



Myndigheten för  
samhällsskydd  
och beredskap

# Metoder för konsekvens- analys på samhällsnivå



MSB:s kontaktpersoner:

Tobias Rosander, 010-240 54 82

Anna Rinne, 010-240 54 15

Publikationsnummer MSB906 - september 2015

ISBN 978-91-7383-595-4

# Konsekvensanalys på samhällsnivå

*Jonas Johansson*

*Henrik Hassel*

*Kurt Petersen*

*Björn Arvidsson*

---

LUCRAM

Lunds universitets centrum för riskanalys och riskhantering

Lunds universitet

Rapport 3002, Lund 2015

# Konsekvensanalys på samhällsnivå

Jonas Johansson

Henrik Hassel

Kurt Petersen

Björn Arvidsson

**Rapport 3002**

**ISRN: LUTVDG/TVRH--3002—SE**

**Antal sidor: 72**

**Sökord:** Konsekvensanalys, Samhällsnivå, Skydd av samhällsviktig verksamhet, SSV, Critical Infrastructure Protection, CIP, Kritisk infrastruktur, Beroenden, Handlingsplan, Kunskapsöversikt, Samhällsfunktioner, Infrastruktur, Sektorer.

**Abstract:** The Swedish Civil Contingencies Agency has during the last years actively addressed the area of Critical Infrastructure Protection (CIP) (Sv. Skydd av samhällsviktig verksamhet) and have in a plan of action pointed out one critical area for which methods and tools should be developed until the year 2020, namely consequence analysis from a societal perspective (Sv. Konsekvensanalys på samhällsnivå). The purpose of this report is to give a foundation and point out important aspects for such work. To gain insights, three different activities were carried out: 1) a review of public actors' risk- and vulnerability analyses to get an idea of current status with respect to dependency analyses and consequence analysis from a societal perspective, 2) interviews with international bodies (DHS/NISAC, TNO, and JRC) on how they have addressed CIP, focused towards modelling and analysis of cross-sectorial dependencies, and 3) a workshop with Swedish local, regional, and national public actors to gain additional insights and feedback on the conclusions from the report. Based on conclusions from these activities, an initial framework is suggested and important aspects for the development of methods and tools within this area are highlighted.

---

LUCRAM

Lunds universitets centrum för  
riskanalys och riskhantering

Lunds universitet

Box 118

221 00 Lund

<http://www.lucram.lu.se>

---

LUCRAM

Lund University Centre for  
Risk Analysis and Management

Lund University

P.O. Box 118

SE-221 00 Lund

Sweden

<http://www.lucram.lu.se>

# Innehåll

1	Introduktion.....	1
1.1	Bakgrund .....	1
1.2	Syfte.....	1
1.3	Konsekvensanalys på samhällsnivå (KAS) .....	2
1.4	Avgränsningar .....	3
1.5	Bakomliggande arbete .....	3
1.6	Medverkande .....	3
2	Analys av risk- och sårbarhetsanalyser .....	5
2.1	Metod och material .....	5
2.2	Resultat .....	7
2.3	Aggregering av individuella beroenden .....	15
2.4	Diskussion och slutsatser .....	20
3	Intervjustudier .....	23
3.1	TNO, Holland.....	23
3.2	JRC, EU .....	26
3.3	DHS samt NISAC, USA.....	27
3.4	Diskussion och slutsatser .....	36
4	Avstämning av tankar för utveckling av KAS .....	39
5	Utgångspunkter för utveckling av KAS .....	43
6	Referenser .....	47
Bilaga 1	Samhällssektorer och samhällsfunktioner .....	i
Bilaga 2	Beroendematriser .....	iii
Bilaga 3	Intervjumaterial .....	v



# 1 Introduktion

## 1.1 Bakgrund

Myndigheten för Samhällskydd och Beredskap (MSB) har under de senaste åren arbetat aktivt med utveckling av området Skydd av samhällsviktig verksamhet, vilket avser ”åtgärder och aktiviteter som behöver vidtas för att säkerställa funktionalitet och kontinuitet hos samhällsviktig verksamhet och därmed samhället i stort” (MSB, 2013, sid. 12). I Handlingsplanen för Skydd av samhällsviktig verksamhet, som utarbetats av MSB och som syftar till ”att skapa ett resilient samhälle med en förbättrad förmåga i samhällsviktig verksamhet att motstå och återhämta sig från allvarliga störningar” (Ibid., sid. 9), är en prioriterad aktivitet för perioden 2014-2020 att utveckla metoder och verktyg för konsekvensanalys på samhällsnivå (KAS). Denna aktivitet är en av flera aktiviteter som ingår i arbetet med att implementera ett systematiskt säkerhetsarbete inom samhällsviktig verksamhet på lokal, regional och nationell nivå. Denna rapport, som är slutredovisningen av ett uppdrag från MSB till Lunds universitets Centrum för Riskanalys och Riskhantering (LUCRAM), kan ses som ett vägledande underlag till utvecklingen av nya metoder och verktyg för konsekvensanalys på samhällsnivå.

I Handlingsplanen för skydd av samhällsviktig verksamhet anger MSB att det ”krävs en utvecklad förmåga och kunskap om vilka konsekvenser en störning eller ett avbrott kan orsaka på olika systemnivåer” (Ibid., sid. 28). Till exempel ska sådan förmåga och kunskap kunna användas för att identifiera effektivare åtgärder i ett förebyggande skede och bidra med kunskap om troliga händelseutvecklingar under en kris, vilka i sin tur kan utgöra ingångsvärden för samverkansarbete, t.ex. förbättrad privat-offentlig samverkan.

Begreppet Konsekvensanalys på Samhällsnivå (KAS) används i detta uppdrag som en typ av konsekvensanalys som tar hänsyn till hur konsekvenser sprids mellan samhällssektorer/-funktioner/-verksamheter på lokal, regional och nationell nivå genom beroenden samt de totala konsekvenserna som uppstår i samhället vid olika former av störningar. Därmed är denna typ av analys mer djuplodande och av annan karaktär än de konsekvensanalyser som typiskt genomförs inom ramen för t.ex. RSA-arbete och kontinuitetsarbete, vilka ofta främst fångar in hur olika hot direkt påverkar samhället och/eller de tjänster olika samhällsviktiga verksamheter levererar. Vidare ses här kritisk infrastruktur som en delmängd av samhällsviktig verksamhet, då MSB-direktiv inte särskiljer mellan dessa utan endast använder begreppet samhällsviktig verksamhet.

## 1.2 Syfte

Syftet för uppdraget kan, utifrån bakomliggande uppdragsbeskrivning och LUCRAMs tolkning av uppdraget i form av en aktivitetsplan, sammanfattas med att det ska ge ett underlag för framtagande av metoder som behövs för att aktörer inom krisberedskapssystemet på lokal-, regional- respektive nationell nivå ska kunna genomföra konsekvensanalyser på samhällsnivå. Speciellt har syftet varit att undersöka och ge vägledning för hur det svenska ”nerifrån-och-upp”-perspektivet kan stödja konsekvensanalyser på samhällsnivå.

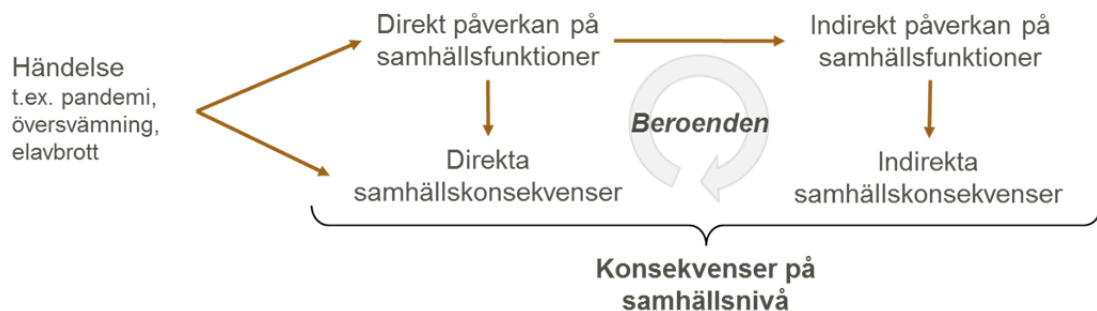
För att uppnå syftet med uppdraget fastställdes tre huvudsakliga aktiviteter i aktivitetsplanen:

1. Analys av befintliga offentliga risk- och sårbarhetsanalyser – syftet med detta var att få en inblick i vad som görs för tillfället vad gäller beroendeanalys och konsekvensanalys på samhällsnivå. Syftet var även att ta fram underlag för hur ”nerifrån-och-upp”-perspektivet kan stödja konsekvensanalyser på samhällsnivå. Denna del av uppdraget redovisas i Kapitel 2.

2. Intervjuer med internationella organ – syftet med denna aktivitet var att få en inblick i hur frågor kring konsekvensanalys på samhällsnivå hanteras i andra länder. Denna del av uppdraget redovisas i Kapitel 3.
3. Avstämning av tankar för utveckling av konsekvensanalyser på samhällsnivå – syftet med denna aktivitet var att utifrån föregående två aktiviteter beskriva ett antal utgångspunkter för det vidare arbetet med konsekvensanalyser på samhällsnivå samt att få synpunkter och återkoppling från olika aktörer i det svenska krishanteringssystemet. Denna del av uppdraget redovisas i Kapitel 4 och 5.

### 1.3 Konsekvensanalys på samhällsnivå (KAS)

Generellt sett handlar konsekvensanalyser om att uppskatta karaktären och storleken på de konsekvenser som uppstår till följd av någon form av hot eller störning i samhället. Konsekvensanalyser ingår t.ex. i de risk- och sårbarhetsanalyser som genomförs i det svenska krishanteringssystemet. Ofta fokuseras konsekvensanalyser på direkta konsekvenser av hot och störningar, t.ex. vilka direkta konsekvenser som en översvämning får på människors liv och hälsa samt vilka samhällsfunktioner som direkt drabbas av översvämningen. Dessa konsekvensanalyser kan vara mycket grova, som de som normalt görs inom ramen för en risk- och sårbarhetsanalys, eller av mer detaljerad karaktär, som den som genomfördes i Mälaruppdraget (MSB, 2012). Det som dock är gemensamt är att de oftast fokuserar på de direkta konsekvenserna, eller som det uttrycks i Mälaruppdraget: ”beroenden har studerats i ett led, endast direkta kostnader och antalet personer som direkt påverkas av utebliven samhällsservice har beräknats” (Ibid.). *Konsekvensanalys på samhällsnivå*, såsom föreslås i föreliggande rapport, skulle t.ex. kunna användas för att även utreda konsekvenser som uppstår i flera led (dvs. indirekta konsekvenser) på ett systematiskt vis i konsekvensutredningar för olika typer av händelser, se Figur 1.1. Detta synsätt med att ta hänsyn till effekter som sprider sig mellan olika samhällsfunktioner är nära relaterat till begreppet kaskaderande effekter (eng. Cascading Effects) och som börjat få ökad uppmärksamhet ur både ett myndighets- och forskningsperspektiv.



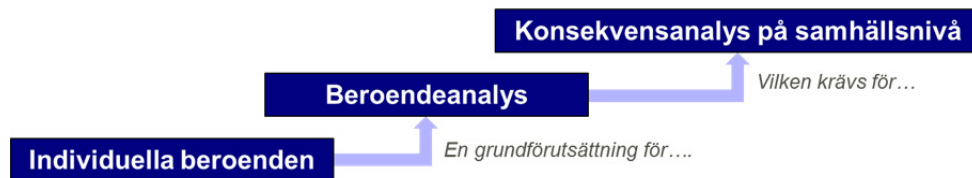
Figur 1.1 Schematisk skiss över vad som avses med konsekvenser på samhällsnivå (KAS)

**Konsekvensanalys på samhällsnivå definieras** som en konsekvensanalys som tar hänsyn till *omfattningen och hur* konsekvenser på grund av en *störning sprids* mellan samhällssektorer/-funktioner/-verksamheter på lokal, regional och/eller nationell nivå genom beroenden och resulterande *totala konsekvenser* som uppstår i *samhället*.

Denna definition är något mer operationell än den beskrivning av KAS som ges i handlingsplanen för skydd av samhällsviktig verksamhet (MSB, 2013, sid. 28). En sådan konsekvensanalys måste därmed alltid utgå från en beroendeanalys som beskriver hur verksamheter, funktioner och sektorer är beroende av varandra och hur konsekvenser kan spridas mellan dessa om någon eller några av dem utsätts för störningar. För att kunna genomföra en beroendeanalys måste i sin tur information om individuella beroenden finnas, vilka sedan kan aggregeras upp till en beroendeanalys som tar hänsyn till beroenden i



flera led. Information om individuella beroenden är sådant som identifierats som en relation mellan en samhällsviktig verksamhet, funktion eller sektor till en annan samt styrka och konsekvenser av denna relation. Ett förenklat fiktivt exempel är: akutsjukvården är starkt beroende av vattenförsörjning och vid bortfall reduceras förmågan att ta emot och behandla akutfall till hälften inom loppet av timmar. Dessa principer sammanfattas i Figur 1.2 nedan och används även som en röd tråd genom rapporten.



Figur 1.2 Kopplingen mellan individuella beroenden, beroendeanalys och konsekvensanalys på samhällsnivå.

## 1.4 Avgränsningar

Rapporten ska ses som ett första steg i arbete med att utveckla konsekvensanalyser på samhällsnivå. Givet uppdragets omfattning och den komplexitet som föreligger inom området har vi inte kunnat ge konkreta förslag, t.ex. ange konkreta metoder eller vilken typ av informationsinfrastruktur som behöver byggas upp, för genomförandet av konsekvensanalys på samhällsnivå inom ramen för det svenska krishanterings-systemet. Istället beskriver vi utgångspunkter för ett sådant arbete som författarna anser är viktiga att ta i beaktande i den vidare utvecklingen av metoder och verktyg inom området. Vidare tas här en mer pragmatisk ansats och forskningsgrunden till föreliggande rapport indikeras i nästföljande avsnitt.

