Kristålighet genom privat-offentlig samverkan

Årlig redovisning från KKrVA avd V den 25 september 2012 av Per Kulling, Bo Richard Lundgren, Bengt Sundelius, Leif Vindevåg och Marie Hafström

I DEN ÅRLIGA redovisningen för 2006 i KKrVA avdelning V (avdelningen för annan vetenskap av betydelse för rikets säkerhet och försvar) var titeln ”Förmåga till ledning och ledarskap vid civil krishantering?”[1] och där rekommenderades ett antal områden för fortsatta studier. Ett av dessa områden utgjorde avdelning V:s årliga redovisning för 2011: ”Fungerar samverkan i krishantering”.[2] I denna studie konstaterades att privat-offentlig samverkan vid krishantering var ett område som behövde belysas ytterligare. Efter diskussioner i Kungliga Krigsvetenskapsakademien, KKrVA, avdelning V beslutades att i årlig redovisning för 2012 skulle privat-offentlig samverkan belysas i ett seminarium med titeln ”Kristålighet genom privat-offentlig samverkan”. Detta seminarium avhölls den 25 september 2012 och sammanfattas här.

Inledning

När Krigsvetenskapsakademiens avdelning V anordnar ett seminarium om kristålighet genom privat-offentlig samverkan är det en satsning som berör ett viktigt ämne. Definitionen och innebörden av begreppet kris kan diskuteras, men i detta sammanhang används regeringens definition, d v s en händelse som drabbar eller berör många människor och stora delar av samhället samt hotar grundläggande värden och funktioner.

Vid allvarliga händelser och kriser med nationella konsekvenser är det främst regeringens uppgift att hantera övergripande normativa och strategiska frågor samt att på en övergripande nationell nivå säkerställa en effektiv krishantering. Men ansvaret för samordning av åtgärder som krävs för att hantera en allvarlig händelse eller kriser av nationell karaktär ligger på de statliga förvaltningsmyndigheterna.

Privat och offentlig samverkan behandlas i budgetpropositionen 2012/13.[3] Där anförs att utvecklingen karaktäriseras av en långtgående specialisering inom samhällsviktig verksamhet, och det blir dessutom allt vanligare att privata aktörer har ett ansvar i den samhällsviktiga verksamheten. Det finns anledning, enligt regeringen, att kontinuerligt se över och analysera hur de s k samverkansområdena på ett mer effektivt och ändamålsenligt sätt kan uppnå målen för samhällets krisberedskap. Det är av största vikt att de myndigheter som ingår i samverkansområdena tillsammans med Myndigheten för samhällsskydd och beredskap, MSB, fortsätter arbetet för att utveckla former för att öka privata aktörers deltagande i arbetet inom samverkansområdena. Syftet med seminariet var att belysa hur det ser ut idag, vad är bra, var finns

bristerna och sårbarheten, vad behöver åtgärdas – på kort och längre sikt, och hur kan vi förbättra kriståligheten genom privat och offentlig samverkan?

Bakgrund

Seminariet fokuserade på diskussioner i två paneler som avhandlade finansiella system respektive hälsa och omvårdnad. Som bakgrund till diskussionerna i panelerna gavs några övergripande presentationer.

Vad görs i dag?

Tommy Arnesson från Myndighetens för samhällsskydd och beredskap, MSB, reflekterade över ämnet ”Vad som görs i dag?”.

En kartläggning presenterades som nyligen gjorts över nuläget dels beträffande privat-offentlig samverkan hos enskilda aktörer på central nivå och på regional nivå och dels beträffande privat-offentlig samverkan med flera samordnade aktörer inom den finansiella sektorn, telesektorn och olje-/gassektorn.[4] Kartläggningen visade att det behövs en strategi för privat-offentlig samverkan, en gemensam syn på kontakterna och att aktiviteterna måste prioriteras. Infrastrukturområdet bör ha högsta prioritet. Exempel på frågor som behöver utvecklas och konkretiseras är risk- och sårbarhetsanalyser samt identifiering av åtgärder som behöver vidtas. Vidare måste hanteringen av kontinuitetsfrågor utvecklas liksom identifiering av ansvarsfrågor och avtalsfrågor. Slutligen behöver behövliga resurser identifieras samt informationshantering och analysförmågor utvecklas.

Vid en nyligen (2012) genomförd workshop som behandlade privat-offentlig samverkan inom ramen för samverkansområdena i krishanteringssystemet framkom att det är viktigt att finna drivkrafterna för att konkretisera vinna-vinn-situationer. Detta kan ske genom robust upphandling och genom överenskommelse om samverkansformer. Dessutom bör åtgärder vara konkreta och avgränsade. Man bör skapa ”robusthetsmärkta företag” och man bör skaffa kunskap om varandra. Att finna rimliga ekonomiska incitament samt att träffas öga mot öga med regelbundna intervall är också viktigt.

Det är väsentligt att skapa en helhetssyn och en gemensam planering bland de olika aktörerna i de olika samverkansområdena (Teknisk infrastruktur; Farliga ämnen; Ekonomisk säkerhet; Transporter; Skydd, undsättning och vård; Geografiskt områdesansvar). Framgångsfaktorer som identifierades är förankring hos högsta ledningen, tydliga avsiktsförklaringar, formulerade ambitionsnivåer och regler för hur information sprids. Vidare bör mandat tydliggöras, resurser avsättas och kontinuitet i processerna säkras. Man bör sträva efter att få aktörerna att finna ett gemensamt intresse i aktiviteterna och att det gynnar den egna ekonomin. Man bör ha tillgång till kvalificerade tjänster och man bör sträva efter att skapa myndighetsneutrala arbeten samt tydliga rutiner för uppföljning. Slutligen bör man försäkra sig om en utveckling av en samverkansområdesgemensam strategi för privat-offentlig samverkan.

Infrastrukturens beroende av IT-system – Kommunikation Internet

Ingvar Hellquist belyste infrastrukturens beroende av IT-system. Nyttan med de moderna systemen är stor, men de skapar samtidigt en rad beroenden. IT har revolutionerat samhället på 30 år. De senaste 10 åren har datakommunikation eskalerat förloppet. De moderna s k smartphones är datorer och i den version av IP (Internet

Protocol)-adress som främst används i dag, IPV 6 (Internet Protocol Version 6), kan adresserna vara lika många som jordens atomer. Nationella gränser och lagar förändras i cyberrymden. Inom några områden som är särskilt viktiga förändras förutsättningarna snabbt.

Inom t ex den *finansiella sektorn* gör köprobotar aktie- och valutaaffärer på delar av sekunder och inom *hälso- sjukvårdssektorn* har elektroniska journaler och elektroniska recept införts. *Elsektorn*s s k smart grid (smarta ledningsnät) hanterar elnätet via Internet, gammal och ny teknik byggs samman och nya sårbarheter uppstår samtidigt som effektiviteten och lönsamheten förbättras. Papperstidningar ersätts av web-tidningar inom *mediesektorn* och sociala medier ökar dramatiskt. I USA har 40 % av befolkningen ett Facebookkonto. Samtidigt finns det 40 millioner falska konton i omlopp där många används för att ”stjäla” information. *Positionering och synkroniseringsektorn* har utvecklat GPS/telenät/W-lan/G-mailÄ/Android m m som kartlägger såväl vad individen ägnar sig åt som var man är eller har varit. Det så kallade *molnet* med bland annat Dropbox privat är också exempel på ett område som utvecklas snabbt. Kommunens infrastruktur i offentlig sektor är exempel på att privat respektive samhällsviktig information läggs i någon annans databas.

