från ”just in case” till ”just in time”, har minskat toleransen för störningar i kritiska IT-infrastrukturer.

Vilken som helst av dessa förändringar borde vara skäl nog till oro. Insikten om den ökande sårbarheten har även lett till viktiga säkerhetsförbättringar i individuella infrastrukturer. Det är dock slående att de möjliga konsekvenserna av den ökade sammankopplingen av infrastrukturer med såväl ensidiga som ömsesidiga beroenden och beroendeförhållanden mellan aktörer nästan inte alls har uppmärksammats.[1]

På grund av beroenden mellan infrastrukturer och beroendeförhållanden mellan aktörer i dessa kan en störning i en infrastruktur enkelt spridas och allvarligt inverka på en annan infrastruktur som i sin tur kan påverka en tredje infrastruktur.[2] I dagens informationssamhälle är dessa intima kopplingar mellan infrastrukturer omfattande, vilket exemplifieras i bilden “Infrastrukturella beroenden och beroendeförhållanden”.

För att beskriva spridningen av en störning i en infrastruktur till en annan kan begreppen *kaskad-* och *eskaleringsfel* användas. Ett *kaskadfel* uppstår när

[1] Schmitz, 2003a.
[2] Beroenden syftar på tekniska kopplingar mellan infrastrukturer. Beroendeförhållanden syftar på kopplingar mellan aktörer/agenter i infrastrukturer.

ett avbrott i en infrastruktur förorsakar avbrott i en annan infrastruktur. Ett *eskaleringsfel* uppträder när ett avbrott i en infrastruktur förvärrar ett, från det första oberoende, avbrott i en annan infrastruktur (till exempel då tiden för återställning efter ett elavbrott förlängs på grund av att tillgången till telekommunikationer är begränsad). Under senare år har vi sett ett antal exempel på förekomsten av dessa fel.

Med anledning av att ICT:s (Information and Communication Technologies) blir allt vanligare i styrning och kontroll av kritiska infrastrukturer är det från ett informations- och IT-säkerhetsperspektiv fruktbart att betrakta dessa sammankopplingar mellan infrastrukturer utifrån ett evolutionärt perspektiv, där IT-infrastrukturen successivt har förskjutits mot centrum.

Denna successiva förändring av det infrastrukturella landskapet, i Sverige och internationellt, föranleder en breddning av det traditionella synsättet på informations- och IT-säkerhet. En analys av sårbarheter i IT-infrastrukturen kan inte enbart fokusera på den primära arkitekturen (t.ex. Internets uppbyggnad) utan måste även analysera försörjnings- och nyttjandeförhållanden. Om inte detta görs riskerar analysen att utelämna de kanske mest kritiska sårbarheterna. En modell utifrån vilken detta bredare perspektiv skulle kunna beskrivas på en övergripande samhällsnivå kan se ut som i bilden ”Det bredare analysperspektivet”.

Då få tidigare analyser har gjorts med detta bredare perspektiv finns det idag ett behov av att utveckla teknologier och metoder för att identifiera sårbarheter och skydda den nationella IT-infrastrukturen mot allvarliga störningar. I Sverige ägs och styrs merparten av IT-infrastrukturen av näringslivet som i egenskap av affärsdrivande organisationer ofta inte har en större drivkraft att investera i säkerhetsrelaterade teknologier och metoder då dessa tenderar till: att vara mycket långsiktiga, innebära hög risk, kunna anammas av konkurrenter eller vara mindre troliga att skapa vinster till investerare. Sådana teknologier och metoder skulle visserligen gynna samhället i sin helhet men sällan ett enskilt företag i tillräcklig utsträckning för företaget att motivera investeringen.[1] Det övergripande ansvaret för att stimulera utvecklingen av teknologier och metoder för att nå en högre robusthet i de infrastrukturer som är kritiska för det svenska samhället måste därför ligga på den statliga sektorn.

Flera internationella studier som analyserat beroenden och beroendeförhållanden har konstaterat att en substantiell analys av framför allt beroenden mellan infrastrukturer (primärt av teknisk natur) förutsätter modellerings och simuleringshjälpmedel på grund av den höga graden av komplexitet i bero-

[1] Sådana tjänster och varor benämns ofta som ”Public Good”.