## 1.5 Bakomliggande arbete

Föreliggande arbete vilar på tidigare arbete som har genomförts i uppdragsform av författarna åt MSB och på författarnas vetenskapliga arbete inom området, som naturligt även inbegriper den nationella och internationella forskningsfronten. För en redogörelse av forskningsbasen bakom föreliggande rapport är lämpliga utgångspunkter följande avrapporteringar av uppdrag som författarna tidigare genomfört åt MSB; i Hassel et al. (2014) genomför vi en bred kunskapsöversikt av forskningen inom området skydd av samhällsviktig verksamhet (där 2813 artiklar översiktligt granskas och där 523 artiklar från 239 olika tidsskrifter ansågs som relevanta och utgjorde basen för kunskapsöversikten), i Johansson et al. (2014) genomförs en studie kring beroenden inom en specifik sektor, nämligen Information och Kommunikation (där nuvarande status för hur aktörerna tar hänsyn till beroenden inom sektorn undersöktes samt en modellerings- och simuleringsansats föreslogs för att ta hänsyn till ömsesidiga beroenden mellan kommunikationsinfrastrukturer utifrån vetenskapligt arbete inom området) och, slutligen, i Johansson et al. (2013) presenteras en studie och utvärdering av metoder för beroendeanalys på sektoriell såväl som tvärsektoriell nivå (där en omfattande litteratursökning kring metoder för beroendeanalys genomfördes och dessa delades in i 8 kategorier, där vetenskaplig nyckelreferenser för respektive kategori ges, som sedan utvärderades gentemot MSB:s identifierade behov).

## 1.6 Medverkande

Uppdraget har utförts av Tekn. Dr. Jonas Johansson, Tekn. Dr. Henrik Hassel, Professor Kurt Petersen och Björn Arvidsson, alla verksamma vid LUCRAM.



## 2 Analys av risk- och sårbarhetsanalyser

För att få en utgångspunkt och statusläge kring hur och till i vilken utsträckning som konsekvensanalyser på samhällsnivå genomförs i den offentliga sektorn gjordes en genomgång av utvalda kommuners, länsstyrelser och centrala myndigheters risk- och sårbarhetsanalyser. Rapporterna som analyserades var de som var inskickade för inrapporteringsåret 2011 för kommunerna och 2013 för länsstyrelserna samt de centrala myndigheterna. Syftet är att ge en översiktlig inblick över i nuvarande status rörande beroenden, som sedan kan ligga till grund för vägledning kring hur en metodik kan utformas för att stödja mer djuplodande beroendeanalyser och konsekvensanalyser på lokal, regional och nationell nivå. Denna analys ger även en inblick i vilka konkreta beroenden som identifieras och analyseras på olika nivåer i samhället, vilket i sig är intressant information för vidare arbete inom området beroende- och konsekvensanalys. Vidare skulle föreliggande analys kunna återupprepas då nya risk- och sårbarhetsanalyser inrapporteras för att genomföra trendanalyser och identifiera utvecklingsbehov.

God kunskap om hur svenska aktörer arbetar med beroende- och konsekvensanalyser är viktigt då den metodik som ska utvecklas bör ta utgångspunkt i det nuvarande kunskapsläget och dagens praktik. Metodiken skulle få betydligt större genomslagskraft om befintliga krishanteringsstrukturer kan utnyttjas och byggas vidare på.

I följande avsnitt presenteras först metoden som användes för att analysera risk- och sårbarhetsanalyserna och det utvalda materialet, vilket sedan följs av ett avsnitt med presentation och diskussion av resultaten. I det tredje avsnittet används resultaten för att genomföra en enklare beroendeanalys som i sin tur ger vägledning kring till vilken grad nuvarande informationsnivå om beroenden i rapporterna kan användas till. Kapitlet avslutas med reflektioner och slutsatser.

### 2.1 Metod och material

Avdelningen för riskhantering och samhällssäkerhet vid LTH har tillgång till RSA-dokumentation från flertalet kommuner, samtliga länsstyrelser och en del myndigheter för åren 2011 respektive 2013. Till grund för analysen valdes tio kommuners, tio länsstyrelser och tio centrala myndigheters dokumentation ut, se Tabell 2.1. Urvalet av rapporterna genomfördes utifrån att få en bred spridning ur synvinklarna sektorstillhörighet, geografi samt storlek. Vidare lästes och kodades endast huvudtexten i rapporterna, eventuella bilagor eller externa referenser kodades ej för att säkerställa en rimlig omfattning. Vidare är det troligt att om en aktör har identifierat ett kritiskt beroende och på något sätt utnyttjat denna information i RSA:n kommer detta att omnämnas i huvudtexten. Om så är fallet och en hänvisning till en referens eller bilaga ges noteras detta, men genomläsning av referensen eller bilagan genomfördes ej.

Tabell 2.1 Utvalda offentliga aktörers risk- och sårbarhetsanalyser.

Myndigheter	Länsstyrelser	Kommuner
Svenska Kraftnät	Blekinge Län	Stockholm Stad
Jordbruksverket	Dalarna Län	Göteborgs Stad
PTS	Gotland Län	Lunds Kommun
Socialstyrelsen	Hallands Län	Hässleholms Kommun
MSB	Jämtlands Län	Nyköpings Kommun
Livsmedelsverket	Jönköpings Län	Varberg Kommun
Trafikverket	Stockholms Län	Skellefteå Kommun
Finansinspektionen	Södermanlands Län	Marks Kommun
Försäkringskassan	Uppsala Län	Eslövs Kommun
Tullverket	Värmland Län	Ljusnabergs Kommun

För att systematiskt kunna analysera dokumentationen, utvecklades en bedömningsmall med kodningskriterier i tre olika nivåer i enlighet med Figur 1.2: 1) Information om individuella beroenden, 2) Information om beroendeanalys samt 3) Information om konsekvensanalys på samhällsnivå (KAS). Övergripande om kodningskriterierna för respektive nivå beskrivs nedan.

### 2.1.1 Detaljerad information om individuella beroenden

I denna kodningsnivå kartlades omnämning av specifika individuella beroenden mellan sektorer och/eller samhällsfunktioner. Kategorisering av samhällssektorer och samhällsfunktioner utgår från rapporten ”Handlingsplan för skydd av samhällsviktig verksamhet” (MSB, 2013). Några samhällssektorer samt samhällsfunktioner lades även till för att möjliggöra kartläggningen. Till exempel anges i en del rapporter ett generellt beroende till, eller av, samhällsviktig verksamhet eller samhällets funktionalitet, dvs. som aktören inte specificerar närmre till en viss sektor eller funktion. Därmed fick till exempel Samhällsviktig verksamhet och Funktionalitet läggas till som funktionskategorier under en ny sektorskategori Samhället. Vidare fick sektorskategorierna Naturresurser samt Forskning och utbildning läggas till för att kunna fånga in angivna beroenden i rapporterna, då dessa ej inkluderas i de elva kategorier enligt (MSB, 2013). I Bilaga 1 återges samtliga använda sektorer och funktioner. Denna kategorisering utgör även en god grund kring fortsatt arbete med att definiera samhällsviktiga sektorer och funktioner.

Syftet med kartläggning är att få en bild över hur och vilka beroenden som anges. Varje unik omnämning av ett beroende bokfördes och kodades, även om beroendet mellan samhällsfunktionerna även nämnts tidigare i rapporten (t.ex. först i sammanfattningen och senare i ett beroendeavsnitt). Ett omnämning av ett beroende är typiskt att aktören har angivit ett beroende eller påverkan från en sektor/funktion till en annan (inte nödvändigt att ordet beroende har använts, utan räcker med att en relation har angivits). Syftet är att kunna analysera vilka beroenden som nämns flest gånger, då detta kan vara en indikation, av flera, på hur kritiskt beroendet anses vara. Endast beroenden mellan sektorer och/eller funktioner kartlades och interna beroenden för samhällsfunktionens ignorerades (t.ex. beroendet till interna IT-system exkluderades, men om det angavs ett beroende mellan dessa interna IT-system och t.ex. Internet inkluderades beroendet).

Kodningskriterierna som användes för varje individuellt beroende var:

- Avsnitt i rapporten (t.ex. risk-/scenariobeskrivning, förmågebedömning, eget beroendeavsnitt)
- Sida i rapporten
- Citatutdrag för beroendet
- Beroendebeskrivning (Nämns, Kvalitativt, Semi-kvantitativt, Kvantitativt)<sup>1</sup>
- Beroendebedömning (t.ex. Saknades, Logiskt resonemang, Workshop, Empiri, Beroendehjulet)
- Beroendets styrka (Saknas, Svag, Medel, Starkt)
- Beroendets konsekvens (Saknas, Liten, Medel, Stora)
- Användning av informationen (t.ex. Bara omnämning, Konsekvensanalys, Åtgärdsförslag)
- Spridande sektor (sektorer i enlighet med MSB (2013) + ytterligare, se Bilaga 1)
- Spridande funktion (funktioner i enlighet med MSB (2013) + ytterligare, se Bilaga 1)
- Mottagande sektor (sektorer i enlighet med MSB (2013) + ytterligare, Bilaga 1)
- Mottagande funktion (funktioner i enlighet med MSB (2013) + ytterligare, Bilaga 1)
- Övriga noteringar (t.ex. osäkerhet i hur ett beroende bör kodas)

---

<sup>1</sup> I Kapitel 1 används begreppen kvalitativt, semi-kvantitativt och kvantitativt. Här avses med kvalitativt att endast ett storleksuttryck använts utan någon underliggande skala presenterats, semi-kvantitativt att en presenterad kvalitativ intervallskala använts och kvantitativt att en presenterad kvantitativ intervallskala eller kvotskala använts.

### 2.1.2 Information om beroendeanalys

Här kartlades om någon form av beroendeanalys genomförts samt hur och till vilken grad dessa i sådana fall genomförts. För att klassificeras som en beroendeanalys måste någon form av högre ordningens spridning mellan olika sektorer och/eller funktioner ha nämnts. Den enklaste typen av beroendeanalys är att ett logiskt resonemang kring spridning mellan flera funktioner, exempelvis ”för att genomföra ledning krävs att de elektroniska kommunikationerna fungerar vilka i sin tur är beroende av elförsörjning”. Ett sådant uttalande klassas som beroendeanalys av ”enstaka indirekta beroenden”. Även användande av beroendematriser eller visualisering av beroenden mellan flera funktioner/sektorer (t.ex. genom uppritning av ett beroendenätverk) klassas som att en beroendeanalys genomförts. Djupare analyser innefattar användandet av en strukturerad metod och aggregering, och möjligen även simulering/beräkning av spridningseffekter som kan uppstå på grund av beroenden.

Kodningskriterierna för beroendeanalys var:

- Avsnitt i rapporten (t.ex. Risk-/scenariobeskrivning, Förmågebedömning, Eget beroendeavsnitt)
- Sida i rapporten
- Analysdjup (t.ex. Enstaka indirekta beroenden, Aggregerat visuellt, Beräkning/simulering)
- Metod (t.ex. Kontinuitetshantering, Matris, Nätverk, MSB:s beroendehjul)
- Användning av analysen (t.ex. Bara omnämning, Konsekvensanalys, Åtgärdsförslag)
- Noteringar (t.ex. mer utförlig information om hur analysen genomfördes)

### 2.1.3 Information om konsekvensanalys på samhällsnivå (KAS)

Här dokumenterades om konsekvensanalys på samhällsnivå (KAS) bedömdes vara genomförd och till i vilken omfattning den i så fall genomfördes. Med konsekvensanalys på samhällsnivå menas här att någon form av metod har använts för att systematiskt ta hänsyn till beroenden för att utreda hur påfrestningar på en sektor eller funktion sprider sig genom beroenden och omfattningen av de totala konsekvenser som uppstår i samhället. Ett exempel på KAS är att, utifrån information om beroenden, en analys har genomförts där en störning har definierats och hur denna störning sprider sig genom beroendena och vilka konsekvenser som uppstår. Dels direkta för respektive samhällsfunktion men även de aggregerade indirekta konsekvenserna som uppstår på samhällsnivå.