Ett antal sårbarheter kan identifieras såsom sammankoppling av gammal och ny teknik. SCADA (Supervisionary Control and Data Acquision) styr kritiska system, samtidigt som det kopplas ihop med internet. Det skapar osäkerheter genom att intrång nu kan ske i tidigare slutna system. Blixtsnabb och okontrollerad spridning av information kan anses som en annan sårbarhet. Myndighetsverksamhet för medborgarna och näringsverksamhet sker på nätet, vilket ökar sårbarheten i systemen. En förlorad generation har tidigare varit ung, nu räknas tiden från andra hållet.

Den privata sektorn inkluderande näringslivet dominerar innehavet av samhällsviktig infrastruktur och i ökande utsträckning också verksamhet. Telesektorn är den viktigaste sektorn därför att den hanterar elektronisk kommunikation, följd av elsektorn.

Ett antal antagonistiska hot kan identifieras, och de kan rangordnas efter hur vanliga de är och vilken betydelse de har: Industrispionage (stöld av intellectual properties) är vanligast följd av nätkriminalitet, organiserad brottslighet, hackare och hacktivister, terrorister samt cyberangrepp mellan och mot stater.

Några kända exempel på nätverksangrepp är händelserna i Estland 2007, Georgien 2008, Iran 2010, Mellanöstern 2012, och fler är att vänta!

Ett genomgående problem är att detektera farliga angrepp och inse att de har betydelse för samhället och andra aktörer. Det är svårt att se intrången i bruset av ”normala fel” och andra driftstörningar.

Det går att försvara samhället mot nätangrepp, men det kräver nationellt och internationellt samarbete och omfattande samverkan med näringslivet. Byggstenarna är grundläggande säkerhet och regelverk, incidentrapportering, gemensamt myndighetsnät med trafikmätning och normalbildskunskap. Andra väsentliga byggstenar är underrättelser och förvarning, samlad lägesbild, responsförmåga, och inte minst att övningar genomförs med regelbundenhet.

Det finns lösningar på dessa problem. Den s k ansvarsprincipen är dock anpassad till ”långsamma” händelseförlopp och tydliga sektorsansvar, vilket gör att den fungerar dåligt vid IT-angrepp. Området

kräver mer av ”omedelbar beredskapshöjning” med utvidgade mandat i gränsområdena mellan Polisen, Försvarsmakten och Myndigheten för samhällsskydd och beredskap, MSB. För att komma ett steg vidare i att göra området säkrare behövs ekonomiska incitament. Ett sådant är försäkringsbranschen. Om viktiga produkter eller system försäkras och är sårbara startar en process där marknadskrafterna samverkar till säkrare produkter, säkrare system och säkrare kommunikation.

Privat-offentlig samverkan i cybervärlden

Åke Holmgren från MSB gav aspekter på privat-offentlig samverkan i cybervärlden. För att illustrera betydelsen av privat offentlig samverkan beskrev han inledningsvis den stora IT-störning som drabbade Sverige i slutet av november 2011. Helgen den 25-27 november 2011 inträffade ett antal it-händelser. Media rapporterade att ca 350 apotek inte kunde expediera recept på grund av störningar, SBAB:s låneverksamhet påverkades och en finansiell aktör stoppade produktionen av kreditkort, allt detta till följd av störningar i IT-systemen. Ett stort logistikföretag (med kunder i den offentliga sektorn) drabbades av kommunikationsproblem. Nästföljande vecka (2011-11-28–12-04) rapporterade ett antal kommuner störningar i sina IT-system. Bilprovningens IT-stöd var borta på 180 kontrollstationer i landet, och flera andra aktörer drabbades av it-störningar. Sammanfattningsvis drabbades ett 50-tal privata och offentliga aktörer i samhället i olika omfattning. Tillgången till IT-system och -tjänster var borta i dagar eller veckor för vissa verksamheter.

Orsaken till händelsen var ett hårdvarufel i datalagringen i en datahall hos it-driftleverantören Tieto. Det tekniska felet var åtgärdat söndag kväll den 27 november, men återställningen av kundernas information och tjänster tog mycket längre tid. MSB tog tidigt kontakt med

IT-leverantören, samlade in information om konsekvenserna i samhället och samverkade med ett stort antal aktörer i samhället (Kammarkollegiet, Socialstyrelsen, drabbade, etc). Vidare analyserade MSB incidenten, informerade allmänheten och rapporterade regelbundet till regeringen (Försvarsdepartementet). MSB påbörjade också planering för att förebygga liknande händelser samt skrev en offentlig rapport.[5] Sammanfattningsvis kan konstateras att privat-offentlig samverkan är en grundförutsättning för att skapa säkerhet i cybervärlden.

Att bygga privat-offentlig samverkan i cybervärlden förutsätter att parterna har förtroende för varandra och att det finns ett mervärde för alla deltagarna. Vidare är det viktigt att alla bidrar med information, att det sker i en konkurrensneutral (opartiskhet) anda och att det sker kontinuerligt. Staten har en viktig funktion som facilitator och ”svänghjul”. Andra förutsättningar är att det även måste finnas sak-kompetens hos de statliga aktörerna samt att det avsatts nödvändiga resurser, att ledningen är engagerad och att verksamheten är långsiktig.

För privat-offentlig samverkan och informationsdelning om olika aspekter av samhällets informationssäkerhet driver MSB ett antal grupper med samlingsnamnet FIDI (Forum för Informationsdelning avseende Informationssäkerhet).

Exempel på organ för privat-offentlig samverkan i cybervärlden är E-delegationen, Informationssäkerhetsrådet, FIDI-Vård och Omsorg, FIDI-Finans, FIDI-SCADA (Supervisory Control and Data Acquisition),

Mediernas beredskapsråd, E-SCSIE (The European SCADA and Control System Information Exchange), FI-ISAC (Financial Institute for Information Sharing and Analysis), Nationella telesamverkansgruppen (NTSG) och CERT-SE (Computer Emergency Respons Team).

MSB:s informationssäkerhetsråd består av representanter från både offentlig förvaltning och näringsliv. Medlemmarna kommer från Rikspolisstyrelsen, Nordea, Post- och telestyrelsen, Säkerhetspolisen, Försvarets radioanstalt, Vattenfall AB, Stiftelsen för Internetinfrastruktur, Karlstads Universitet, Försvarsmakten, Ericsson, Västra Götalandsregionen, Försvarshögskolan, Riksgälden, Försvarets materielverk, Scania AB. MSB:s överdirektör är ordförande i informationssäkerhetsrådet.

Rådet ska i huvudsak bistå MSB med information om utvecklingstrender inom området informationssäkerhet (skydd av information och säkring av informationssystem) och ge synpunkter på inriktning, prioritering och genomförande av MSB:s arbete inom området. Rådet ska vidare säkra kvalitet och trovärdighet till MSB:s arbete genom att vara rätt sammansatt och i viss utsträckning ha koppling till vitala samhällsfunktioner. Vidare ska rådet bidra till spridning av information om MSB:s arbete med informationssäkerhet i omvärlden. Rådet sammanträder fyra gånger per år, varav ett möte utgörs av en studieresa inom eller utom Sverige.

FIDI-Vård och Omsorg startade 2010 och syftet med forumet är att stödja vård och omsorg genom att utveckla god informationssäkerhet för att på det sättet öka samhällets möjlighet att fungera i både ett normalläge och ett krisläge. Forumet har medlemmar från fem landsting/regioner och kommunerna representeras av KIS (kommunnätverket). Övriga medlemmar är SKL (Sveriges kommuner och landsting), Inera AB, CeHis (Center för eHälsa i samverkan), Socialstyrelsen, Datainspektionen, Läkemedelsverket, Riksarkivet, Apotekens Service AB och Kammarkollegiet.