DET BREDARE ANALYSPERSPEKTIVET

Nyttjande
Krishantering
Finans och Handel
Energistyrning
Telekomstyrning
Hälsa och sjukvård
Transportstyrning etc.

Tjänster
Elektroniska transaktioner
Datautbyte
Multimediaobjekt
Samverkansstöd
Resurssökning etc.

Bit vägar
Telekommunikationer
Satellit
Fiberoptik
Kabel-TV
Mobilt etc.

Försörjning
El
Vatten
Transporter etc.

endeanalysen. Beroendeförhållanden å andra sidan, primärt av mänsklig natur och syftandes på kopplingar mellan aktörer och så kallade agenter i infrastrukturer, kan förmodligen analyseras med hjälp av enklare och mer kostnadseffektiva analysverktyg och metoder, exempelvis scenarioplanering, något som vi har tagit fasta på i denna studie.[1]

[1] Se till exempel, Schmitz, 2003a.

Projektets belysning av sårbarheter

I pilotprojektet *Kritiska beroendeförhållanden – i den nationella IT-infrastrukturen* som redovisas i denna skrift har vi prövat scenarioplanering som metod för att identifiera kritiska beroendeförhållanden mellan statliga och privata aktörer i den nationella IT-infrastrukturen.[1] Inom projektet genomfördes tre scenarioövningar med representanter från näringsliv, stat och kommuner. Utifrån resultaten från den första scenarioövningen identifierades betydelsen av att ha en g*emensam lägesuppfattning* samt att undvika *beredskapskollisioner* som nödvändiga komponenter för att öka robustheten i den nationella IT-infrastrukturen. Vid den andra scenarioövningen prövades behovet av att ha en gemensam lägesuppfattning och nödvändigheten av att undvika beredskapskollisioner. Scenarioövningen visade att de två faktorerna utgjorde reella kritiska beroendeförhållanden mellan centrala aktörer i den nationella IT-infrastrukturen. Under den tredje och avslutande scenarioövningen låg fokus på att söka möjliga lösningar till de kritiska beroendeförhållanden som tidigare identifierats. Nedan följer en mer detaljerad analys och redovisning av dessa två beroendeförhållanden.

En gemensam lägesuppfattning

Vid den inledande scenarioövningen visade det sig att en gemensam lägesuppfattning är en viktig tillgång vid en störning i samhället som påverkar den nationella IT-infrastrukturen. Om inte en gemensam lägesuppfattning existerar kan enskilda aktörers handlande leda till en försämring för samhället i stort.

I händelse av en kris eller en allvarlig störning skulle de flesta aktörerna söka

[1] Ett scenario visar på en tänkbar framtida utveckling. Bakom scenariot ligger en fri analys av hur framtiden kan utveckla sig. Scenarier är inte prognoser över framtiden utan fokus ligger snarare på ”tänk om detta händer”. För mer information rörande scenarioplanering och integreringen av såväl kognitiva som fysiska aspekter, se Heugens & van Oosterhout, 2001, och Schoemaker, 1988.

information om situationen från många olika källor.[1] Detta beror på att i dagsläget har varken stat eller näringsliv en organisation eller instans för att förse myndigheter och företag med analyserad och validerad information om läget före, under och efter en kris, något som innebär att förutsättningarna för en snabb och kostnadseffektiv krishantering är svåra att uppnå. Vid den andra scenarioövningen visade det sig tydligt att de IT-ansvarigas sätt att handla vid en kris kan leda till framförallt två oönskade fenomen. Dessa fenomen har vi valt att beteckna *förvrängd information* och *obearbetad information*.

Med myndigheters och företags nuvarande rutiner för att samla in information riskerar informationen att förvrängas innan den når andra myndigheter och företag. Fenomenet kan liknas vid den populära viskningsleken hos barn där en rundgång av en relativt stor informationsmängd i slutändan har påverkat informationen så till den grad att den har fått en ny innebörd, informationen är förvrängd.