Kodningskriterierna för konsekvensanalys på samhällsnivå var:

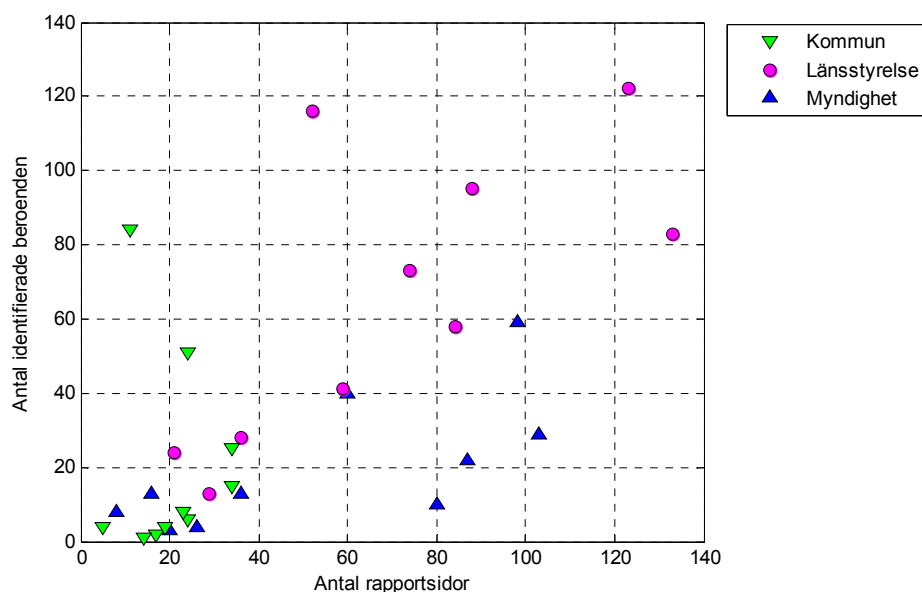
- Avsnitt i rapporten (t.ex. Risk-/scenariobeskrivning, Förmågebedömning, Eget beroendeavsnitt)
- Sida i rapporten
- Metod för KAS (Aggregerad summering - första ordningens), Aggregerad analys - första + högre ordningens, Beräkning/simulering)
- Beskrivning konsekvens (Nämns, Kvalitativt, Semi-kvantitativt, Kvantitativt)
- Enhet konsekvens (Ekonomisk, Funktion, Döda, Skadade, Övrig)
- Användning av analysen (t.ex. Bara omnämning, Konsekvensanalys, Åtgärdsförslag)
- Noteringar (t.ex. mer utförlig information om hur analysen genomfördes)

## 2.2 Resultat

Resultatet från genomgången av dokumentationen rörande angivna beroenden i aktörernas risk- och sårbarhetsanalyser presenteras först översiktligt och sedan i ett avsnitt var i enlighet med de tre kodningsnivåerna: Information om individuella beroenden, Information om beroendeanalys samt Information om konsekvensanalys på samhällsnivå (KAS). Diskussion av resultaten ges i samband med

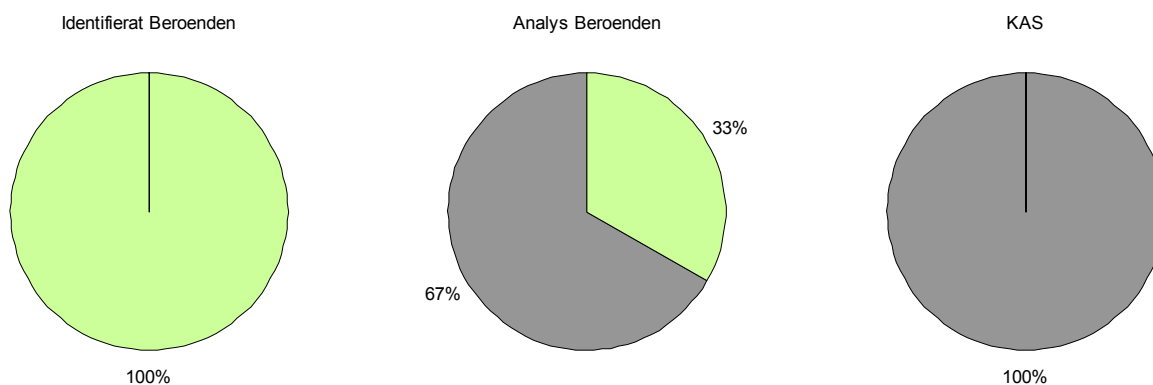
presentation av resultaten. Det ska noteras att resultaten härstammar från en genomgång av rapporter från 2011 samt 2013 och fångar därmed inte den eventuella utvecklingen de senaste åren inom området.

Omfattning i antal sidor för risk- och sårbarhetsanalyserna varierade kraftigt mellan de olika aktörerna, från 5 till 133 sidor (från 5 till 298 sidor inklusive bilagor). Antalet identifierade beroenden varierade också mellan rapporterna, från 1 som minst till 122 identifierade beroenden som mest. Det finns en viss korrelation mellan rapportens omfattning i antal sidor och antal identifierade beroenden, se Figur 2.1. Generellt är länsstyrelsernas risk- och sårbarhetsanalyser mest omfattande, sett till både antal sidor och antalet identifierade beroenden, följt av myndigheternas och minst omfattande var kommunernas – även om individuella skillnader finns. Totalt har författarna läst igenom och analyserat ca 1400 sidor (om bilagor inkluderats ca 2000 sidor), dvs. en relativt omfattande genomgång - även då endast tio stycken rapporter från respektive aktörsnivå valdes ut. Det sammanlagda antalet kartlagda unika omnämningar av beroenden uppgick till 1054 st.



Figur 2.1 Antal identifierade beroenden i förhållande till antalet huvudrapportsidor för respektive aktörs risk- och sårbarhetsanalys.

I samtliga rapporter nämndes ett eller flera beroende mellan två samhällssektorer eller samhällsfunktioner, se Figur 2.2. Endast i storleksordningen en tredjedel hade dock genomfört någon form av beroendeanalys (t.ex. presenterat data i en beroendematrix eller gjort uttalande av effekterna av indirekta beroenden). Ingen av aktörerna hade genomfört någon form av konsekvensanalys på samhällsnivå i enlighet med hur denna typ av analys är definierad i föreliggande rapport enligt avsnitt 1.3.

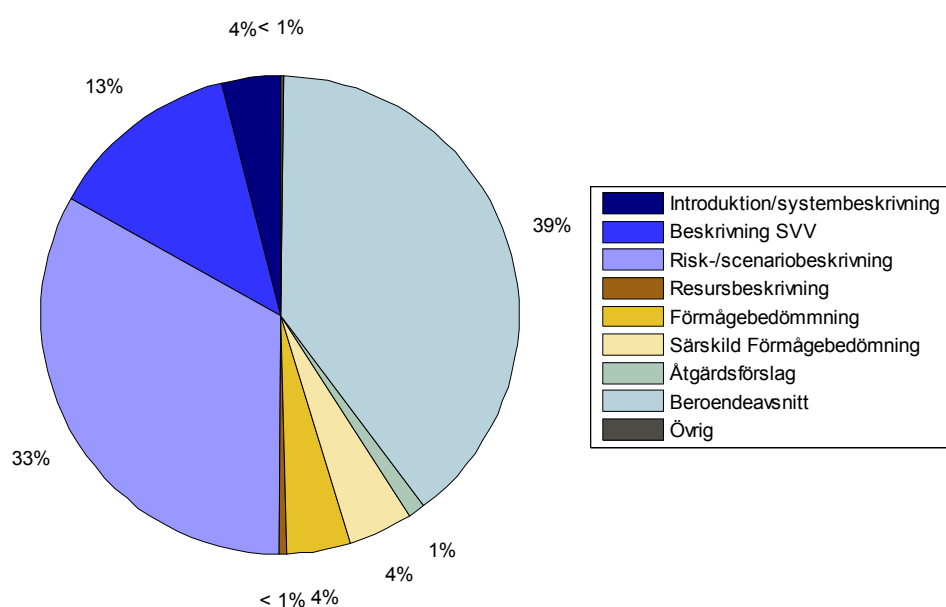


Figur 2.2 Fördelningen över antal rapporter som har identifierat beroenden, analyserat beroenden och genomfört konsekvensanalys på samhällsnivå (andelen markerad i grönt).

## 2.2.1 Individuella beroenden

Varje enskilt beroende mellan samhällssektorer eller samhällsfunktioner som nämndes i rapporterna kategoriserades i enlighet med tidigare nämnda kodningskategorier. I vissa fall har ett visst omnämmande varit svårt att kategorisera. I de fall tvetydighet fanns togs omnämmandet upp till diskussion bland författarna varvid en viss transparens av bedömningar uppnåddes. Om samma beroende nämndes flera gånger (t.ex. mellan el- och vattenförsörjning) i olika delar av en rapport togs varje enskilt fall med och kodades, i enlighet med vad som nämnts tidigare.

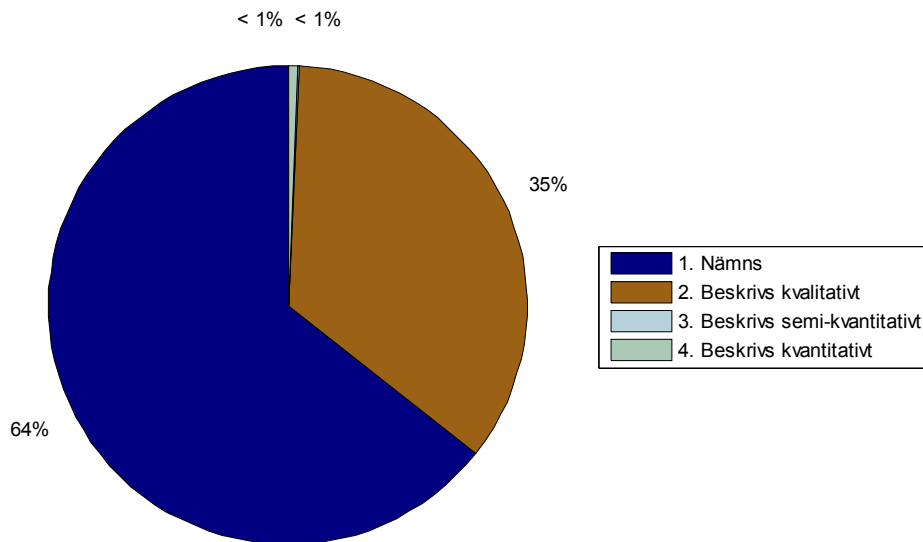
De flesta omnämningarna av beroenden återfanns i rapportavsnitten som handlade om risk- och scenariobeskrivningar (33 %) eller i ett eget beroendeavsnitt (39 %), se Figur 2.3. Ett mindre antal av beroendena omnämndes i avsnittet angående beskrivning av samhällsviktig verksamhet (13 %). Under avsnitten rörande introduktion/systembeskrivning, förmågebedömning och särskild förmågebedömning omnämndes även en del beroenden, om än i mycket mindre omfattning (ca 4 % för respektive kategori).



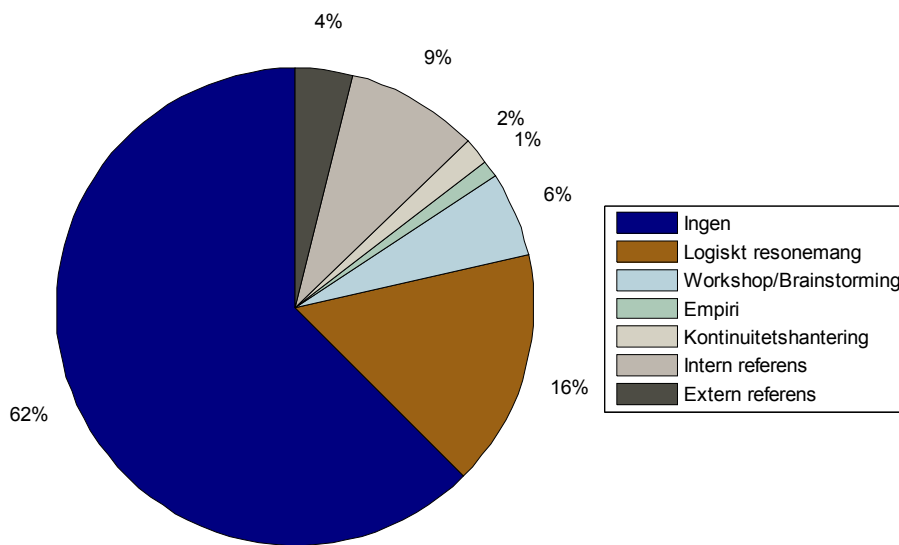
Figur 2.3 Fördelning över vilka avsnitt som beroende nämns i rapporterna.

Med avseende på hur beroendena uttrycks (se Figur 2.4), är det relativt många (64 %) som endast är ett generellt omnämmande att ett beroende föreligger och en del (35 %) där någon form av kvalitativt uttryck ges (t.ex. att det är ett kritiskt beroende eller att beroendet kan ge upphov till stora konsekvenser). Endast i ett ytterst fåtal falls används en semi-kvantitativ eller kvantitativ skala vid angivelsen av beroendet.

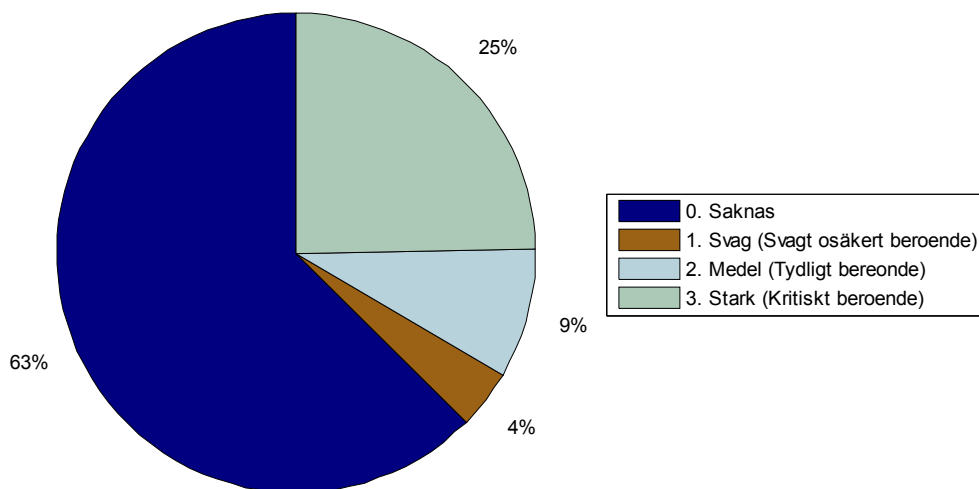
Beroendena som angavs i rapporterna kodades även efter vad som låg till grund för bedömningen, se Figur 2.5. I merparten av fallen (62 %) nämndes endast beroendet, utan något bakomliggande logiskt resonemang, workshop, empiri, etc. använts för att stödja omnämmandet. I en del fall användes dock ett logiskt resonemang (16 %), att beroendet härstammade från en workshop (6 %) eller från ett tidigare internt arbete (9 %). Endast i sällsynta fall härstammade beroendet från en extern utredning (4 %), en kontinuitetshanteringsprocess (2 %) eller hade empiriskt stöd (1 %) (t.ex. omnämmande om en tidigare inträffad händelse). Värt att notera är att kontinuitetshantering ej fått större genomslag vid identifieringen av de nämnda beroendena i de RSA-rapporter som analyserades och att det är ett relativt stort antal beroende som endast omnämns utan ytterligare stöd av någon metod eller empiri. Noteras bör dock att även om underlaget för en bedömning ej kunnat identifieras behöver det inte innebära att bedömningen är grundlös, utan kan bero på bristande transparens och tydlighet i rapporten.