FIDI-Finans startade 2009 och syftar till att identifiera och initiera åtgärder som kan medverka till att öka säkerheten och minska gemensamma sårbarheter för den finansiella sektorn. Medlemmarna är Bankföreningen, BGC (Bankgirocentralen), Handelsbanken, Euroclear, Finansinspektionen, Nasdaq-OMX Nordnet, Riksbanken, Riksgälden, Skandinaviska Enskilda Banken, Rikspolisstyrelsen, IT-Brottsroteln och Försvarets radioanstalt.

FIDI-SCADA startade 2005 och syftar till att förbättra de deltagande organisationernas informationssäkerhet avseende industriella informations- och styrsystem (SCADA) samt att på lämpligt sätt förmedla valda delar av informationen eller resultat av gruppens arbete till andra aktörer i samhället. Medlemmar i FIDI-SCADA är EON AB, Fortum AB, MSB, Norrvatten, Preem Petroleum AB, AB Storstockholms lokaltrafik (SL), Stockholm Vatten AB, Svenska kraftnät, Säkerhetspolisen, VA Syd AB, Vattenfall AB och Trafikverket.

En betydelsefull del i MSB:s arbete med medieberedskap är den samverkan som sker i Mediernas beredskapsråd. Samarbetet mellan staten och medieföretagen startade redan på femtiotalet. Inom rådet förs en kontinuerlig dialog kring medieföretagens säkerhet, beredskap, krisledningsförmåga och samverkan. Arbetet sker på frivillig basis och en av rådets viktigaste uppgifter är att arbeta för en öppen dialog och ett ömsesidigt förtroende mellan aktörerna. Medlemmarna i Mediernas beredskapsråd är Canal Digital, Com Hem, Radiobranschen, Sveriges Radio Sveriges Television, Teracom, Tidningarnas Tele-

grambyrå, Tidningsutgivarna, TV4, Post- och telestyrelsen, Viasat. Ordförande i rådet är MSB:s generaldirektör.

Sammanfattningsvis är informationsutbyte (Information Exchange) i dag en etablerad modell för privat-offentlig samverkan (POS) internationellt. I Sverige tillämpas denna modell bl a inom ramen för MSB:s FIDI-koncept samt även i Post och Telestyrelsens (PTS) grupp NTSG (nationella telesamverkansgruppen). Grunden för arbetet enligt denna modell är överenskomna mötesregler, informationsdelning vid slutna möten, mekanismer för att dela information (Traffic Light Protocol), personligt deltagande (inga ersättare), personligt förtroende mellan deltagarna, regelbundna möten med närvarokrav och praktisk verksamhet i arbetsgrupper.

Avslutningsvis gavs en kort sammanfattning av MSB:s arbetsuppgifter inom informationssäkerhetsområdet. *Policy och inriktning* är ett område som inbegriper strategi, handlingsplan, föreskrifter och analys. Ett annat område är *medieberedskap* där medie- och etermedieberedskap avhandlas. *Respons- och hanterarfrågor* berör den nationella samverkansfunktionen informationssäkerhet (NOS), nationell responsplan och CERT-SE liksom övningar. *Stöd till verksamheters m fl förebyggande informationssäkerhetsarbete* inbegriper förebyggande informationssäkerhetsarbete, kritisk informationsinfrastruktur (s k SCADA-frågor), kommunikationssäkerhet och e-utveckling. Vidare ingår frågor relaterade till vård- och omsorg, standardisering, medvetandehöjning och risk- och sårbarhetsanalyser liksom förmågebedömning, informationssäkerhet, utbildning och forskning samt utveckling. Se vidare MSB:s hemsida om Informationssäkerhet och förebyggande informationssäkerhet[6] samt CERT.se:s hemsida.[7]

Nya mål – ny rollfördelning mellan privata och offentliga aktörer

Bo Richard Lundgren presenterade aspekter på ”den nya säkerheten”, vilka främst handlar om hur man kan resonera när det gäller hot mot den nationella säkerheten och hur ett sådant resonemang påverkar rollfördelningen mellan ansvariga aktörer. Hit hör frågan om privat-offentlig samverkan inom samhällets krisberedskap.

Till att börja med kan man konstatera att statsmakterna formulerade år 2006[8] en strategi för Sveriges säkerhet. Här formulerades nya *mål* för svensk säkerhet. Dessa är:

- att värna befolkningens liv och hälsa,
- att värna samhällets funktionalitet och
- att värna vår förmåga att upprätthålla våra grundläggande värden såsom demokrati, rättssäkerhet och mänskliga fri- och rättigheter.

En viktig fråga är nu på vilket sätt dessa mål kan äventyras, d v s vad utgör *hot* mot dessa mål. En genomgång av ytterligare riksdagstryck (betänkanden och propositioner) ger vid handen tolv hot som ofta återkommer i dessa sammanhang och som betraktas som hot mot nationell säkerhet. Dessa är:

- väpnat angrepp,
- terrorism,
- organiserad brottslighet,
- avbrott i vitala system och flöden,
- finanskris, massarbetslöshet,
- politisk extremism,
- hot mot demokrati och rättssystem,
- socialt utanförskap,
- hot mot värdegrunder,
- klimatförändringar,
- naturkatastrofer,
- pandemier.

Ett sätt att strukturera dessa hot och försöka analysera vilken typ av säkerhet som hotas erbjuder den statsvetenskapliga s k Köpenhamnsskolan.[9] Här delas den nationella säkerheten in i fem sektorer. Dessa är: Militär säkerhet, politisk säkerhet, ekonomisk säkerhet, social säkerhet och miljösäkerhet. Om vi försöker relatera de ovan uppräknade hoten till såväl mål som säkerhetssektor får man en bild enligt illustrationen i figur 1.

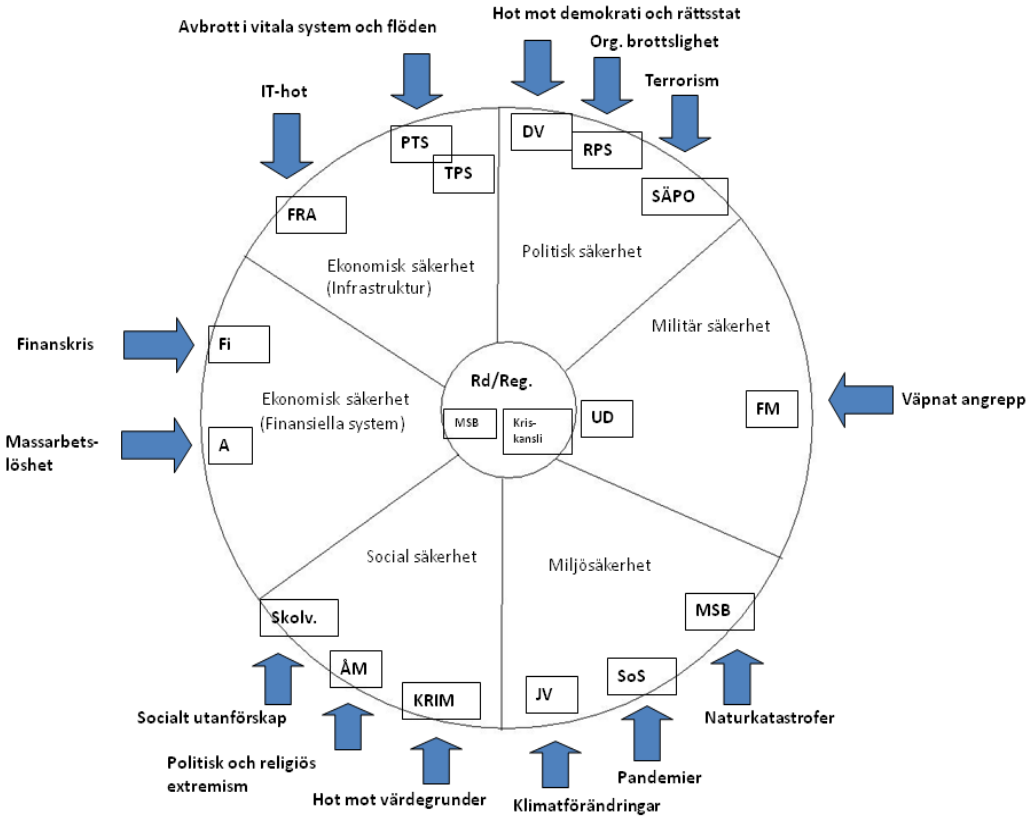
En vidare analys i syfte att identifiera de statliga aktörer som på central nivå är ansvariga för säkerhetsarbetet inom varje sektor illustreras i figur 2. Lägg märke till att sektorn Ekonomisk säkerhet är uppdelad i Infrastruktur och Finansiella system.