I dag genomförs även all väsentlig analys av obearbetad information hos enskilda myndigheter och företag, ett förhållande som kan innebära att det övergripande och mest kritiska perspektivet inte belyses. Det är till exempel svårt för en teleoperatör att känna till hur de ska agera vid störningar i deras telekommunikationsnät utan att negativt påverka andra infrastrukturer och därmed funktionen i andra viktiga samhällssektorer.[2] Detta problem förefaller vara allvarligast på nationell nivå där ansvarsförhållandena upplevs som avsevärt mer oklara än på lokal och regional nivå. Det bör även understrykas att de kommuner, länsstyrelser, myndigheter och företag som deltagit i detta projekt framhållit att det är vid kriser på nationell nivå som de stora problemen och kostnaderna inträffar. Flera representanter från de deltagande företagen påtalade därför särskilt behovet av tillförlitlig och bearbetad information. Obearbetad information förefaller idag finnas hos myndigheter, men den varken sammanställs, bearbetas eller delges kritiska aktörer, vare sig statliga eller privata.

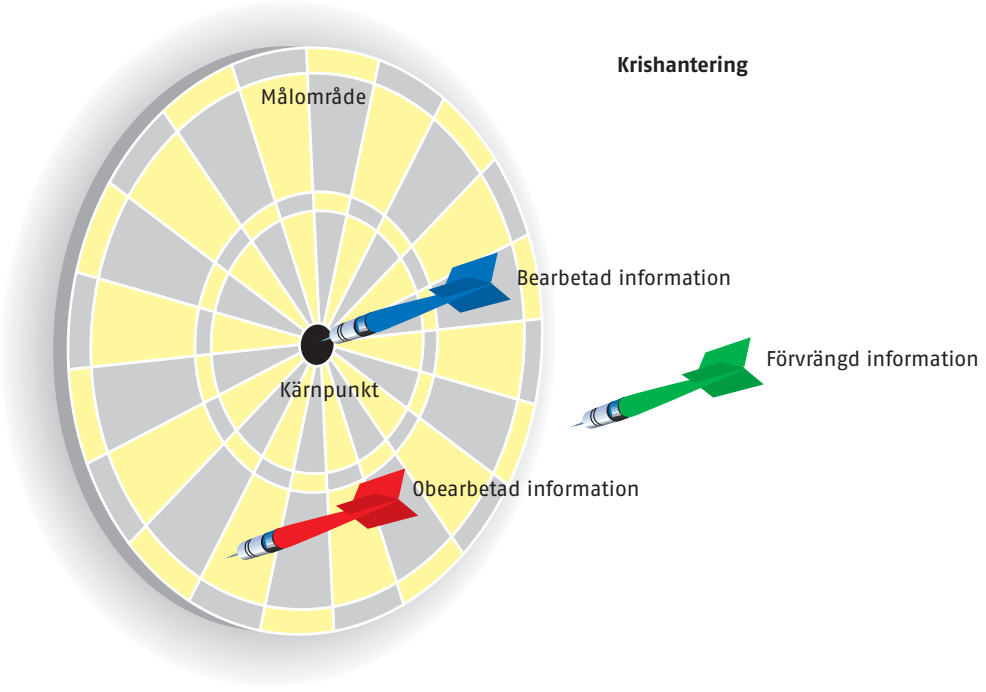
För att kunna uppnå fördelarna med en gemensam lägesuppfattning hos de aktörer som är centrala för funktionen av det svenska samhället prövades i en scenarioövning ett webbaserat informationssystem för att inhämta och sprida obearbetad information. Även om detta informationssystem kan tänkas minska uppkommande problem såsom förvrängd information, ansåg deltagarna vid scenarioövningen att det inte är tillräckligt med att enbart sammanställa och sprida information.[3] För att en gemensam lägesuppfattning skall upp-

[1] Med reservation för det begränsade antalet deltagare som detta projekt arbetat med.

[2] En typ av fel inom kategorin kaskadfel = ett avbrott i en infrastruktur förorsakar spridningsavbrott i en andra infrastruktur.

[3] Det undersökta webbaserade informationssystemet är tänkt att initialt vara tillgängligt för statliga/kommunala aktörer i krishanteringsstrukturen. Möjligen skall denna krets utvidgas till att även omfatta privata aktörer.

VIKTEN AV EN GEMENSAM LÄGESUPPFATTNING



nås bör informationen även bearbetas. Ett ansvar för denna uppgift borde ligga på en instans som samlar in och sprider information vid en kris eller störning. Uppgiften kan eventuellt finnas på lokal, regional och central nivå.