Figur 2.4 Fördelning över hur beroendena uttrycktes.



Figur 2.5 Fördelning över vad som låg till grund för angivelsen av beroendet.

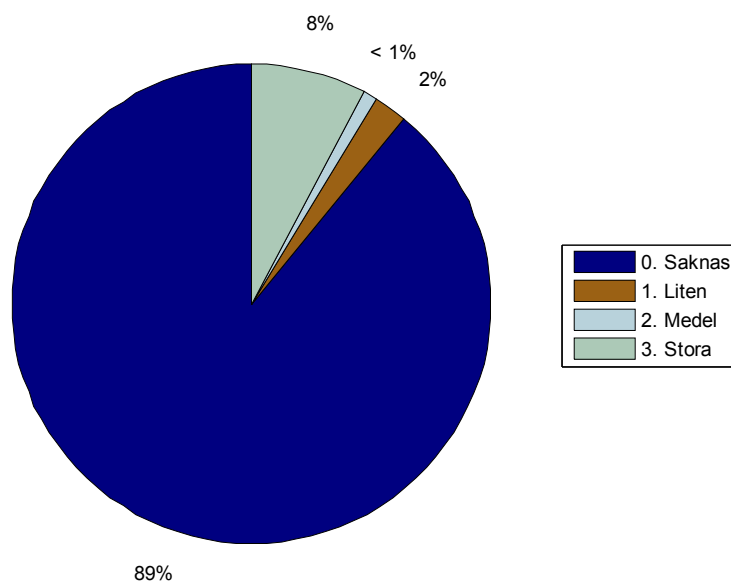


Figur 2.6 Fördelning av styrkan av angivna beroenden.



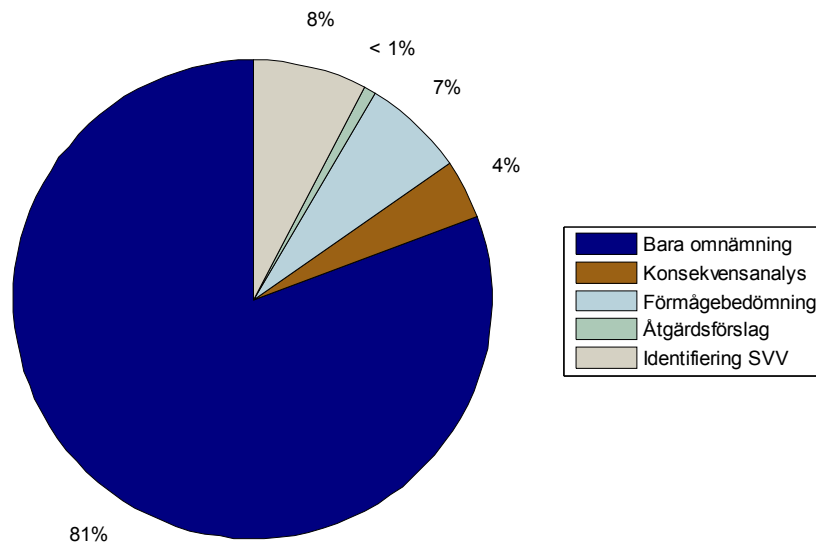
För varje beroende kodades även vilken styrka som angivits för beroendet, se Figur 2.6 För ca 37 % av beroendena hade någon form av styrka angivits, fördelat på svagt/osäkert beroende (4 %), medel/tydligt beroende (9 %) och starkt/kritiskt (25 %) beroende. I de fall styrka angivits, var övervägande del bedömda som starka (kritiska) beroenden, vilket är logiskt då föreskrifterna (MSBFS 2010:6 & 2010:7) anger att det just är kritiska beroenden som ska identifieras i risk- och sårbarhetsanalyserna.

Endast i ett fåtal fall (11 %) angavs någon form av skattning av allvarlighetsgraden i de konsekvenserna som uppstår ifall ett beroende realiserats, se Figur 2.7, medan för det överhängande antalet angavs ingen konsekvens (89 %). En orsak kan vara att konsekvensen är en naturlig del utav uppskattandet av beroendets styrka, det ger dock vissa negativa signaler kring möjligheterna att använda nuvarande information i risk- och sårbarhetsanalyserna för att försöka skatta konsekvenser som kan uppstå på samhällsnivå på grund av beroenden. I storleksordningen 8 % av konsekvensskattningarna tillhörde kategorin stora konsekvenser, 1 % medelkonsekvenser och 2 % liten konsekvens.



Figur 2.7 Angivelse av konsekvenser i samband med omnämning av beroenden.

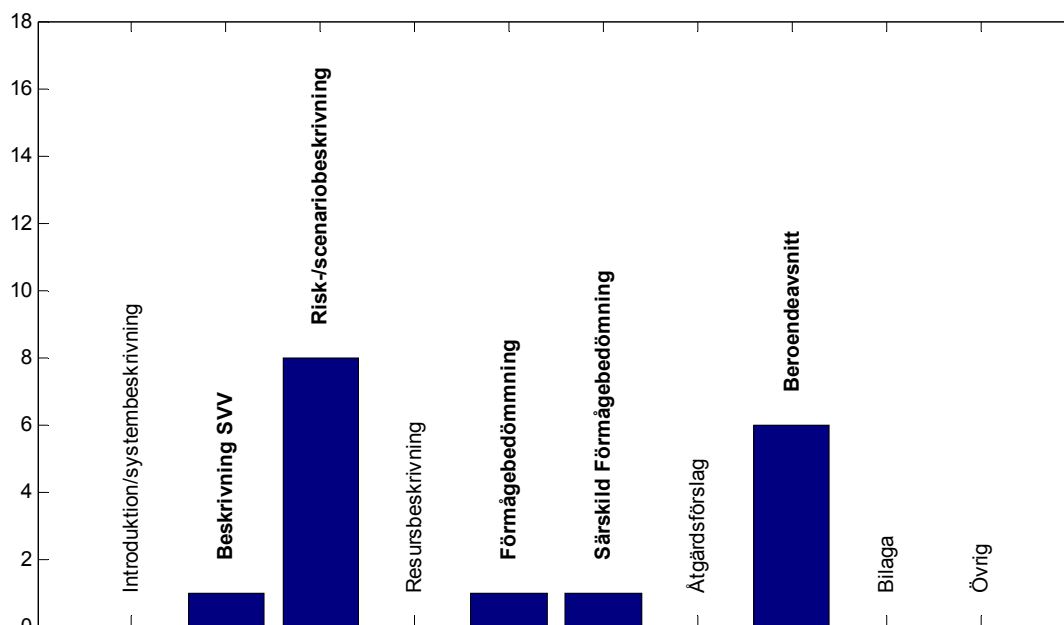
I Figur 2.8 anges i vilket syfte omnämmandet av beroenden skett. För merparten av beroendena handlade det endast om ett omnämning, utan vidare användning av informationen (81 %). Utav beroendeomnämningarna användes i 8 % av fallen informationen för att identifiera samhällsviktig verksamhet, i 7 % av fallen för någon form av konsekvensanalys, i 4 % av fallen i samband med en förmågebedömning och i 1% av fallen användes beroendeinformationen för åtgärdsförslag. Detta visar tydligt att det är relativt dålig koppling mellan identifiering av beroenden och faktisk användning av informationen.



Figur 2.8 Fördelning över vad informationen om beroendet användes till.

## 2.2.2 Beroendeanalys

Endast i en tredjedel av rapporterna genomfördes någon form av beroendeanalys, dvs. i tio av de trettio rapporterna. Merparten av beroendeanalyserna kan hänföras till avsnitten kring risk-/scenariobeskrivning (8 st.) alternativt ett eget avsnitt avseende beroenden (6 st.), se Figur 2.9. Endast i ett fall omnämndes en beroendeanalys i samband med beskrivning av samhällsviktig verksamhet. Totalt identifierades sjutton beroendeanalys i de tio rapporterna, dvs. mer än en beroendeanalys genomförs i vissa av rapporterna. Det var främst Länsstyrelser (7 av 10 rapporter) som genomfört en beroendeanalys. Kommuner (2 av 10 rapporter) och myndigheter (1 av 10 rapporter) hade i mycket lägre utsträckning genomfört någon form av beroendeanalys.

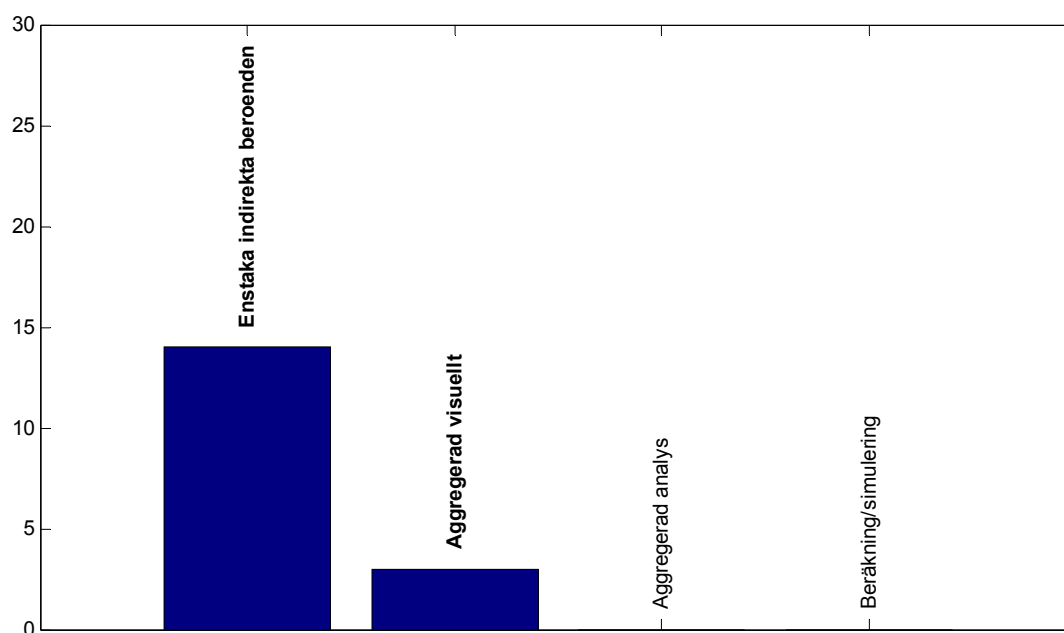


Figur 2.9 Rapportavsnitt i vilka beroendeanalys genomförs.

Det ska noteras att tolkningen kring vad som kan anses utgöra en beroendeanalys har varit ganska frikostig, där omnämmandet av effekter av indirekta beroenden har bedömts som utförande av en beroendeanalys. Till exempel bedöms ett textavsnitt liknande ”vid elbortfall kommer mobilnäten att gå ner

inom loppet av timmar vilket leder till kommunikationsproblem som försvårar länsstyrelsens hantering av en kris” som en beroendeanalys av enstaka indirekta beroenden. Utöver denna typ av beroendeanalys (14 st.) var det även en del (3 st.) som använde någon form av visuellt aggregerad analys (t.ex. beroendematrix eller ett nätverk), dock utan att djupare analysera konsekvenserna av dessa beroenden, se Figur 2.10.

Det bör noteras att ingen aktör har genomfört någon form av aggregerad analys, dvs. analyserat djupare kring konsekvenserna av de identifierade beroendena. Vidare var det ingen aktör som använt någon form av simulerings- eller beräkningsstöd för att genomföra djupare beroendeanalys. Därmed är det tydligt att *nuvarande fokus i rapporterna* är på att *identifiera beroenden* snarare än att *analysera konsekvenserna av beroendena* inom respektive aktörs geografiska områdesansvar eller sektorsansvar.



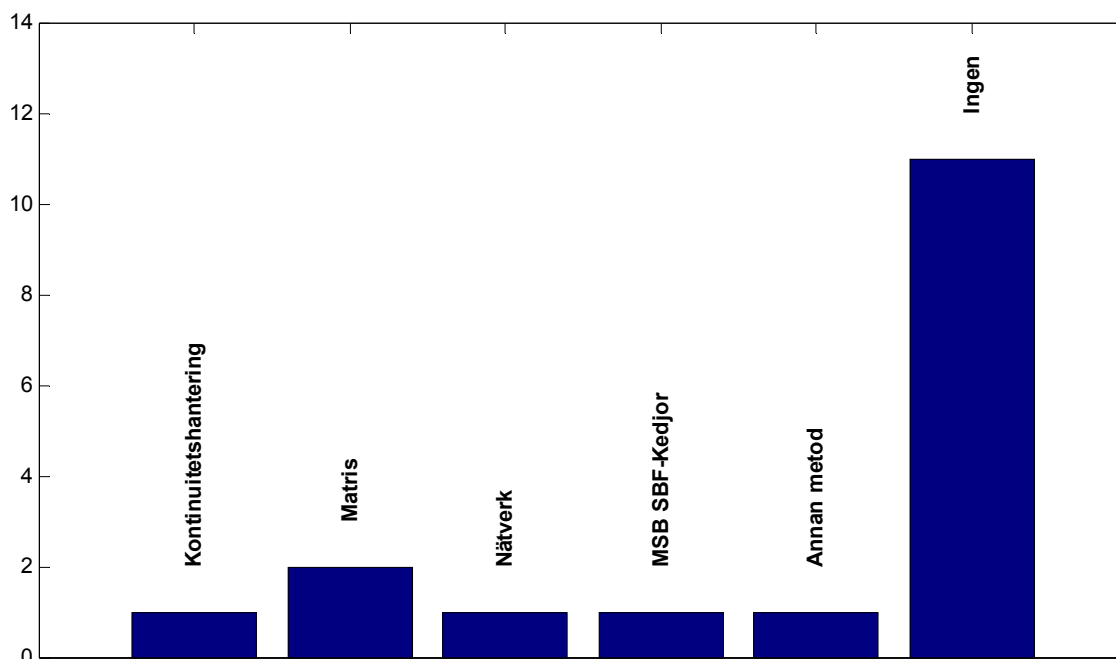
Figur 2.10 Typ av beroendeanalys som genomförs.