Som kan avläsas av figur 2 är ansvaret spritt på ett stort antal statliga aktörer. Ansvaret för att hålla ihop det nationella säkerhetsarbetet vilar ytterst på regeringen, men Myndigheten för samhällsskydd och beredskap, MSB, och kriskansliet i statsrådsberedningen har också viktiga roller för att se till helheten.

Alla vet emellertid – och det är ju detta seminarium bl a till för att belysa – att nationell säkerhet inte skapas av statliga organ på central nivå. Här finns många andra viktiga aktörer både inom den offentliga sektorn och inom den privata. Dessa åter-

Figur 1. Hot mot nationell säkerhet. Mål och säkerhetssektor.

	MILITÄR SÄKERHET	POLITISK SÄKERHET	EKONOMISK SÄKERHET	SOCIAL SÄKERHET	MILJÖ-SÄKERHET
Värna befolkningens liv och hälsa	• Väpnat angrepp				• Klimatförändringar • Naturkatastrofer • Pandemier
Värna samhällets funktionalitet			• Avbrott i vitala system och flöden • Finanskris • Massarbetslöshet		
Värna vår förmåga att upprätthålla grundl. värden		• Politisk extremism • Hot mot demokrati och rättssystemet		• Socialt utanförskap • Politisk och religiös extremism • Hot mot värdegrunder och rättssystem	



Figur 2. Statliga aktörer på central nivå ansvariga för säkerhetsarbetet.

finns också på regional och lokal nivå. På den offentliga sidan har vi kommunala och landstingskommunala organ. På den privata sidan finns näringsliv, organisationer (av ideell, religiös eller politisk karaktär) samt enskilda individer. Det är nu intressant att fundera över hur denna mix av aktörer förhåller sig till de mål som statsmakterna formulerat. I figur 3 görs ett försök att illustrera hur relationen mellan aktörerna kan komma att te sig i förhållande till varje mål.

Illustrationen gör inte anspråk på att utgöra någon exakt vetenskap, men visar att inslaget av privata aktörer är betydande. När det gäller att värna samhällets funktionalitet har näringslivet en vital roll. Att värna grundläggande värden är i huvudsak en uppgift för individer, sammanslutningar och organisationer även om skolan har en viktig roll.

Slutsatsen av detta resonemang är att de nya målen kräver en ny syn på rollfördelningen mellan de aktörer som ansvarar för den nationella säkerheten. Arbetssättet kommer därför också att uppvisa stora skillnader. Förmågan till samverkan mellan privata och offentliga organ blir i framtiden en viktig faktor för att samhället skall kunna hantera hot mot den nationella säkerheten.

Finansiella system

Stärkt krisberedskap i centrala betalningssystemet

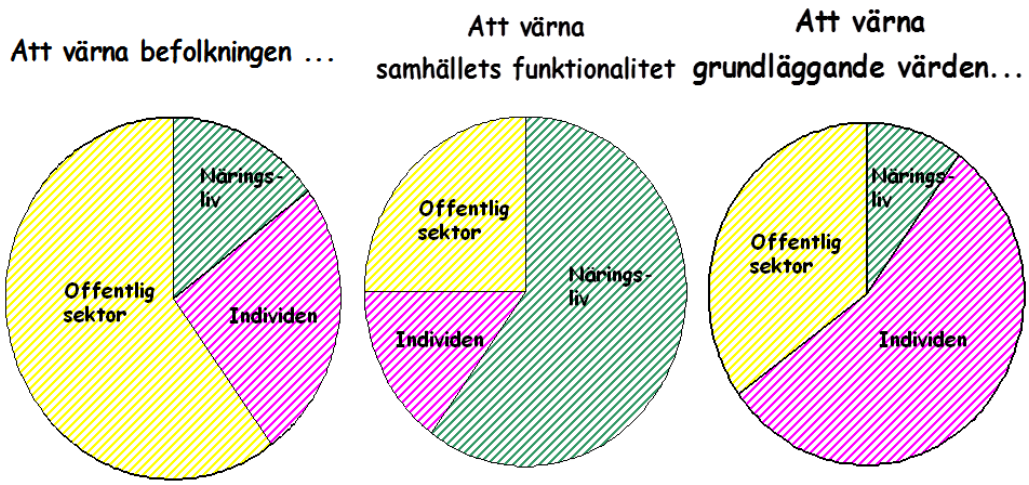
Åke Pettersson sammanfattade den offentliga utredning från 2011 med rubriken *Stärkt krisberedskap i det centrala betalningssystemet*, som han ansvarade för.[10]

Bakgrund till utredningen var Riksrevisionens kritiska rapport 2007, Finansinspektionens och Riksgäldskontorets kommentarer, samverkansövningen SAMÖ 2008 liksom SKRIB-rapporten (Stärkt krisberedskap i betalningssystemen) från 2010.[11]

Direktiven till utredningen var att formulera grundläggande säkerhetsnivåer och kvantitativa (mätbara) mål, föreslå ansvarig samordnande myndighet, utarbeta författningsförslag, ta vara på internationella erfarenheter samt redovisa eventuellt behov av finansiering. Med centrala betalningssystemet avses de delar av det nationella betalningssystemet som har en sådan betydelse att ett bortfall eller allvarlig störning, direkt eller över tid, skulle innebära risk eller fara för samhällets funktionalitet eller samhällets grundläggande värden.

Det centrala betalningssystemet kan sammanfattas bestå främst av RIX-systemet och dess tjugotal deltagare, som utgör den centrala knutpunkten i det svenska betalningssystemet. Aktörer är bl a Riksbanken, de stora bankerna, Bankgirocentralen; Euroclear Sweden AB (VPC-systemet); Nasdaq OMX Derivatives Market och Riksgäldskontoret.

De grundläggande säkerhetskraven är enligt utredningen att målen är definierade, kritiska beroenden identifierade, risk- och sårbarhetsanalyser gjorda, funktionskrav formulerade, och att det finns en kontinuitetsplanering. Målen föreslås vara att alla transaktioner ska avvecklas enligt gällande avtal och lagar, i regel senast under pågående bankdag. Vid störning eller avbrott ska återstart ske inom två timmar. Reservsystemen ska anpassas för detta. Om detta inte är möjligt ska de viktigaste transaktionerna prioriteras. Principer och metoder för att i ett krisläge prioritera de viktigaste transaktionerna ska utvecklas.



Figur 3. Samhällets säkerhet. Relation mellan aktörerna i förhållande till varje mål.

Krisberedskapen kräver en nära privat-offentlig samverkan. Värdet av den Finansiella sektorns privat-offentliga samverkansorgan (FSPOS) betonas.