Under scenarioövningarna framkom även kritik mot att enbart använda ett webbaserat informationssystem eftersom det inte skulle vara en tillräcklig lösning för att skapa en gemensam lägesuppfattning. Detta beror på att de myndigheter och företag som drabbats av en allvarlig kris ofta har problem med att nå den information de behöver för sitt fortsatta agerande. Inte minst vid elavbrott är det svårt för ansvariga av IT-driften i den drabbade regionen att ha någon nytta av ett webbaserat informationssystem, då datorer utan tillgång till reservkraft inte fungerar! Detta problem expanderar betydligt vid kriser på nationell nivå, till exempel vid långvariga el-bortfall på grund av avsiktliga eller oavsiktliga störningar i energiförsörjningen.

En annan viktig aspekt är vart myndigheter, företag och allmänhet vänder sig i händelse av en kris för att få reda på vad som hänt. Vid exempelvis tele-

störningar kontaktas Telia eller den anlitade teleleverantören. Det är med andra ord inte självklart att en statlig myndighet skulle kontaktas för att få information. Därför är det fördelaktigt om all rapportering och informationsspridning liknar det normala så mycket som möjligt. Med anledning av dessa reflektioner bör man innan kriser inträffar ha funderat på följande frågeställningar:

– Vilken information skall nå ut till de olika målgrupperna vid olika typer av kriser? – Vilka kriser kan bli/vara aktuella som hotar informationshanteringen? Vid scenarioövningarna framkom det att återkommande och realistiska scenarioövningar, med ett brett deltagande från kommuner, statliga myndigheter och företag kan hjälpa till att besvara dessa frågeställningar.

I händelse av en större kris, av regional eller nationell karaktär, kan även problem uppkomma hos myndigheter och företag på grund av tillgången till en gemensam lägesbild. Föreställ dig att en central instans har inhämtnings-, analys- och delgivningsansvar av information i syfte att undvika att privata aktörer enbart agerar utifrån egna affärsmässiga hänsyn, vilket kan vara negativt ur ett samhällsperspektiv. Utifrån informationen som sänds genom den gemensamma lägesbilden är det upp till var och en av myndigheterna och företagen att fatta beslut om åtgärder, ett förhållande som förefaller önskvärt. Den implicita vägledning som analyserad och bearbetad information skapar kan dock förorsaka en otydlighet i ansvars- och rollfördelningen. Man behöver bara gå så långt som att fundera över vem som har det politiska, ekonomiska och juridiska ansvaret i denna situation? Vad händer till exempel om den enskilda privata aktörens agerande, baserat på en publicerad men felaktig gemensam lägesbild, förorsakar skada eller lidande som kunnat undvikas om informationen hade varit korrekt?

En slutsats från de genomförda scenarioövningarna är att ett webbaserat informationssystem bör, innan en eventuell utveckling inleds, studeras noggrannt utifrån ett centralt, regionalt och lokalt perspektiv, då lösningen endast ter sig funktionell i vissa syften och under vissa faser av en samhällsstörning. Frågan om att uppnå en gemensam lägesuppfattning, hos de myndigheter och företag som är nödvändiga för funktionen av det svenska samhället, bör också analyseras i ett vidare sammanhang. I dagsläget är frågorna många och svaren få, något som följande frågeställningar belyser: var borde funktionen för att inhämta, analysera, bearbeta och delge information ligga; hur bör organisationen för detta vara dimensionerad; vilka kanaler och kommunikationsmedel bör nyttjas; vilka utgör de mest kritiska statliga respektive privata aktörerna som skall få ta del av informationen; hur skall media hanteras; hur hanteras ekonomiska, juridiska och politiska ansvarsfrågor som följer med en informell och implicit ledning av statliga, privata och kommunala aktörer?