Avseende vilken metod som använts för beroendeanalys har i merparten av fallen ingen uttalad metod använts (11st). I vissa fall har dock en metod för analysen angivits, med fördelningen kontinuitetshantering<sup>2</sup> (1st), användande av en beroendematrix (2 st.), uppritning av ett nätverk (1 st.), MSB:s spridnings-/beroende-/fokusedjor<sup>3</sup> (1 st.) och annan metod (1 st.). I fallet då en annan metod använts handlar det om FOI:s metod för risk- och sårbarhetsanalyser (FORSA). Det är således en relativt stor spridning i metodval i de fall en beroendeanalys genomförs.

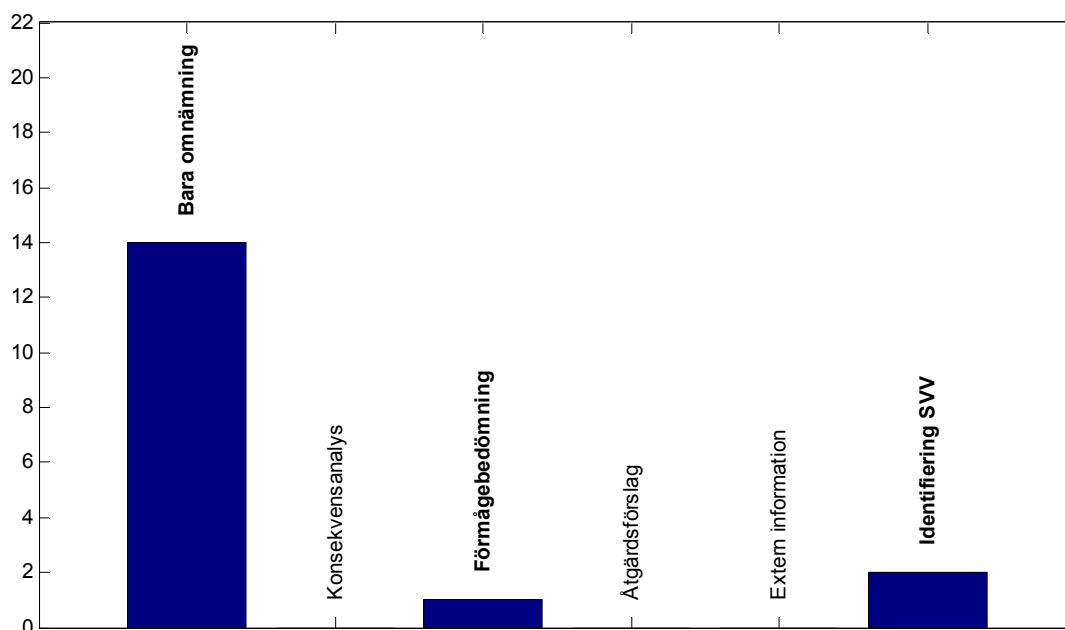
I likhet med omnämningen av de individuella beroendena används resultatet från beroendeanalyserna i relativt liten utsträckning (åtminstone inte tydligt hur resultatet använts), se Figur 2.12. I 14 fall handlar det endast om en omnämning av enstaka indirekta beroenden medan i ett fall användes beroendeanalysen för att informera en förmågebedömning och i två fall vid identifiering av samhällsviktig verksamhet.

<sup>2</sup> Kontinuitetshantering är en process där det bland annat det ingår att *identifiera direkta beroenden* för en verksamhet. Om en kontinuitetshanteringsprocess har lett fram till identifiering av de omnämnda beroendena i rapporten och deras inverkan på verksamheten, har det här klassats som att kontinuitetshantering använts som en metod för beroendeanalys (kanske något missvisande). Det ska dock inte tolkas som att kontinuitetshantering är en metod för att aggregera och analysera ömsesidiga beroenden mellan flera verksamheter.

<sup>3</sup> I enlighet med MSB:s rapport ”Faller en, faller då alla?” (MSB, 2009).



Figur 2.11 Metod som använts vid beroendeanalyserna.



Figur 2.12 Användning av resultatet från beroendeanalyserna.

### 2.2.3 Konsekvensanalys på samhällsnivå

Ingen aktör har genomfört en konsekvensanalys på samhällsnivå i enlighet med hur en sådan analys är definierad i denna rapport. En grundförutsättning för genomförande av konsekvensanalys på samhällsnivå är att en systematisk metod används för genomförandet av beroendeanalyser, men i enlighet med föregående avsnitt genomförs sådana beroendeanalyser i väldigt liten utsträckning. Det kommer därmed krävas arbete med att först säkerställa att beroendeanalyser genomförs med någon metod innan det är möjligt för aktörerna att genomföra konsekvensanalys på samhällsnivå, i enlighet med diskussionen i avsnitt 1.3.

## 2.3 Aggregering av individuella beroenden

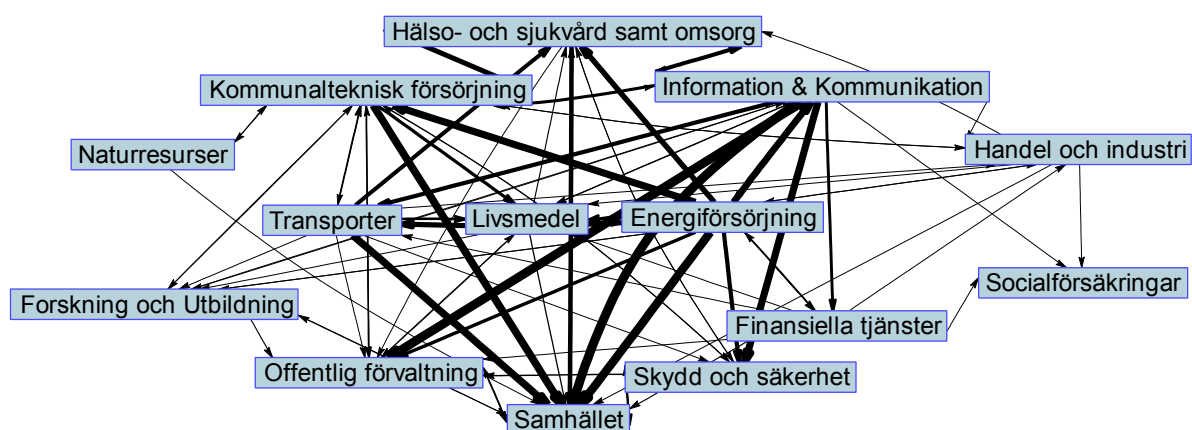
Var och en av de individuella beroendena som identifierades i risk- och sårbarhetsanalyserna kodades utifrån vilken som var den spridande samhällssektorn/ samhällsfunktionen och den mottagande samhällssektorn/samhällsfunktionen. I Bilaga 1 anges samtliga använda samhällssektorer och samhällsfunktioner, och som är ett resultat av vilka sådana som faktiskt omnämns i risk- och sårbarhetsanalyserna. Därmed fick en del sektorer och samhällsfunktioner läggas till i den lista som återfinns i MSB:s ”Handlingsplan för skydd av samhällsviktig verksamhet” (MSB, 2013). För sektorer fick samhällssektorerna ”Forskning och utbildning” (för att t.ex. möjliggöra inkludering av beroenden till utbildad personal), ”Naturresurser” (för att t.ex. möjliggöra inkludering av beroenden till sjöar och vattendrag) och ”Samhället” (för att t.ex. möjliggöra inkludering av mer generella omnämning av samhällsviktiga verksamheter och allmänhetens beroenden) läggas till. För funktioner fick samhällsfunktioner såsom t.ex. ”Forskning”, ”Kompetent personal” och ”Satellit/GNSS” läggas till.

I följande avsnitt presenteras översiktligt data, först för de identifierade beroendena mellan samhällsfunktioner och sedan för de identifierade beroendena mellan samhällsfunktioner, i form av nätverk samt enklare analyser av insamlad data. I Bilaga 2 presenteras även insamlad data i form av beroendematriser. Styrkan i beroendena motsvarar endast hur många gånger totalt ett specifikt beroende har nämnts i de analyserade rapporterna, vilken i sin tur troligen i stor utsträckning är starkt korrelerade av de fokusområden och scenarier som MSB pekat ut under de senaste åren (t.ex. fördjupad förmågebedömning angående GNSS) och annat arbete (t.ex. Styrel-arbetet som bl.a. bestod i prioritering av samhällsfunktioner utifrån deras elberoende). Vidare hittades flest antal omnämning av beroende i länsstyrelsernas RSA:er (se Figur 2.1), vilket gör att resultaten i viss mån speglas av detta. Därmed ska resultaten användas med försiktighet. Det kan dock vara intressant att i förlängningen genomföra jämförande studier med de beroendedata som MSB samlade in inom ramen för projektet ”Faller en, faller då alla?” (MSB, 2009) och fortsatt arbete som följt efter den rapporten samt jämförelser med andra typer av beroendedata (t.ex. nationalekonomisk data angående handel med produkter och tjänster mellan samhällets olika sektorer).

För presentation av insamlad data i följande avsnitt har fokus varit att tydliggöra vilka beroenden som nämns av aktörerna snarare än att använda insamlad data för att undersöka faktiska beroendeförhållanden, då i många fall styrka för beroendena inte anges (se Figur 2.6). Denna presentation ger därmed endast en grov bild över hur beroendeförhållande ser ut mellan samhällssektorer och samhällsfunktioner samt indikerar typ av väldigt begränsade beroendeanalyser som kan genomföras med insamlad data. Det ska dock poängteras att informationen som finns tillgänglig i RSA-rapporterna inte är av den kvalitet eller omfattning som krävs för att möjliggöra djupare beroendeanalyser och i sin tur konsekvensanalyser på samhällsnivå. Det positiva, och som vi vill spegla här, är dock att det går att extrahera viss information om beroenden från rapporterna. Diskussion av möjligheter och begränsningar med hänsyn till detta tas upp i kapitel 1.

### 2.3.1 Beroenden mellan samhällssektorer

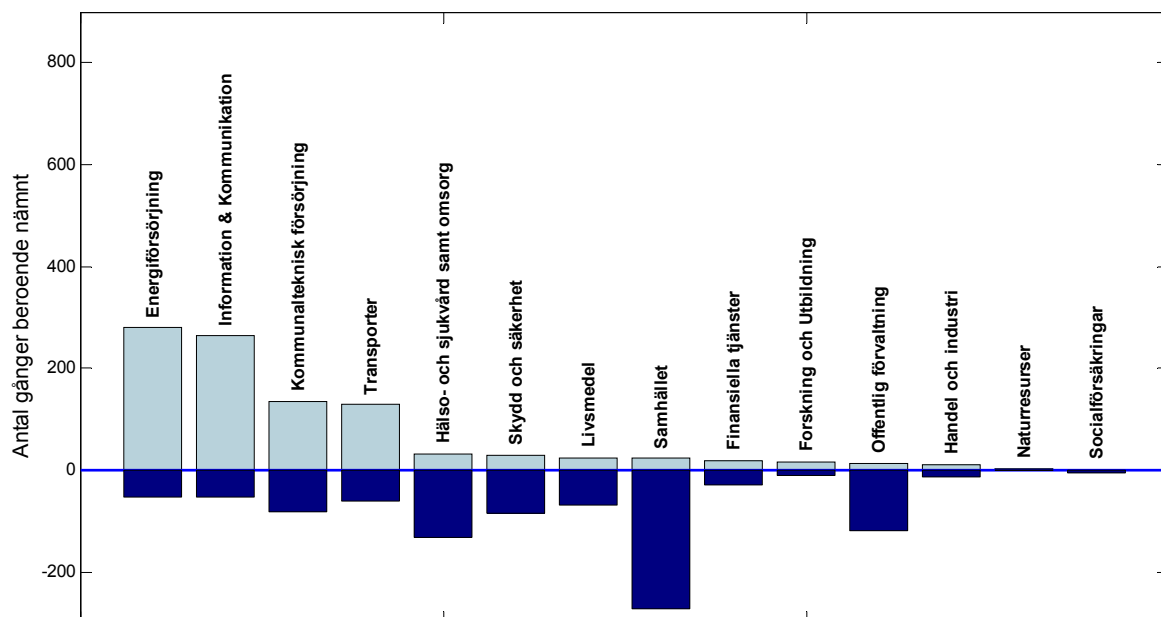
Totalt omnämndes beroenden mellan fjorton samhällssektorer, i enlighet med diskussionen i avsnitt 2.1 och kategorierna i Bilaga 1. I de flesta fall anges dock inte beroendet mellan samhällssektorer utan mellan samhällsfunktioner, i dessa fall har författarna även kategoriserat dessa som tillhörande en sektor utifrån vilken samhällsfunktion som angivits (i enlighet med Bilaga 1). I Figur 2.13 återges beroendenätverket utifrån aggregerade data av omnämnda sektorsberoenden i aktörernas dokumentation av risk- och sårbarhetsanalyserna. Tjockleken på beroendena är skalade i enlighet med antal omnämnande av ett specifikt beroende. Utifrån figuren kan bland annat slutsatsen dras att sektorer i samhället är i hög grad beroende av varandra och att det är svårt att intuitivt förstå hur spridningen av störningar kan manifesteras sig.