Riksbanken föreslås få samordningsansvaret. Före en kris ska Riksbanken utforma föreskrifter om grundläggande säkerhetskrav, genomföra risk- och sårbarhetsanalyser för det centrala betalningssystemet och samordna beredskapsplaneringen. Riksbanken ska även utbilda och öva personal, verka för effektiv privat-offentlig samverkan samt lämna information om beredskapsläget till Regeringen och Myndigheten för samhällsskydd och beredskap, MSB. Under en kris ska Riksbanken samordna de åtgärder som vidtas, upprätta lägesrapporter till riksdagen, regeringen och vissa myndigheter samt samordna information som riktas till allmänhet och media.

Beträffande ansvarsfördelningen så ska Riksbankens samordningsansvar omfatta det centrala betalningssystemet, Finansinspektionen ska ha ett fortsatt ansvar för den finansiella sektorn i övrigt. Riksbankens nationella samordningsansvar ska inte omfatta uppgifter som ingår i Finansinspektionens tillsynsansvar.

Utredningen lämnar förslag till en ny fristående lag där en definition av det centrala betalningssystemet inkluderas. Lagens syfte är att förebygga, förbereda för och samordna agerandet vid en kris. Riksbanken ska bemyndigas att meddela föreskrifter, utfärda sanktioner, hantera överklaganden och sekretessfrågor. Smärre ändringar i Riksbankslagen och Sekretesslagen föreslås som komplement.

Utredningen betonar nödvändigheten av systematiskt säkerhetsarbete med stöd av ISO/IEC 27 000. Incidentrapportering ska ske sekretesskyddat till CERT-funktionen. CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter.[12]

Några perspektiv på hot och risker mot distribution av finansiella tjänster

Pär Karlsson från Svenska Bankföreningen gav några perspektiv på hot och risker mot distribution av finansiella tjänster. Ca 60 procent använder internet i sina kontakter med banken, medan ca 27 procent gör det genom ett personligt besök. Andelen personer över 15 år som betalar sina räkningar via internetbank har ökat från 9 procent 1999 till 72 procent 2011. I de yngre åldersgrupperna är det upp till 99 procent som betalar sina räkningar via internet. Samtidigt har andelen som brevledes betalar med bank- och postgiro minskat från nästan 79 procent 1999 till 15 procent 2011. Upp till 80 procent av svenskarna använder nätet för köp av artiklar och upp nästan 90 procent för bankärenden. Upp till ca 65 procent av svenskarna litar mycket eller ganska mycket på nätet när de t ex handlar och gör bankärenden. Antal transaktioner som görs med användandet av kortbetalning har ökat kraftig de senaste åren från drygt 200 miljoner transaktioner 1999 till drygt 1600 miljoner transaktioner 2010.

Definition av operativ risk är risken för förluster till följd av icke ändamålsenliga eller misslyckade processer, mänskliga fel, felaktiga system eller externa händelser och definitionen inkluderar legal risk.

Tendenser som på senare tid iakttagits beträffande hotbilder är att bankrån har en tendens att minska kraftigt, medan hot mot personal ökar något. Angrepp mot automater är konstant, bedrägerier mot in-

ternetbanker ökar något, kortbedrägerier minskar men det sker en ökning av ID relaterade hot kopplade till IT-system. Det förekommer fler anmälningar beträffande penningtvätt och en viss ökning av insiderrelaterade brott. För dataintrång och informationsförlust sker inte någon ökning, men hotbilden har ändrats. Hotbilden har ändrats t ex som en följd av allt mer komplexa IT-miljöer med ökat inslag av outsourcing. Risken för informationsförluster per se har dock inte ökat.

Det finns många olika IT-relaterade hot som t ex skadlig kod, intrång, ”man i mitten”, social engineering och DoS (Denial of Service). Andra exempel är DNS (Domane Name System) attacker inkluderande s k pharming och SPAM som inkluderar s k phishing och popups. Ytterligare exempel är attacker mot fysiskt nät och mot trådlöst nät liksom obehörig utrustning.

I en ”*man i mitten*” (Man-In-The-Middle – MITM) attack har angriparen tagit sig in på förbindelsen mellan två parter och kan avlyssna och/eller förvanska den information som skickas mellan parterna. Inom internetbankverksamhet är det vanligt att MITM används i samband med phishing där kunden luras till en falsk banksida varifrån bedragaren kan utföra bankärenden i kundens namn.

SPAM – oönskad e-post kan användas för att utföra s k *phishing*, vilket är en metod att lura innehavare till bankkonton och andra elektroniska resurser att delge kreditkortsnummer, lösenord eller annan känslig information. *Pop-up fönster* är ett fenomen då ett fönster visas framför andra fönster i webbläsaren, ofta utan att användaren själv gjort något särskilt för att fönstret ska visas. Denna metod kan användas för att utföra phishing.

DoS (Denial of Service) attack är en tillgänglighetsattack och/eller en [över]belastningsattack, som innebär att en specifik aktivitet förhindrar behöriga att få åtkomst till resurser i ett IT-system eller att tidskritisk verksamhet fördröjs.

Med *DNS-attack* (Domane Name System) menas angrepp som syftar till att göra obehöriga ändringar i namnuppslagningsfunktionen på Internet och i datorer. Detta kan göras genom att man manipulerar DNS-databaser eller manipulerar lokal namnuppslagningsfiler (t ex local hosts). Överbelastningsattacker (DoS) mot DNS-servrar och varumärkesintrång genom domänregistering omfattas inte av begreppet DNS-attack. *Pharming* är ett sätt att lura användare att lämna ifrån sig användarnamn, lösenord, kontokortsnummer etc. Det är med andra ord en typ av phishing. Pharming innebär att man påverkar DNS funktionaliteten på ett sådant sätt att användaren får en annan IP-adress än den riktiga.

Den finansiella sektorns privat-offentliga samverkansgrupp (FSPOS) har visionen att samhällsviktiga finansiella tjänster alltid ska fungera. Verksamhetsidén är att stärka den finansiella infrastrukturen genom att samverka, öva, kartlägga och dela information och på så sätt värna sektorn och samhället. Verksamheten bygger på frivilligt arbete bland deltagarna och bedrivs för närvarande i fem arbetsgrupper: betalningsförmedling, information, kritisk infrastruktur, övning och grundläggande säkerhetsnivåer (GSN).

De viktigaste aktörerna i FSPOS är bankerna, försäkringsbolagen, clearingorganisationerna, Riksbanken, Riksgälden, Försäkringskassan och Finansinspektionen

Ett antal s k nulägesanalyser har genomförts. En nulägesanalys beträffande *elsystemen* visar att det svenska elsystemet är byggt för hög driftsäkerhet och är i sin helhet generellt robust och tåligt. Det finns

dock hot och sårbarheter i elförsörjningen såsom tekniska fel i viktiga anläggningar (t ex driftcentraler), långvariga störningar i vitala system för elektronisk kommunikation, intrång eller haveri av driftstödsystem.

Nulägesanalysen för *drivmedel* visade att den finansiella sektorn är främst beroende av drivmedel i händelse av ett större elavbrott, då reservkraft behöver användas. Dagens beredskap att försörja samhället med bränsle vid ett mer omfattande elavbrott är bristfällig. De största sårbarheterna finns i den begränsade tillgången till transporter av drivmedel och bristen på chaufförer samt i prioritetsproblem vid en bristsituation.

För *elektronisk kommunikation* visade nulägesanalysen att stabila nät är viktiga för att den mängd information som transporteras ska levereras med hög säkerhet och precision. Nätet för elektronisk kommunikation är omfattande och det finns en mängd redundanta förbindelser, vilket betyder att man snabbt kan leda om trafik vid ett kabelbrott. Det finns möjlighet att avtala om avbrottsfri leverans av elektronisk kommunikation, men ibland saknas dock beställarkompetens.