Beredskaps-kollisioner

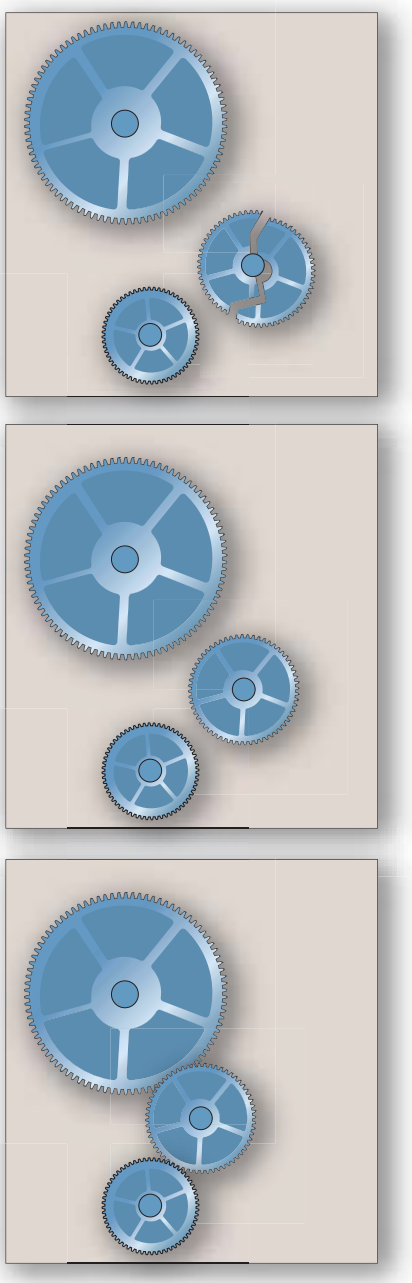
I denna studie har det bland annat konstaterats att flera infrastrukturer har ett ömsesidigt beroende av varandra. Detta ömsesidiga beroende kan leda till vad vi har valt att benämna *beredskapskollisioner*. En beredskapskollision är när en eller flera aktörers agerande vid en kris kan leda till en enskild fördel och samtidigt till en kollektiv nackdel. Ett hypotetiskt exempel på detta är om elen skulle slås ut och det finns en tidslucka på ett antal timmar innan ett utslaget kraftverk kan startas upp. För att kunna starta upp ett kraftverk efter ett avbrott behövs telekommunikationer, som ibland har batteridrift för en viss tid efter att elen fallit bort. Om en uppstart av kraftverket inte kan genomföras innan batterierna tar slut finns det en risk att uppstarten av kraftverket kan försenas från timmar till dagar.[1]

Detta exempel på beredskapskollisioner har vi valt att benämna *temporala kollisioner,* då tidsfaktorn i de två infrastrukturella aktörernas beredskapsplanering inte är synkroniserad. Utöver denna typ av beredskapskollisioner har pilotstudien även visat på förekomsten av *fysiska* och *logiska beredskapskollisioner*. Fysiska kollisioner inträffar när ett flertal aktörer vid kriser förlitar sig på resurser, varor eller tjänster från andra aktörer för att kunna fungera, och dessa aktörer inte kan täcka de förstnämda aktörernas samlade behov. Ett exempel på fysiska beredskapskollisioner är när Försvarsmakten kort inför millennieskiftet kontaktades av en länsstyrelse, som tidigare sett möjligheten att förlita sig på Försvarsmaktens el/beredskapsaggregat i händelse av eventuella störningar i energiförsörjningen. Det visade sig då att det inte var möjligt nyttja dessa aggregat eftersom Försvarsmaktens el/beredskapsaggregat inte levererar växelström, som i det civila samhället, utan likström. *Logiska beredskapskollisioner* å andra sidan syftar på fallen där en aktör, kanske beroende på bristande information, beslutar och agerar på ett vis som direkt eller indirekt förvärrar eller försvårar den övergripande situationen för den nationella IT-infrastrukturen.

För att undvika beredskapskollisioner behövs två kompletterande lösningar. För logiska beredskapskollisioner är lösningen densamma som för den gemensamma lägesuppfattningen. En lösning på tänkbara temporala och fysiska beredskapskollisioner hos olika myndigheter och företag borde däremot ligga i en jämförelse av deras beredskapsplaner. Hos de flesta organisationer finns dock en medvetenhet om att beredskapsplaner i samband med störningar snabbt blir föråldrade, var-

[1] En typ av fel inom kategorin eskaleringsfel = ett avbrott i en infrastruktur förvärrar ett självständigt/oberoende avbrott i en andra infrastruktur.