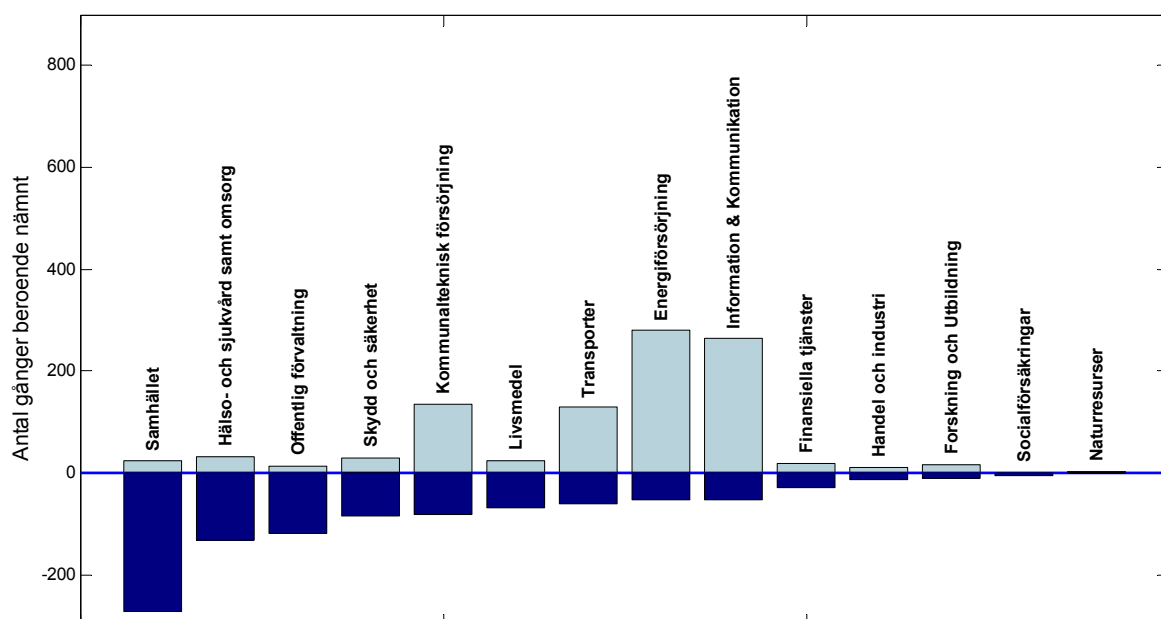
Figur 2.13 Riktat beroendenätverk för samhällssektorer. Tjocklek på beroendet är en viktning utifrån hur många gånger beroendet mellan två specifika sektorer angivits i aktörernas dokumentation över risk- och sårbarhetsanalyserna. Pil anger beroenderiktning (pil in = beroende av, pil ut = påverkan på).

För att dra några övergripande slutsatser av sektorsberoendena har en enklare beroendeanalys genomförts avseende antalet gånger ett beroende för en sektor omnämnts, uppdelat på perspektiven: 1) hur andra sektorer beror av en viss sektor och 2) en viss sektors beroende till andra sektorer. Resultatet presenteras i Figur 2.14 och Figur 2.15, som endast skiljer sig i sorteringen av sektorerna utifrån de två perspektiven. Utifrån dessa figurer kan vissa övergripande slutsatser dras angående vilka sektorer som utifrån aktörernas bedömningar av beroenden är spridare, mål, nav och solitärer i enlighet med MSB:s terminologi i rapporten "Faller en, faller då alla?" (MSB, 2009).

Spridare är sektorer som många andra sektorer är beroende av, men som själva inte är beroende av många andra sektorer. Utifrån data insamlad i detta projekt framgår det att sektorerna Energiförsörjning och Information och Kommunikation är tydliga spridare. Mål (mottagare) är sektorer som är beroende av många andra sektorer, men som få andra sektorer är beroende av. Sektorerna Samhället, Hälso- sjukvård samt omsorg och Offentlig förvaltning är tydliga mål. Nav är sektorer som både många andra sektorer är beroende av och som själva är beroende av många sektorer. Till denna kategori kan Kommunalteknisk försörjning och Transporter sägas tillhöra. Solitärer är sektorer som få andra sektorer är beroende av och som själva ej heller är beroende av andra sektorer. Det är dock svårt att dra några generella slutsatser utifrån insamlad data, då denna ej kan anses vara en komplett representation av samtliga beroende i samhället utan endast vilka beroenden som nämnts oftast i risk- och sårbarhetsanalyserna.



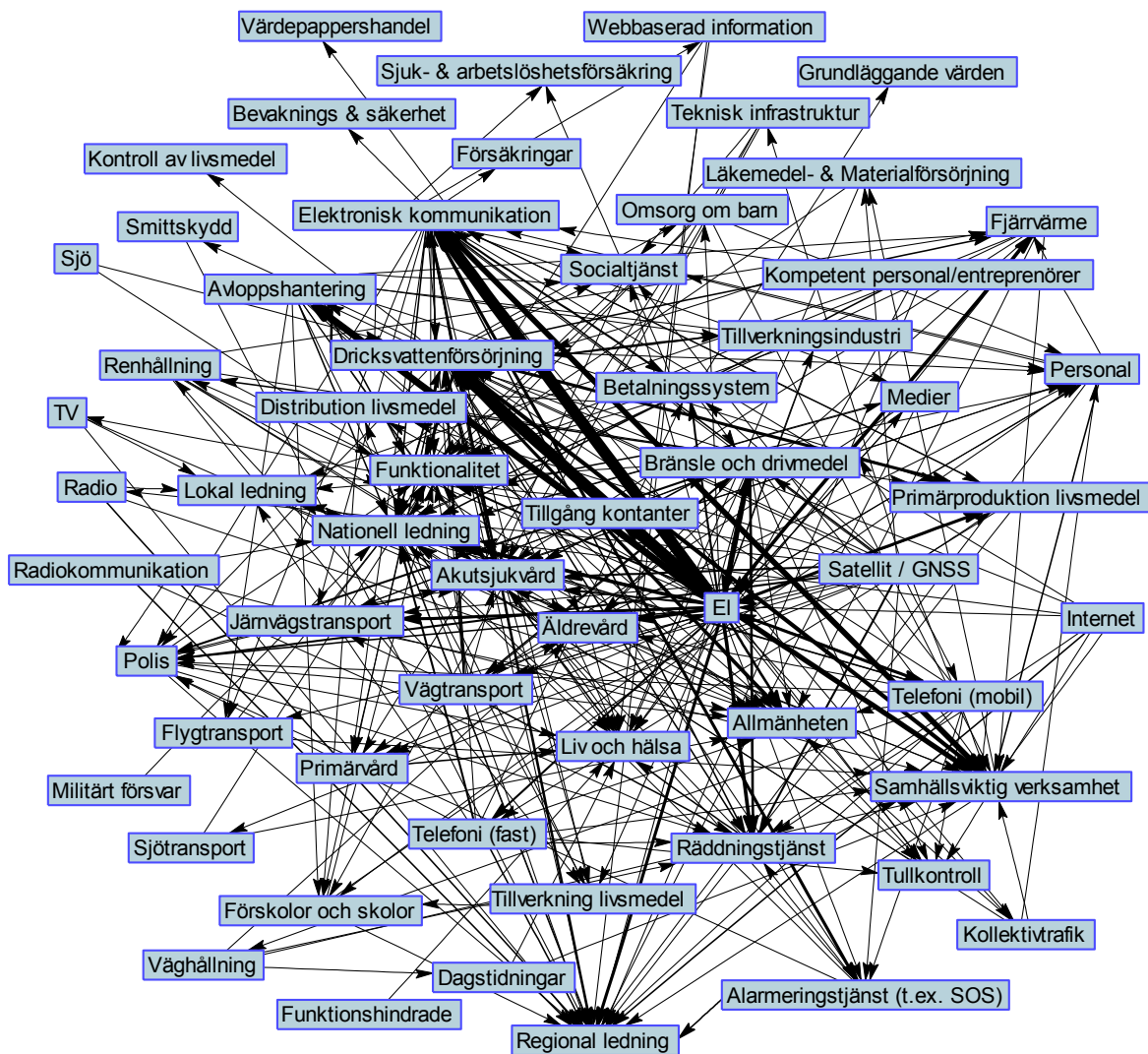
Figur 2.14 Antal gånger ett beroende är nämnt för en samhällssektor, uppdelat på hur andra sektorer är beroende av sektorn (ljusblå stapel) och hur sektorn är beroende av andra sektorer (mörkblå stapel). Sorterat utifrån andra sektorer beroende av en viss sektor.



Figur 2.15 Antal gånger ett beroende är nämnt för en samhällssektor, uppdelat på hur andra sektorer är beroende av sektorn (ljusblå stapel) och hur sektorn är beroende av andra sektorer (mörkblå stapel). Sorterat utifrån en viss sektors beroende av andra sektorer.

### 2.3.2 Beroenden mellan samhällsfunktioner

I likhet med presentationen av data för samhällssektorer presenteras här insamlad data över beroende mellan samhällsfunktioner. Beroende som omnämns mellan en samhällsfunktion och en samhällssektor (dvs. ej funktion till funktion) har ej tagits med i följande analys (dock skulle intressanta inom- och utomsektoriella analyser även kunna göras, men fått uteslutas på grund av uppdragets begränsade omfattning). I Figur 2.16 återges beroendenätverket utifrån aggregerade data av omnämnda funktionsberoenden i aktörernas dokumentation av risk- och sårbarhetsanalyserna. I förhållande till beroendenätverket över sektorsberoendena är det tydligt att en högre upplösning ger upphov till ett mer komplext nätverk, som är än svårare att intuitivt greppa och förstå hur spridningar av konsekvenser kommer att ske mellan olika samhällsfunktioner och de totala samhällskonsekvenserna som uppstår vid störningar.

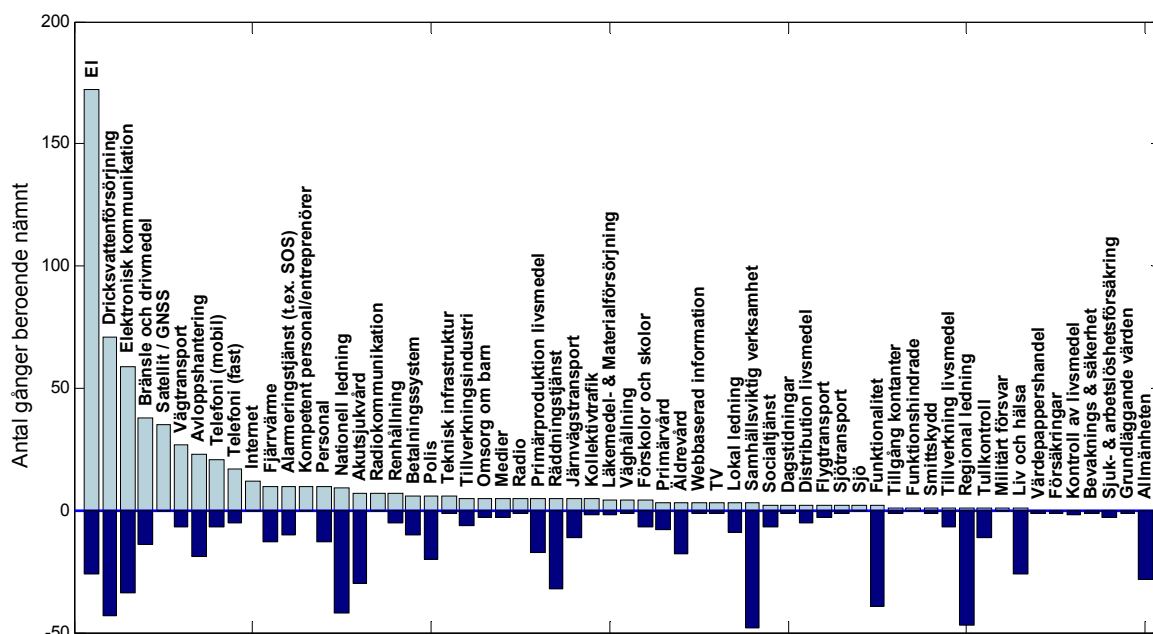


Figur 2.16 Riktat beroendenätverk för samhällsfunktioner. Tjocklek på beroendet är en viktning utifrån hur många gånger beroendet mellan två specifika funktioner angivits i aktörernas dokumentation över risk- och sårbarhetsanalyserna. Pil anger beroenderiktning (pil in = beroende av, pil ut = påverkan på).