Kommunalteknisk försörjning omfattar bl.a. fjärrvärmeleverans, vattenförsörjning och avloppshantering. Nulägesanalysen för *kommunalteknisk försörjning* visade att ledningsnätet för vatten är omfattande och leveransen av vatten kan oftast ledas om vid ett avbrott. De största riskerna med den kommunaltekniska försörjningen är problem med de olika ledningsnäten eller hot om sabotage och skadegörelse. Slutsatserna av nulägesanalyserna presenteras i figur 4.

Hälsa och omvårdnad

Stockholms läns landsting

Håkan Lindberg från Stockholms läns landsting (SLL) påpekade att lärandet från inträffade händelser är väsentligt och att det finns ett utmärkt system för detta genom Kamedo-verksamheten (Katastrofmedicinska observatörsstudier), som bedrivs i Socialstyrelsens regi. Akutsjukvården inom SLL bedrivs i olika driftformer, mer än 50 % av vårdcentralerna drivs i privat regi, ambulanssjukvården drivs huvudsakligen av privata entreprenörer och dirigering av ambulanser sker av SOS-Alarm, som är en från landstinget fristående organisation. En allt större del av psykiatrin privatiseras. Sjukvården är helt beroende av infrastukturen och det mesta av logistiken beträffande läkemedel och sjukvårdsutrustning sker inom ramen för just-in-time-principen.

Den allt mer strikta tillämpningen av den s k ansvarsprincipen innebär att de statliga bidragen för utbildning och övning upphört liksom bidragen för utrustning m m inom CBRN (Chemical, Biological, Radio-Nuclear)-områdena, vilket är stora utmaningar för landstingen. Vidare har de statliga bidragen för det robusta sjukhuset minskat betydligt.

Den katastrofmedicinska beredskapen innefattar såväl somatiskt som psykosocialt omhändertagande. Den ökade privatiseringen av psykiatrin ställer till stora organisatoriska problem inom det psyko-sociala omhändertagandet i samband med krissituationer.

Landstinget har inkluderat krisberedskapsaspekten i alla avtal med samtliga vårdgivare, i vissa fall har särskilda tilläggsavtal tecknats med vårdgivare och

Elförsörjning	Slutsatser
Elförsörjning	• Sektorn bör ställa krav på hög leveranssäkerhet. • Aktörerna bör säkra upp med egen reservkraft. • Arbeta för att den finansiella sektorn inkluderas som en prioriterad elanvändare.
Elektronisk kommunikation	• Det finns redundanta lösningar. • Finansiella sektorns kravställning behöver bli bättre. • Behov av information och utbildning inom finansiella sektorn.
Kommunalteknisk Försörjning	• Hög inbyggd redundans i systemen. • Största sårbarheterna finns i ledningsnäten (avgrävningar, skadegörelse/sabotage) och produktions-/leveransproblem på grund av större elavbrott • Finns extra redundanta lösningar som kan implementeras om särskilt behov, t.ex. av vattenförsörjning.
Drivmedelsförsörjning	• I en elavbrottssituation kan drivmedelsförsörjning bli en kritisk faktor. • Finns utmaningar kopplat till leveransen: – Flaskhals vid depåerna – Transportproblematik – Prioriteringsproblematik

Figur 4. Slutsatser av nulägesanalyserna inom finansiella sektorn.

med andra aktörer som levererar varor och tjänster.

För framtiden ser landstinget det som väsentligt att system säkras som garanterar att utbildnings- och övningsverksamheten kan hållas på minst samma nivå som hittills. Utbildning och övning är nyckeln till framgång. Det är viktigt att det sker en regional och nationell likriktning som garanterar samordning inom krisberedskapsområdet. Samverkan genom s k nätverkande är kritiskt liksom att forskning och utveckling inom krisberedskapen och det katastrofmedicinska området fortsätter att utvecklas. Det finns ett behov av att tolka vad den s k ansvarsprincipen egentligen innebär för krisberedskapen och den katastrofmedicinska beredskapen inom landstingsvärlden.

Capio S:t Göran

Från Capio S:t Göran deltog Måns Belfrage. Capio S:t Göran (CStG) har sedan länge deltagit i landstingets beredskaps- och katastrofplanering. CStG är ett privatägt akutsjukhus med avtal med Stockholms läns landsting (SLL). Ca 65 % av patientkontakter är akuta, med ca 75 000 akutbesök årligen. Finansieringen utgörs till ca 99,5 % av offentliga medel.

CStG deltar i beredskapssamordningen som alla andra akutsjukhus inom SLL bl a genom i av landstinget anordnade övningar. Vid sjukhuset finns t ex en saneringsstation i händelse av kemiska och radioaktiva händelser. Utveckling av kursverksamheten inom det katastrofmedicinska området liksom forskning med bl a utveckling av kvalitetsindikatorer särskilt beträffande

sjukvårdsledning vid katastrofer sker inom ramen för sjukhusets verksamhet. Det finns en katastrofledningsgrupp, specifik ledningscentral och en katastrofkommitté vid sjukhuset. Risk- och sårbarhetsanalyser görs regelbundet och CStG deltar även i SLL:s katastrofmedicinska råd.

Det finns vissa svårigheter att vara s k privat aktör. Förutom huvudavtalet med SLL finns ett eget underavtal med REK (Regionala enheten för kris- och katastrofberedskap). Vad som dock inte är reglerat är den s k psykologiska katastrofledningen (PKL).

Driften av kris- och katastrofberedkapen är dock underfinansierad, och samarbetet med kommunerna och stadsdelnämnderna behöver utvecklas. Reglering saknas beträffande fastighetsägaren Locums roll och ansvar för att garantera det robusta sjukhuset och reglering saknas med underleverantörer. Exempelvis är det oklart hur bl a gasleveranser ska garanteras under icke kontorstid liksom elförsörjningen till pumpstationer för att garantera vattenförsörjningen.

Inför framtiden är det oklart hur den ökade specialiseringen kommer att påverka utvecklingen och hur beredskapsaspekten ska regleras.

Sammanfattningsvis kan det konstateras att det är viktigt att det finns tydliga avtal och att utbildnings- och övningsverksamheten får det ekonomiska stöd som behövs. Det är väsentligt att upprätthålla motivationen i organisationen för en kris-och katastrofmedicinsk beredskap. Samverkan mellan olika myndigheter och privata aktörer behöver utvecklas.

LIF – Branschföreningen för de forskande läkemedelsföretagen

Anita Finne-Grahnén från LIF presenterade aspekter från sin organisation. LIF är ”Branschföreningen för forskande läkemedelsföretag som utvecklar och bedriver forskning på läkemedel”. LIF har ca 80 medlemmar med ca totalt 13 000 anställda, som tillsammans står för ca 80 % av alla läkemedel som säljs i Sverige. Företagen lägger årligen 13 miljarder svenska kronor på Forskning och Utveckling.

LIFs mission är att i partnerskap med regering, landsting, statliga verk och centrala hälsovårdsaktörer förbättra livskvaliteten för alla patienter i Sverige. Detta gör man genom att medverka i utvecklingen av det svenska sjukvårdssystemet och genom att verka för utvecklingen av, tillgång till, samt korrekt användning av innovativa läkemedel och vacciner.

LIF fullföljer sin mission genom påverkansarbete i för den forskande läkemedelsindustrin viktiga policyfrågor. LIF arbetar dessutom för att stödja medlemmarna så att företagen kan uppnå sina respektive affärsmål.