SYNKRONISERING AV BEREDSKAPSPLANER OCH INTUITIVT AGERANDE



efter ett intuitivt och situationsanpassat beslutsfattande tar vid. Detta innebär inte att behovet av att jämföra och i slutändan synkronisera beredskapsplaner mellan myndigheter och företag försvinner eftersom själva processen skapar en förståelse för beroenden och beroendeförhållanden parterna emellan. Förståelsen blir som ett ramverk vid ett intuitivt beslutsfattande och kan vara en lämplig lösning för att undvika beredskapskollisioner i samtliga faser av en störning. Samordningen av denna verksamhet kan genomföras på regional, lokal och central nivå genom exempelvis regelbundna scenarioövningar inom de olika samverkansområdena.[1]

Pilotprojektet *Kritiska beroendeförhållanden – i den nationella IT-infrastrukturen* har också visat att det största hindret för att inleda ett närmare samarbete mellan stat och näringsliv ligger i förtroendeklyftan som idag finns dem emellan. Vissa samhällsviktiga aktörer i näringslivet är idag tveksamma till att öppet och ärligt redovisa beredskapsrutiner, resurser och tidsförhållanden på grund av den nuvarande utformningen och tillämpningen av sekretesslagstiftningen, offentlighetsprincipen och tillsynsansvaret. Det kan därför finnas anledning att i mer detalj utreda formerna för hur privat-offentlig samverkan skall utformas inom området beredskapskollisioner för att överbrygga förtroendeklyftan mellan stat och näringsliv. Denna förtroendeklyfta är i själva verket en beredskapskollision i sig där ett samarbete för att öka den kollektiva informationssäkerheten hindras av den nuvarande informationssäkerhetslösningen hos den ena parten, i detta fall staten.

[1] Krisberedskapsmyndigheten arbetar idag med 6 olika samverkansområden: Teknisk infrastruktur; Transporter; Spridning av allvarliga smittämnen, giftiga kemikalier och radioaktiva ämnen; Ekonomisk säkerhet; Områdesvis samordning, samverkan och information; Skydd, undsättning och vård.

Slutsatser

En första övergripande slutsats av pilotprojektet *Kritiska beroendeförhållanden – i den nationella IT-infrastrukturen* är att en hög medvetenhet om behovet av en gemensam lägesuppfattning och undvikandet av beredskapskollisioner bör kännetecknа privat-offentlig samverkan på lokal, regional och central nivå. Det finns också ett behov av en central funktion för kontinuerlig uppdatering av nationella risker och sårbarheter i samhället. Dessa uppdateringar är grunden för ett strategiskt, operativt och taktiskt säkerhetsarbete i såväl kritiska företag som statliga och kommunala instanser. Funktionen bör vara fristående från de tillsynsmyndigheter som finns idag och införandet av nationella risknivåer bör övervägas för vägledning. Om risknivån höjs till ”hög” skulle det kunna föranleda åtgärder hos ett företag såsom exempelvis begränsningar i tillgång till system hos användare och att så kallade krisportaler upprättas mellan företag och myndigheter.

En andra övergripande slutsats av projektet är att en kartläggning bör genomföras av vilka system som är kritiska för att samhället skall fungera. Därefter bör en kartläggning göras ner till lämplig detaljnivå för att finna ut vilka andra system som är beroende av dessa samhällskritiska system. Om man kan ge en korrekt bild av hur systemen i den nationella IT infrastrukturen påverkar varandra är det möjligt att modellera, simulera och visualisera eventuella problem vid allvarliga störningar. Initialt kan ett sådant ”kartläggningsprojekt” begränsas i omfattning för att inte dra ut på tiden och bli ohanterligt komplext. Informationen bör hanteras i ett databasformat för att kontinuerligt kunna uppdateras och analyseras. Ett sådant system skulle göra det möjligt för beslutsfattare att plocka ut analyserad information som ger förutsättningar för informerat beslutsfattande som tar hänsyn till effekter på tredje part och eventuella beredskapskollisioner. Den här typen av informations- och analyskapacitet skulle ge förutsättningar för att upprätthålla en hög säkerhetsnivå och robusthet på lokal, regional och central nivå.