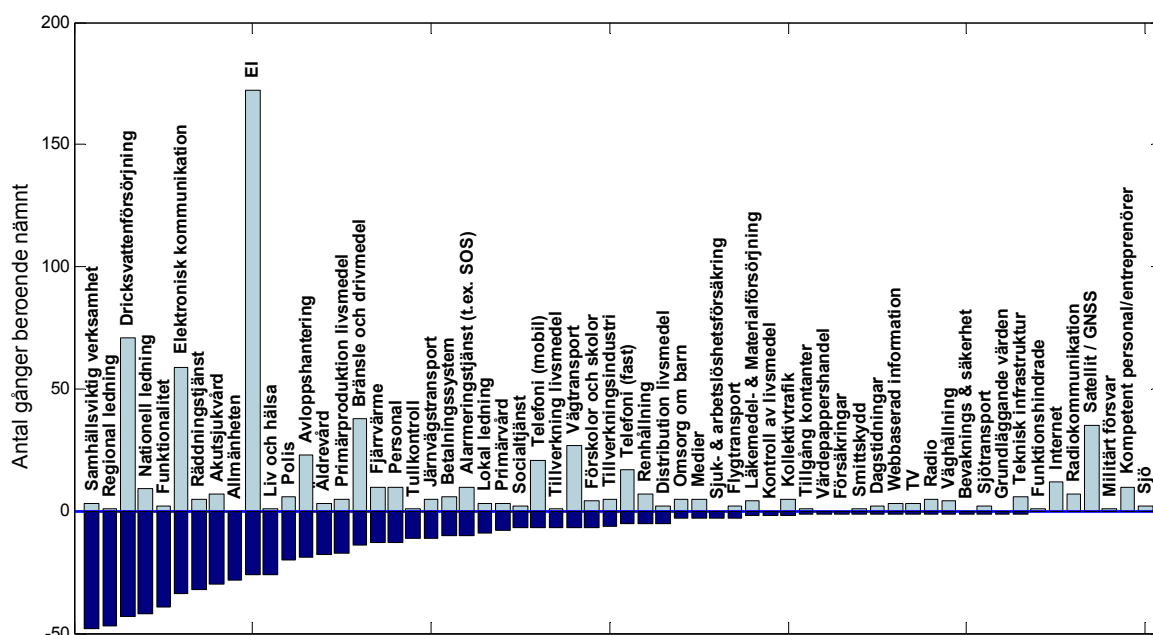
I Figur 2.17 och Figur 2.18 presenteras antalet gånger ett beroende har omnämnts för de olika samhällsfunktionerna, med perspektiv i likhet med föregående avsnitt över sektorsberoendena. Här framgår det tydligt att EI och Elektronisk kommunikation är centrala försörjare till samhället, dvs. så



kallade spridare. Tydliga mål (mottagare) är Samhällsviktig verksamhet (en kategori som författarna använde då aktören inte närmre specificerat vilken funktion som är beroende utan mer generellt angett samhällsviktig verksamhet) och Regional ledning. Dricksvattenförsörjning är många samhällsfunktioner beroende av samtidigt som den i sig själv är beroende av många andra funktioner, dvs. ett typiskt nav. I likhet med sektorer är det utifrån insamlad data svårt att uttala sig om vilka funktioner som kan anses vara solitärer.



Figur 2.17 Antal gånger ett beroende är nämnt för en samhällsfunktion, uppdelat på hur andra funktioner är beroende av funktionen (ljusblå stapel) och hur funktionen är beroende av andra funktioner (mörkblå stapel). Sorterat utifrån andra funktioners beroende av en viss funktion.



Figur 2.18 Antal gånger ett beroende är nämnt för en samhällsfunktion, uppdelat på hur andra funktioner är beroende av funktionen (ljusblå stapel) och hur funktionen är beroende av andra funktioner (mörkblå stapel). Sorterat utifrån en viss funktions beroende av andra funktioner.

## 2.4 Diskussion och slutsatser

Här ges en övergripande diskussion samt slutsatser av analysen av kommunernas, länsstyrelsernas och myndigheternas dokumentation av deras risk- och sårbarhetsarbete med avseende på beroenden. Positivt är att i samtliga dokument omnämns beroenden, medan det är relativt få (10/30) som genomför någon form av beroendeanalys, då främst Länsstyrelser (7/10), och det är ingen som genomför en konsekvensanalys på samhällsnivå i enlighet med den definition som används i föreliggande rapport. De beroendeanalyser som genomförs är dock i regel av mindre djup karaktär, som i merparten av fallen handlar om en kvalitativ beskrivning av enstaka indirekta beroenden och i enstaka fall en visuell aggregering av beroendena i form av ett beroendenätverk eller beroendematrix, men utan någon djupare analys av spridningseffekter. En anledning till att antal identifierade beroende, antal och nivå av beroendeanalyserna samt bristen på KAS kan till viss del bero på att analyserna är från åren 2011 och 2013 men kan även bero på att aktörerna anser att denna typ av information kan vara känslig och av sekretessskäl väljer att ej redovisa detaljerat (en åsikt som fördes fram under workshopen med samhällsaktörer, se Bilaga 3).

Vidare är det förvånande att relativt få beroenden nämns i samband med identifiering av samhällsviktig verksamhet, men det kan ha sin grund i MSB:s vägledning för identifiering av samhällsviktigt verksamhet (MSB, 2014) - där identifiering av kritiska beroenden ligger i sista steget, efter identifiering av den samhällsviktiga verksamheten. Merparten av omnämmandet av beroenden görs antingen i avsnitten som handlar om risk- och scenariobeskrivningar eller i ett eget beroendeavsnitt, det sistnämnda är positivt då det pekar på att behovet av identifiering och formaliseringen av kritiska beroenden har fått ett visst genomslag hos aktörerna. Å andra sidan skulle även ett sådant angreppssätt kunna leda till minskad användning av resultaten från beroendeanalyserna, vilket så klart inte är önskvärt.

Till nackdel för möjligheterna till aggregering av beroendedata är att det endast i ett fåtal fall används en semi-kvantitativ eller kvantitativ skala vid angivelsen av beroendets styrka och endast i fåtal fall kopplas någon form av konsekvensuppskattning till beroendet. Vidare använder aktörerna en stor mängd olika termer för att beskriva samhällsfunktioner (vilka författarna var tvungna att tolka för att kunna kategorisera och aggregera data) och en enhetlig terminologi för samhällssektorer och samhällsfunktioner saknas. Dessa har inverkan på vad resultaten kan användas till och pekar ut ett problemområde för att kunna använda informationen om beroendena för att i förlängningen möjliggöra genomförandet av djupare beroendeanalyser. Därmed är det från rådande status mycket svårt att använda informationen om beroenden som ingångsvärden för att genomföra konsekvensanalyser på samhällsnivå, vilket ej heller någon aktör genomfört.

I de fåtal fall en beroendeanalys genomförs är det en relativt stor spridning i metodval, där det är något förvånande att kontinuitetshantering ej fått större genomslag vid identifiering av beroenden. Anledningen kan vara att kontinuitetshantering inte etablerat sig som en möjlig metodlösning för analys av direkta beroenden för en verksamhet förrän under de senaste åren, dvs. i samband med eller efter åren för de studerade dokumenten (2011 och 2013 års analyser). I endast ett fåtal fall har en beroendematrix eller ett beroendenätverk använts som metod för att visualisera beroenden, dvs. lägsta kravet för att i förlängningen kunna genomföra mer djuplodande beroendeanalyser.

De övergripande slutsatserna som dras utifrån genomgången av dokumentationen är att vikten av att identifiera beroenden mellan samhällssektorer och samhällsfunktioner i stort har uppmärksamats och lett till att beroenden explicit uttrycks. Däremot stannar det oftast vid en omnämning av ett potentiellt beroende, där styrka för beroendet och konsekvenser som uppstår ifall ett beroende realiserats saknas. Att det saknas ett gemensamt arbetssätt hos aktörerna och att information om beroenden till synes inte används i speciellt stor utsträckning kan bero på att i föreskrifterna (MSBFS 2010:6; MSBFS 2010:7) och

Vägledningen för Risk- och sårbarhetsanalyser (MSB, 2011) ges inte några konkreta krav eller förslag på tillvägagångssätt när det gäller analys av kritiska beroenden eller hur resultat från sådana analysen kan användas. Därmed kommer det generellt att behövas formalisering av kategorisering, angreppssätt och metoder innan beroendeanalyser kan genomföras på ett systematiskt sätt av olika samhällsaktörer. Detta är också en grundförutsättning för att kunna aggregera data för att i förlängningen kunna genomföra konsekvensanalyser på samhällsnivå.

Det bör dock påpekas det positiva i det faktum att offentliga aktörer på olika nivåer i samhället genomför risk- och sårbarhetsanalyser där beroenden faktiskt adresseras.



## 3 Intervjustudier

Som en del av uppdraget genomfördes ett antal intervjustudier med internationella aktörer i syfte att få inblick i andra länders arbete med skydd av samhällsviktig verksamhet och beroenden. I Bilaga 3 framgår de frågor som ställdes och de detaljerade svar som framkom under intervjuerna (på engelska). I detta kapitel ges en sammanfattning av den information som framkom under intervjuerna och som ansetts viktigaste att förmedla inom ramen för syftet med uppdraget. Intervjuerna som genomfördes var semi-strukturerade, dvs. användning av en tematisk struktur med på förhand givna frågor och med öppna svarsmöjligheter. Aktörer från tre länder/organisationer intervjuades: 1) Holland och TNO (Netherlands Organisation for Applied Scientific Research), 2) EU och JRC (Joint Research Center) samt slutligen 3) USA och DHS (Department of Homeland Security) samt NISAC (National Infrastructure Simulation and Analysis Center).

### 3.1 TNO, Holland

#### 3.1.1 Bakgrund, arbetsområden och projekt

TNO är en icke-vinstdrivande forsknings- och konsultorganisation som bl.a. stödjer de Nederländska myndigheterna. De som intervjuades, Eric Luijff och Marieke Klave, har jobbat inom området skydd av samhällsviktig verksamhet sedan 1995 – då främst inom informationssektorn. TNO är och har varit involverade i flertalet projekt inom området skydd av samhällsviktig verksamhet. I många fall är det EU-finansierade forskningsprojekt det handlar om såsom: PREDICT, Intact, CIPRnet och Smart grid. De har även genomfört en intervjustudie avseende olika länders (Sverige, Australien, UK och USA) arbete med tvärssektoriella beroenden (TNO, 2013) som har tydliga beröringspunkter med detta uppdrag.

#### 3.1.2 Lagstiftning, ramverk och riktlinjer

I Nederländerna är det Ministry of Security and Justice som driver och koordinerar frågan om tvärssektoriella beroenden mellan samhällsfunktioner. Dock finns ingen övergripande lagstiftning som reglerar detta arbete. Däremot finns lagstiftning inom vissa specifika sektorer, där telekomsektor är den sektor som kommit längst med arbetet med skydd av samhällsviktig verksamhet, t.ex. finns s.k. ”incident response boards” etablerade som ska kunna ge stöd då händelser inträffar. I denna sektor har EU i huvudsak varit huvuddrivande men de nederländska myndigheterna driver på denna utveckling ytterligare. Det finns ambitioner att bredda arbete inom telekomsektorn till andra sektorer.

Inom tre områden finns det lagstiftning och vägledning som berör skydd av samhällsviktig verksamhet. Det första området är *Identifiering av nationell kritisk infrastruktur*. Här koordinerar och ställer Ministry of Security and Justice krav på att varje sektor ska identifiera infrastruktur/samhällsviktiga verksamheter som är speciellt kritisk. De som genomför identifieringen är dock departementen för respektive sektor. Det andra området är *Nationell riskanalys*, som till viss del berör området skydd av samhällsviktig verksamhet, där det finns en scenariobaserad metodstruktur utarbetad. Denna riskanalys används framför allt på nationell nivå för att ta fram policyer och prioritera resurstilldelning på nationell nivå. Det tredje området är *Regionala riskanalyser* som måste genomföras av de s.k. *Safety and Security Regions*. Samma metod som används för den nationella riskanalysen rekommenderas, men är inget krav. Det ska noteras att den lokala nivån inte har krav på sig att genomföra riskanalysarbete, dock ingår ofta lokala aktörer som representanter i regionerna, speciellt för de större städerna.

### 3.1.3 Metoder och verktyg

Ett antal metoder och verktyg som är relevanta för detta uppdrag framkom under intervjun:

**Identifieringen av nationell kritisk infrastruktur.** Tidigare användes den s.k. quick-scan metoden som utvecklats av TNO för att identifiera nationellt kritisk infrastruktur. Numer används en annan metod, men denna är inte offentlig. Den är dock främst workshop-baserad och Ministry of Security and Justice jobbar med att införa olika nivåer av ”kritiskhet” (tidigare var det bara ja/nej) av anledningen att i stort sett alla infrastrukturer helt enkelt klassades som kritiska. Typiskt används identifieringen till att avgöra vad som är viktigt, vilket skydd som behövs och om det nuvarande skyddet är tillräckligt.

**Nationell riskanalys.** Metoden som används är workshop-baserad där personer från olika sektorer bjuds in. Hittills har totalt 60 scenarier analyserats. I metoden ingår att ta hänsyn till direkta effekter men ingen systematik kring kaskadeffekter (dvs. indirekta högre ordningens konsekvenser). Dock är det något som håller på att ses över.

**PREDICT.** Detta EU-projekt som TNO deltar i fokuserar på att ta fram metoder och verktyg för hur beroenden kan analyseras på en regional nivå. Tre kontexter berör man där målgrupperna är något olika: a) Översvämning, b) Järnvägsolycka, c) Fartygsincident. Fokus ligger på förberedande fasen och planeringsfasen, samt delvis även på akuta fasen.

**CIPRnet.** Detta är ett Center of Excellence där olika forskningsinstitutioner i Europa ingår. Tanken är att utbyte av idéer, metoder och liknande för modellering och simulering ska ske vilket ska ge liknande förmågor som NISAC i USA (fast inte i form av en enskild centrumbildning). Man fokuserar även på standardisering av termer då detta kan öka interkompabilitet.

**TNO-databasen.** TNO har samlat data om händelser (via media och via incidentutredningar) som samlas i en databas (se mer info nedan), främst avseende elavbrott. Denna information används t.ex. i workshops som TNO håller i med syftet att ge en faktabakgrund till t.ex. scenariot som analyseras.