LIF har arbetet med beredskapsfrågor under lång tid. T ex deltog LIF i SOLK (Socialstyrelsens kommitté för läkemedelsfrågor vid kris eller beredskap), som dock upphörde 2008. I denna verksamhet deltog representanter från apotek, Socialstyrelsen, Försvarsmakten, Oriola, Tamro, LIF, Läkemedelsverket samt några läkemedelsföretag. Syftet med den verksamheten hade flera dimensioner. Omvärldsbevakning, d v s att man delgav sin syn på vad som händer i omvärlden, var en viktig aktivitet. Lägesrapportering genom att man informerade varandra om vad som var på gång inom respektive arbetsområde var ett annat område som avhandlades liksom att man

gav information om slutförda eller kommande projekt. Probleminventering genom att man informerade om sådant som kunde orsaka problem inom läkemedelsområdet, så att eventuella nödvändiga åtgärder kunde vidtas, ingick också i SOLK-verksamheten. SOLK verkade också som ett diskussionsforum för olika frågeställningar kring läkemedel och beredskapsaspekten och verkade som en rådgivare/expertpanel åt Socialstyrelsen. LIF beklagar att denna mycket viktiga verksamhet upphörde.

Erfarenheter från en pandemiövning 2006 tillsammans med ett antal aktörer var att ett antal områden identifierades där prioriteringarna och ansvarsförhållanden måste klargöras såsom behöver lagerhållningen ökas? vem gör listan? vilken myndighet har befogenhet att fatta snabba ransoneringsbeslut? finns ersättning för IT-system?

Socialstyrelsens beredskapsplan för läkemedel, som reviderades 2012, inbegriper tillgång och tillgänglighet av beredskapsläkemedel och information om vilka läkemedel som är inköpta. Sjukvårdshuvudmännen ansvarar för kostnaderna för beredskapsläkemedlen. Det finns dock fortfarande några frågeställningar som behöver klarläggas. Hit hör beredskapslagrets storlek och om och hur ransonering av läkemedel ska göras. Värdefull vägledning kan man få genom att studera hur t ex grannländerna (t ex Finland och Norge) har löst dessa frågor.

Avslutande reflexioner

Helena Lindberg, GD för Myndigheten för samhällsskydd och beredskap och ledamot av KKrVA, gav avslutningsvis sina reflexioner över seminariet. Dagens ämne anknyter väl till temat för hennes inträdesanförande i KKrVA förra året; ”Från skyddsrum och beredskapslager till samhällsskydd och globala flöden”.[13] Där betonades att det finns anledning att återuppväcka det goda privat-offentliga samarbete som fanns inom totalförsvarets ram – bl a idén bakom de s k K-företagen och kanske också det systematiska arbete som bedrevs utifrån krigsviktiga civila funktioner. På den tiden gällde det beredskap inför krigets villkor. Dagens utmaning är att engagera några som vi kan kalla ”Kris-företag” i detta arbete. Då gällde det tillverkning och lagring av krigsviktiga varor och transporter för försvarsmaktens behov. Nu handlar det framförallt om att engagera tjänsteproducerande företag – t ex inom finansvärlden eller inom hälsa och omvårdnad – som detta seminarium främst handlat om.

Idag står också medborgaren och dennes behov av att ha tillgång till grundläggande samhällsviktiga funktioner mycket tydligare i centrum. Samhällskydd och -beredskap utgår ifrån individen och sträcker sig över hela samhället – ”whole-of-society”. Och den kristålighet som byggs upp måste förhålla sig till en högst föränderlig värld – med ett brett och skiftande hot- och riskspektrum.

Det har påpekats att näringslivet kan ses som något skyddsvärt eller till och med som en måltavla eller ett offer för andras aktioner. Det finns sådana exempel från Danmark i närtid. Näringslivet kan dessutom ses både som en del av problemet för samhällsskydd och beredskap och en del av den gemensamma lösningen. En hel del sker redan, som tidigare påpekats. MSB driver olika projekt och har olika samverkansformer med näringslivet. Former och effekter varierar samtidigt en hel del mellan samhällssektorer.

De goda exempel vi har måste spridas över sektorsgränser, och vi behöver samti-

digt ännu mer av internationell samverkan kring denna fråga. Det är faktiskt inte bara Sverige som sliter med att fylla begreppet PPP (Public-Private Partnership) med mer konkretion än ofta rätt luddiga formuleringar om partnerskap baserade på ”win-win” o s v. En diskussion pågår för närvarande runt om i Europa och även på andra sidan Atlanten, kring hur man kan bära sig åt för att få till stånd ett mer kontinuerligt och närmare samarbete med näringslivet kring frågor om kristålighet. Ett av de länder där dessa frågor diskuteras intensivt är Nederländerna. Just därför arrangerar MSB, i samverkan med sin motsvarighet i Nederländerna, en gemensam högnivåkonferens i februari 2014 i Haag på detta tema. Ansvarig EU-kommissionär medverkar i programmet.

Ett annat inspel för det fortsatta arbetet kan hämtas från MSB:s arbete i en arbetsgrupp inom OECD kring ”Corporate Governance for Process Safety” som i somras resulterade i en internationell handbok för företagsledare inom kemisk och petrokemisk industri. Skriften presenterades i Paris och skall användas internationellt för att stimulera en bättre säkerhetskultur bland de högsta cheferna inom denna mycket känsliga industrisektor.

Utan ett tydligt engagemang från högsta ledningen i dessa frågor är det svårt att nå bra resultat. Vi minns hur British Petroleums ledning brottades med svåra frågor sommaren 2010 efter olyckan i mexikanska Gulfen. Sådant vill vi helst slippa i vårt närområde. Med stolthet konstateras att MSB:s experter har varit med och utformat denna Guide, som förhoppningsvis kommer till konkret användning även bland svenska företagsledare. Ett annat arbete med en tydlig koppling till näringslivet och inte minst till den privatägda infrastrukturen handlar om solstormar. MSB:s omvärldsbevakning omfattar numera även rymden och skeendet på solskorpan. Effekterna av det som händer där kan vara förödande för olika kritiska samhällsfunktioner.

Ett antal expertmöten arrangeras kring denna problematik och inte minst deltagare från näringslivet har visat ett stort intresse – säkert av egenintresse. MSB arbetar nu fram rutiner för förvarningskonferenser kring rymdväder, liknande de vi redan har etablerat för vanligt väder. I detta arbete behöver vi ett starkt engagemang från näringslivet som står för teknikkunnandet och mycket av berörd materiel på marken och i rymden. MSB gör naturligtvis en hel del tillsammans med näringslivet även på det viktiga och växande informationssäkerhetsområdet.

”Resilience” är ett samlande begrepp som kan användas för att markera vad man vill åstadkomma med en helhetssyn före, under och efter diverse svåra händelser. Översatt betyder resilience snabb återhämtningsförmåga. Det finns en omfattande vetenskaplig diskussion om detta begrepp och dess tillämplighet på samhällsfrågor och särskilt på samhällssäkerhet. Klart är att det rymmer en mycket tydlig dimension av privat-offentlig samverkan. Rubriken för dagens möte använder begreppet ”kristålighet”. Man skulle kunna ha använt begreppet ”*resiliens*” i stället.

De rekommendationer och förslag som detta seminarium utmynnar i kommer att diskuteras vidare inom MSB bland berörda experter. Några kan kanske även lanseras i olika internationella sammanhang framöver. Alla är överens om att Något behöver göras snarast för att stärka samverkan mellan det offentliga och det privata inom vårt arbetsområde. De svåra frågorna kvarstår emellertid om vad vi Kan och vad

vi Bör göra och hur detta kan Genomföras hemma och internationellt.

Slutsatser och rekommendationer

Slutsatserna och rekommendationerna nedan baserar sig på de diskussioner som fördes främst i de två panelerna.