På en mer detaljerad nivå står det klart att en *gemensam lägesuppfattning* bland de privata och statliga aktörerna

inom den kritiska IT-infrastrukturen utgör ett kritiskt beroendeförhållande parterna emellan. Det webbaserade informationssystemet som analyserats ovan verkar endast vara en funktionell lösning för vissa syften och under vissa faser av en samhällsstörning. Frågan om en gemensam lägesuppfattning bland de kritiska aktörerna bör för att komplettera denna lösning analyseras i ett vidare sammanhang, vilket tydligare belyser och utreder de frågeställningar som identifierats i detta pilotprojekt. Det vill säga: var borde funktionen för att inhämta, analysera, bearbeta och delge information ligga; hur bör organisationen för detta vara dimensionerad; vilka kanaler och kommunikationsmedel bör nyttjas; vilka utgör de mest kritiska statliga respektive privata aktörerna som skall få ta del av informationen; hur skall media hanteras; hur hanteras ekonomiska, juridiska och politiska ansvarsfrågor som följer med en informell och implicit ledning av statliga, privata och kommunala aktörer?[1]

Med anledning av detta pilotprojekt står det även klart att möjliga beredskapskollisioner förorsakar reella beroendeförhållanden mellan aktörer i kritiska infratrukturer. Olika former av privat-offentlig samverkan kan eventuellt vara ett sätt att arbeta bort *beredskapskollisioner*. Internationellt sett finns ett antal olika modeller för ett sådant samarbete idag. Dessa modeller i kombination med svenska erfarenheter kan ligga till grund för en försöksverksamhet med en infrastrukturell gränsöverskridande samverkan i syfte att identifiera och arbeta bort existerande beredskapskollisioner.[2] Bland deltagarna på scenarioövningarna tycks det råda konsensus om att scenarioplanering är en mycket lämplig metod för att uppnå detta. I förlängningen bör dock scenarioplanering kompletteras med modellerings-, simuleringsverktyg och mer substantiella analyser. Förutsättningar för en verksamhet som denna borde kunna utredas i det större perspektivet kring förutsättningarna för en funktion för nationella risk- och sårbarhetsanalyser.[3]

Avslutningsvis kan nämnas att scenarioplaneringsmetoden som nyttjats under denna studie visade sig vara en framgångsrik och kostnadseffektiv metod för att identifiera, analysera och diskutera kritiska beroendeförhållanden i den nationella IT-infrastrukturen. *Scenarioplanering* förefaller därför vara en lämplig metod för kommuner, staten och näringslivet för att skapa ny kunskap om såväl beroendeförhållanden

[1] För erfarenhetsinhämtning kan vi i detta sammanhang hänvisa till CERT funktioner i USA, WARP-projektet och UNIRAS i Storbritannien samt TISN-projektet i Australien. Det sistnämnda utgör en instans för allmän delning av information rörande krishantering mellan aktörer i näringslivet samt staten.

[2] De svenska initiativ som åsyftas är SITIC och samarbeten inom HEL-projektet.

[3] En utveckling som skulle ligga i linje med resultaten av den forskning som genomförts inom området under den Europeiska Kommissionens ”Information Society Technology” program (FP6). Se Schmitz, 2003b.

som tänkbara framtida sårbarheter i den kritiska nationella IT-infrastrukturen.[1] I projektet har metoden även lett till nya frågeställningar om ömsesidiga beroendeförhållanden, som i sin tur kan ge uppslag till nya forskningsinsatser. Förutom att faktisk generera ett substantiellt underlag för analys har scenarioplaneringsmetoden även skapat ett mervärde i form av engagemang och intresse för samhällskritiska frågor hos de deltagande aktörerna, något som får betecknas som mycket positivt. Vår sammantagna bedömning är därför att scenarioplaneringsmetoden, likväl som flera av de verktyg som använts och utvecklats i detta projekt, med fördel kan användas för liknande projekt i större skala.[2]

[1] För mer detaljerad information rörande scenarioplanering, se Godet, 2000.

[2] För detaljerad information om den scenarioplaneringsmetod som användes i pilotprojektet och de verktyg som nyttjades, se Malm et al, 2003.

Referenser

Alberts, D. & D. Papp, (red.), 1997. *The Information Age: An Anthology on its Impacts and Consequences, vol. 1*. Washington DC: National Defense University.

Beck, U., 1999. *World Risk Society*. London: Polity.

Castells, M., 1996. *The information age: Economy, Society and Culture, vol. 1*: *The rise of the network society*. Malden: Blackwell.

Eriksson, J., 2001. *Hotbildernas politik*. Stockholm: Utrikespolitiska institutet.

Godet, M., 2000. ”The art of scenarios and strategic planning: tools and pitfalls”. *Technological Forecasting And Social Change*, Vol. 65. nr. 1.

Gunnarsson, J., (E-mail). Chairman of the Information Society Task Force, Prime Minister's Office, Iceland. 2002-07-09.

Heugens, P. & J. Van Oosterhout, 2001. ”To boldly go where no man has gone before: integrating cognitive and physical features in scenario studies”. *The Journal of Forecasting Planning and Policy.* Vol. 33. no. 10.

Hinnfors, J., 1995. *På dagordningen?: Svensk politisk stil i förändring*. Stockholm: Nerenius & Santérus Förlag AB.

Holmgren, J., & J. Softa, 2003. *Functional Security*. Manuscript.

Holmgren, J., & J. Softa (2001) *Årtusendets hot? Y2k-buggen på dagordningen i Ryssland, Sverige och USA*. Stockholm: Utrikespolitiska institutet.

Karlsson, M., & L. Sturesson (1995) *Världens största maskin*. Stockholm: Carlssons.

KBM 2003:5. *Basnivå för IT-säkerhet (BITS) – Rekommendationer från Krisberedskapsmyndigheten*. Stockholm: Krisberedskapsmyndigheten.

KBM 0735/2003. *KBM:s inriktning för utredningsarbetet inför 2004 års försvarsbeslut*. Opublicerad rapport.

Kingdon, J. 1995. *Agendas, Alternatives and Public Choices*. 2nd ed. New York: Harper Collins College Publishers.

Malm, A., K Lindström & J. J. Andersson, 2003. *Kritiska beroendeförhållanden – i den nationella IT-infrastrukturen*. Krisberedskapsmyndigheten. Opublicerad rapport

Prop. 1995/96:12. *Totalförsvar i förnyelse*. Stockholm: Försvarsdepartementet.

PTS-ER-2002:24. *Tillit till IT vid Internetanvändning*. Stockholm: Post & Telestyrelsen.

Rapport ITS 6 - terminologi för informationssäkerheten, 1994. Stockholm: Informationstekniska Standardiseringen.

Schmitz, W., 2003a. *Summary of cross-connections between WP1 and WP6 Deliverables*. European Commission: ACIP-IST-2001-37257 D 6.1.

Schmitz, W., 2003b. *Roadmap "Information and Communication Technology (ICT) Security Assesment Methods in Critical Infrastructures"*. European Commission: ACIP-IST-2001-37257. D 2.5.

Schoemaker, P. J.H., 1988. *The Scenario Approach To Strategic Thinking: Methodological, Cognitive And Organisational Perspectives*. Chicago: University of Chicago.

Softa, J., 2003. *De glömda pusselbitarna vid uppfattningen och analysen av IT-hot*. Manuskript.

Pilotprojektet KRITISKA BEROENDEFÖRHÅLLANDEN I DEN NATIONELLA IT-INFRASTRUKTUREN utfördes under sommaren och hösten 2003 av Krisberedskapsmyndigheten. Syftet med pilotprojektet var att pröva och utvärdera scenarioplanering som metod för att identifiera kritiska beroendeförhållanden mellan olika aktörer i den nationella IT-infrastrukturen i Sverige.

Med utgångspunkt i resultatet av pilotprojektet beskriver vi i denna temaskrift hur insikten om beroendeförhållanden utgör en grundläggande och nödvändig del i säkerhetsarbetet kring den allt mer kritiska nationella IT-infrastrukturen. Vi redogör för de olika beroendeförhållanden som analyserats i projektet, *en gemensam lägesuppfattning och beredskapskollisioner*, och diskuterar hur dessa kan hanteras för att minska sårbarheten i det totala systemet. På det övergripande planet visar vi även på behovet av och möjligheterna till att analysera beroendeförhållanden, en analys som bör utgöra en integrerad del i ett bredare arbete med att reducera samhällets sårbarhet i kritiska infrastrukturer. Konsultfirman 4C Strategies AB har på uppdrag av Krisberedskapsmyndigheten utfört pilotprojektet.

ISBN 91-85053-27-9

Krisberedskapsmyndigheten

Box 599
101 31 Stockholm

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

kbm@krisberedskaps
myndigheten.se

www.krisberedskaps
myndigheten.se