Ytterligare reglering behövs

- Ytterligare regleringar för privat-offentlig samverkan behövs, regleringar bör genomföras i förväg och man bör inte vänta på att något händer.
- Det är viktigt att identifiera hur motivation kan vidmakthållas i organisationen när inget händer och att systematisk utbildnings- och övningsverksamhet bedrivs.
- Nya institutioner har en tendens att hamna utanför, och därför måste det finas system för att få med dem så snart som möjligt. En framgångsfaktor kan vara att analysera kundernas redundans och föra en dialog med dem om en lägsta acceptabel nivå.
- Plattformar måste byggas, förtroendefrågor och mervärdesaspekter måste belysas.
- Statens roll som initiativtagare och samordnare är viktig.
- Beträffande genomförande måste klara mål finnas och kontrollmöjligheter bejakas.
- Det som behöver göras måste genomföras och man bör ta reda på om rätt saker görs och vad som behöver mätas för att få veta det.

Statliga medel har stor betydelse

- Statliga medel för att stimulera utbildning och övningar är av vital betydelse.
- Nationell likriktning och samordning är viktig liksom forskning och utveckling.
- Hur ska ansvarsprincipen tolkas – som det är nu trycks ansvaret ner i organisationerna till det lokala planet, som då också får ett ekonomiskt ansvar som det inte alltid finns utrymme för.

Tydliga avtal behövs

- Tydliga avtal behövs och regleringar där beredskapsaspekten finns med.
- Det behövs bättre beslutsstöd för beslutsfattare på det regionala/lokala planet och det är viktigt att identifiera vad som är gränssättande.
- Tillverkares och distributörers ansvar behöver förtydligas.
- De offentliga myndigheterna behöver utveckla sin förmåga att upphandla tjänster och produkter inom krisberedskapsområdet.

Sammanfattning

Hur förbättra privat-offentlig samverkan?

Några slutsatser och rekommendationer vid seminariet var att ansvaret för krishantering beror mycket på problemets dimensioner. Alla problem går inte att planera bort ty det oväntade kommer alltid att hända. När verksamheter privatiseras eller konkurrensutsätts måste särskild omsorg ägnas åt att de krismarginaler som tidigare fanns inte tappas bort i övergången.

Ytterligare reglering behövs

Ytterligare regleringar för privat-offentlig samverkan behövs, regleringar bör genomföras i förväg, och man bör inte vänta på att något händer. Det är viktigt att man identifierar hur motivation kan vidmakthållas i organisationen, när inget händer, och att systematisk utbildnings- och övningsverksamhet bedrivs. Nya institutioner har en tendens att hamna utanför, och därför måste system finnas för att få med dem så snart som möjligt. En framgångsfaktor kan vara att analysera kundernas redundans och föra en dialog med dem om en lägsta acceptabel nivå. Plattformar måste byggas, förtroendefrågor och mervärdesaspekter måste belysas. Statens roll som initiativtagare och samordnare är viktig. Beträffande genomförande måste klara mål finnas och kontrollmöjligheter bejakas. Det som behöver göras måste genomföras och man bör ta reda på om rätt saker görs och vad som behöver mätas för att få veta det.

Statliga medel har stor betydelse

Statliga medel för att stimulera utbildning och övningar är av vital betydelse. Nationell likriktning och samordning är viktiga liksom forskning och utveckling. Hur ska ansvarsprincipen tolkas? Som det är nu trycks ansvaret ner i organisationerna till det lokala planet, som då också får ett ekonomiskt ansvar, som det inte alltid finns utrymme för.

Tydliga avtal behövs

Tydliga avtal behövs och regleringar där beredskapsaspekten finns med. Det behövs bättre beslutsstöd för beslutsfattare på det regionala/lokala planet och det är viktigt att man identifierar vad som är gränssättande. Tillverkares och distributörers ansvar behöver förtydligas. De offentliga myndigheterna behöver utveckla sin förmåga att upphandla tjänster och produkter inom krisberedskapsområdet.

Författarna är Marie Hafström, jur kand, f d generaldirektör och ordförande i avd V, Per Kulling, med lic, f d medicinalråd, Bo Richard Lundgren, jur kand, f d chef för Institutet för högre totalförsvarsutbildning (IHT), Försvarshögskolan, Bengt Sundelius, professor i statsvetenskap vid Försvarshögskolan, strategisk rådgivare vid MSB, samt Leif Vindevåg, pol mag, f d bankdirektör; samtliga ledamöter av KKrVA.

Noter

1. Kulling, Per; Ericson, Sture; Lindgren, Karin och Pärnerteg, Folke: ”Förmåga till ledning och ledarskap vid civil krishantering”, *KKrVAHT* , 4. häftet 2006, s 3-26. (Ability of management and leadership in civil crises, *The Royal Swedish Academy of War Sciences. Proceedings and Journal,* No. 4 2006, pp 3-26, English summary). *http://www.kkrva.se/wp-content/uploads/Artiklar/064/kkrvaht_4_2006_1.pdf* (2012-11-23).
2. Kulling, Per; Hall, Bo G; Jarlsvik, Helén; Lundgren, Bo Richard; Mattsson, Therese; Pärnerteg, Folke och Wisén, Jan: ”Fungerar samverkan i krishantering? En studie med fokus på hälsosektorn”, *KKrVAHT*, 4. häftet 2011, s 39-58. (Does collaboration in crisis management work well? A study focusing on the health sector, *The Royal Swedish Academy of War Sciences. Proceedings and Journal*, No. 4 2011, pp. 39-58, English summary)
3. Regeringen: ”Budgetproposition för 2013 (2012/13:1) Utgiftsområde 6”, s 101 f, *http://www.regeringen.se/sb/d/15677/a/199189* (2012-11-23).
4. Myndigheten för Samhällsskydd och Beredskap, MSB: *Kartläggning av privat-offentlig samverkan inom krisberedskapen*, konsultrapport utarbetad av UW Konsult AB, 2011-11-23, (D nr 2011-2330).
5. Myndigheten för Samhällssäkerhet och beredskap, MSB: ”Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter. En studie av konsekvenserna i samhället efter driftstörningen hos Tieto i november 2011”, *https://www.msb.se/RibData/Filer/pdf/26170.pdf* (2012-11-23).
6. Myndigheten för samhällsskydd och beredskap, MSB: ”Förebyggande informationssäkerhet.” *https://www.msb.se/sv/Forebyggande/Informationssakerhet/* (2012-11-23); Myndigheten för samhällsskydd och beredskap, MSB: ”Informationssäkerhet.” *http://www.informationssakerhet.se/* (2012-11-23).
7. Cert.se hemsida, *www.cert.se*
8. Regeringen: ”En strategi för Sveriges säkerhet”, (Ds 2006:1), *http://www.regeringen.se/sb/d/306/a/56226* (2012-11-23).
9. Buzan, Barry; Ole Waever och de Wilde, Jaap: *Security: A new Framework for Analysis*, Lynne Rienner Publishers, Boulder CO 1997.
10. Regeringen: ”Stärkt krisberedskap i det centrala betalningssystemet”, (SOU 2011:78) *http://www.regeringen.se/sb/d/108/a/181656* (2012-11-23).
11. Riksrevisionen: *Krisberedskap i betalningssystemet* (RiR 2007:28) *http://www.riksrevisionen.se/sv/rapporter/Rapporter/EFF/2007/Krisberedskap-i-betalningssystemet-/* (2012-11-23); Krisberedskapsmyndigheten. ”Utvärdering av Samverkansövning 2008”, *https://www.msb.se/en/Kunskapsbank/Utvarderingar--strategiska-analyser/Utvardering-av-ovningar/* (2012-11-23); Finansinspektionen: ”SKRIB (Stärkt krisberedskap i betalningssystemen)”, Fi 2010/1619.
12. Op cit, CERT.se, se not 7.
13. Lindberg Helena: ”Från skyddsrum och beredskapslager till samhällsskydd och globala flöden”, *KKrVAHT* , 4. häftet 2011, s 69-81. *http://www.kkrva.se/wp-content/uploads/Artiklar/114/kkrvaht_4_2011_10.pdf* (2012-11-23).