### 3.1.4 Databasinsamling och spridning av resultat

TNO-databasen som byggts upp bygger framför allt på medierapporter (Google-sökning på 9 språk) och delvis incidentutredningar, främst avseende elavbrott. I databasen kodas händelser som involverat kaskadeffekter och hittills finns 10340 inmatningar i databasen. Till exempel kodas påverkad sektor/subsektor, mänskliga handlingar, tidpunkt, plats och konsekvenser.

TNO har även arbetat med att samla in ytterligare data, t.ex. via de som äger och driver samhällsviktiga verksamheter. Det har visat sig vara svårt att få data från dessa aktörer vilket framförallt beror på att mycket av data är känslig ur sekretessynpunkt och är man inte tydlig med vilken nytta aktörerna kan få är dessa obenägna att lämna ut data. Dock kan det vara svårt att få ut data som visar på precisa geografiska platser. Men dessa data behövs sällan eftersom ungefärliga platser ofta är nog för att dra vettiga slutsatser. Är det dessutom endast test av metoder det handlar om räcker det med realistisk, snarare än faktisk och fullständig, data. I många fall kommer man även långt med ”open-access” data.

När det gäller de lite mer ”mjuka” samhällsviktiga verksamheter, såsom livsmedelssektor eller sjukvårdssektorn är TNOs erfarenhet att det är svårare att hitta och få fram data.

### 3.1.5 Lärdomar och planer inför framtiden

Ett antal lärdomar och framtidsplaner beskrevs av TNO under intervjun.

Att använda en GIS-plattform för informationsdelning och visualisering av resultat har visat sig vara effektivt för att få aktörer intresserade och att få dem att dela med sig av information,

Vissa privata aktörer (och även offentliga) verkar på nationell nivå vilket gör att det inte överensstämmer med det system av regionala analyser som används i Nederländerna. Dessa nationella aktörer har inte möjlighet att delta i samtliga regioners arbete. Ett annat problem kan uppstå då många aktörer har liknande ansvar i en region (t.ex. många telekom-operatörer). Dock kan inte samtliga av dessa aktörer delta utan någon representant måste väljas ut vilket inte alltid är enkelt.

För att lyckas med den privat-offentliga samverkan måste de olika aktörerna förstå och ta hänsyn till att man har olika mål.

TNO menar att många av byggblocken för arbetet med skydd av samhällsviktiga verksamheter är på plats men arbetet är fortfarande fragmenterat och det är viktigt att lärdomar sprids på ett bättre sätt mellan t.ex. länder och sektorer.

En viktig del av det framtida arbetet handlar om att avgöra vilken detaljeringsgrad som behövs i olika delar av arbetet med skydd av samhällsviktig verksamhet.

2016 kommer Nederländerna att vara ordförande i EU och förhoppningen är att man då ska föra skydd av samhällsviktig verksamhet som en viktig fråga.

## 3.2 JRC, EU

### 3.2.1 Bakgrund, arbetsområden och projekt

JRC bedriver forskning inom skydda av samhällsviktig verksamhet (CIP) vid Institute for Protection and Security of Citizens. De har utvecklat en ICT-Elkraftsystemmodell som kopplar kontrollen av elkraftsystemet med det fysiska elkraftsystemet, vilket ger operatören information om störningar och avbrott. De utvecklar även en plattform för att illustrera kaskadeffekter, GRASP, som är baserad på en ekonomisk input-output modell. Denna plattform är tänkt för Europeiska eller nationella analyser. Slutligen stödjer de även ett projekt i samarbete med Politecnico di Milano och Lombardo-regionen som går ut på att kartlägga beroenden mellan tillgångar, men inkluderar bara första ordningens effekter och inte kaskadeffekter som uppstår på grund av andra eller högre ordningens beroenden mellan tillgångar eller aktiviteter.

### 3.2.2 Lagstiftning, ramverk och riktlinjer

Det existerar ingen lagstiftning, ramverk eller riktlinjer på den Europeiska nivån vad gäller konsekvensanalys på samhällsnivå. Vidare har JRC ingen information om liknande aktiviteter i medlemsländerna. Initiativet DG ECHO har 2011 års riskkartläggning av alla medlemsländerna, men den tar inte explicit hänsyn till alla samhällssektorerna.

### 3.2.3 Metoder och verktyg

På den Europeiska nivån är det ett initiativ som är pågående, nämligen ett europeiskt nätverk för flygledning. Denna adresserar dock inte konsekvenser, varken direkta konsekvenser av händelser eller kaskaderande effekter.

### 3.2.4 Datainsamling och spridning av resultat

Det finns ingen direkt insamlad eller tillgänglig data. De nationella riskkartläggningarna inom DG ECHO är på en hög nivå och konfidentiell till medlemsländerna. Endast störningar och olyckor vid industrianläggningar under Seveso-direktivet samlas in och är tillgängligt för medlemsländerna. Generellt adresserar data inte kaskaderande effekter.

### 3.2.5 Lärdomar och framtidsplaner

Inga lärdomar kom fram under intervjun, förutom MARS-databasen som beskriver olyckor vid Seveso-anläggningar i Europa, men som inte innehåller någon beskrivning av konsekvenser på samhällsnivå.



## 3.3 DHS samt NISAC, USA

### 3.3.1 Bakgrund, arbetsområden och projekt

Department of Homeland Security (DHS), och mer specifikt avdelningen Office of Cyber and Infrastructure Analysis (OCIA) (tidigare Homeland Infrastructure Threat and Risk Analysis Center, HITRAC, som bildades 2006), har under senare år fokuserat mer på konsekvenserna av störningar och kritiska infrastrukturer jämfört med tidigare som handlade mer om terrorism och sannolikhetsbedömningar (med anledning av 9/11) av hot. Orkanen Katrina år 2005 hade en stor inverkan på inriktningen och numera är det en mycket tydligare all-hazard-inriktning för arbetet inom området. I stort tar OCIA fram analyser inom områdena:

- 1) Steady-state analyser (t.ex. hur hot såsom orkaner och översvämningar påverkar samhället)
- 2) Breda tvärspektoriella infrastrukturanalyser, med försök att fånga effekterna av ömsesidiga beroenden på en något högre analysnivå, samt
- 3) Snabbanalyser (t.ex. om en faktisk orkan närmar sig USA och effekterna det får ur ett mer operativt perspektiv).

DHS har även ett prioriteringsprogram för kritisk infrastruktur där de försöker identifiera infrastrukturer som uppfyller vissa kritiska tröskelvärden. Detta genomförs på en hög nivå där olika stater nominerar infrastrukturer och där NISAC (se beskrivning nedan) och andra laboratorier hjälper dem att ta reda på konsekvenserna som kan uppstå om infrastrukturen utsätts för påfrestningar. DHS sammanställer sedan en lista som används för finansieringsbidrag för att säkra infrastrukturerna. DHS genomför även prioriteringar för organisationer och funktioner under en händelse för att försöka ta reda på vilka som är de kritiska elementen. De inser problematiken med och har börjat arbeta med att kritiskhet är i hög grad kontextberoende (t.ex. för vissa händelser såsom terrorism så kan en stor sportstadium vara mest kritisk medan vid steady-state kan en elkraftstation vara mest kritisk). DHS försöker även arbeta på en operationell nivå med andra federala organ (t.ex. FEMA) för att hjälpa dem att förstå risker och specifika frågor kopplat till nationens säkerhet i relation till deras ansvarsområde. I storleksordningen 28 000 människor arbetar inom DHS.

USA är indelat i totalt 16 sektorer, varvid DHS endast arbetar med de civila sektorerna (inte de militära såsom Defense industrial base som tillhör Department of Defense), dvs. prioriterar de 5-6 sektorer som kan anses vara ryggraden i civilsamhället (transport, kommunikation, elkraft, vatten, hälso- och sjukvård, räddningstjänst, och kommersiella anläggningar).

Ett helt avgörande stöd för DHS i arbetet enligt ovan är National Infrastructure Simulation and Analysis Center (NISAC). NISAC bildades 1999 som ett samarbete mellan Sandia och Santa Fe National Laboratories (dvs. innan HITRAC) och pekades senare ut genom Patriot Act från 2001 att de skulle vara ett center of excellence inom området modellering och simulering av kritisk infrastruktur åt DHS. NISAC har bland annat varit involverat och gjort analyser under händelser såsom Katrina, BP oljeutsläppet och pandemiscenario (dock ej epidemiologiska studier, som genomförs inom Center for Disease Control). NISAC består således av personal från både Los Alamos National Lab och Sandia National Labs, som är nationella laboratorier för Department of Energy (DoE) (dvs. federala laboratorier). Det är dock privata entreprenörer som förvaltar laboratorierna. Därmed är de personer som arbetar där privat och inte offentligt anställda. I huvudsak kan de ses som privata entreprenörer men som endast arbetar åt de federala myndigheterna (dvs. ej på den privata marknaden). I storleksordningen 20-30 personer heltidsarbetar och 10-20 personer deltid arbetar vid NISAC, de senare utgör olika stöd- och kompetenspersoner som tas in från andra delar av laboratorierna beroende på vilka frågeställningar som ska besvaras och därmed vilken expertkompetens som behövs (varje laboratorium har totalt ca 10 000 anställda).

NISAC måste ständigt vara noga med att välja ut vilka frågeställningar som faller inom ramen för centret och vilka som faller utanför. I början studerade NISAC endast på händelser innanför USAs gränser, på senare år har de dock även börjat studera gränsöverskridande problem (eng. cross-border), t.ex. inom försörjningskedjor och energiområdet.

NISACs arbete kan generaliseras till tre huvudområden:

- 1) Analyser av ömsesidiga beroenden (Interdependencies) och kaskadeffekter
- 2) Analyser av försörjningskedjor (Supply chain)
- 3) Ekonomisk analys, t.ex. ekonomiska konsekvenser av fallerande infrastrukturer

I huvudsak har det varit två stora skiften under de senaste två decennierna; a) Från terrorism till all-hazard och b) från skydd/säkerhet till resiliens (konsekvenshantering, anpassning och återhämtning). Dessa skiften har inte i någon större grad påverkat NISAC och deras förmåga utan snarare hur DHS diskuterar och använder resultaten. Vidare har NISAC gått från en mer operationell/taktisk nivå till en mer strategisk nivå över åren. Tidigare genomförde NISAC även främst analyser som fokuserade på hot och direkta konsekvenser av händelser såsom orkaner. Nu är analyserna mer framåtlutande, som t.ex. åldrande infrastrukturer och klimatförändringar, vilket i förlängningen kan påverka arbetet som NISAC är ombedd att utföra.

Att NISAC ligger som en separat enhet från DHS anser de vara en viktig framgångsfaktor för USAs arbete inom området. Det har funnits misslyckade försök att lägga liknande arbete som NISAC utför under en myndighet (t.ex. Risk management and analysis group som tvingades läggas ner av kongressen). NISAC säkerställer t.ex. kontinuitet av expertis i jämförelse med den höga personalomsättningen som råder vid DHS samt att arbetet naturligt faller inom ramen för den federala forskningsfinansieringen och organisationen. Då NISAC inte är ett privat företag, kan de arbeta inom alla sekretessnivåer och hantera olika typer av känslig information. Vidare är de inte en myndighet och kan säkerställa genom non-disclosure avtal att data de samlar in inte kommer att användas t.ex. i regleringssyfte eller delas till andra aktörer (som de poängterar är av mycket stor vikt för att få in data från privata aktörer). För att säkerställa relevans för deras arbete kan NISAC inte endast arbeta isolerat utan behöver vara bryggan mellan industrin och myndigheterna. De anser att det är en mycket svår kommunikationsuppgift att försöka överbrygga detta glapp till politiker och beslutsfattare och även att förstå och verka inom tidslinjen för deras beslutsramar (t.ex. under N1HI-pandemin var NISACs analysresultat klara först efter beslut redan tagits, och som dessutom i stort motsade de beslut som tagits). Det är kritiskt att avväga analyserna så att de passar dessa tidslinjer samt kommuniceras i ett mindre akademiskt format. I denna kommunikation fungerar DHS som en nödvändig brygga mellan NISAC och andra myndigheter.

NISAC existerar endast på den nationella nivån och liknande initiativ finns ej på den statliga eller lokala nivån. Dock finns det lokala initiativ som har liknande inriktning som NISAC, t.ex. universitet i staten Louisiana inom sårbarheter för orkaner och i New York med "#Center for Urban Science and Progress" som har ett visst infrastrukturintresse. Det finns dock inte mycket arbete inom området på statlig och lokal nivå som DHS och NISAC känner till. Det som finns är mer fokuserat mot traditionell hotmodellering (t.ex. jordbävningar, orkaner, översvämningar) och adresserar mer specifika loka problem. NISAC samarbetar med en del universitet och center of excellences (t.ex. CREATE som genomför ekonomisk modellering vid University of Southern California och inom livsmedel med personer från University of Utah). Det finns även informella samarbeten, t.ex. mellan anställda på NISAC och deras forna handledare vid universitet, men det finns inga formella mekanismer utan bygger på en mer ad-hoc basis. DHS sponsrar dock sommarstudenter från olika universitet för att kunna arbeta och lära vid NISAC.

### 3.3.2 Lagstiftning, ramverk och riktlinjer

USAs samhällsviktiga verksamheter (critical infrastructures) är indelade sexton olika sektorer och där ett övergripande ramverk finns, den s.k. National Infrastructure Protection Plan (NIPP) (se referens DHS (2013)), som behandlar hur arbetet ska organiseras inom sektorer och mellan sektorer, t.ex. olika typer och konstellationer av samverkansgrupper, samt vilka myndighet som har huvudansvar för respektive sektor kallad National Infrastructure Protection Plan (NIPP) (se referens DHS (2013)). För varje sektor finns det även nedbrutna sektorsspecifika planer (SSP) utifrån NIPP (se referens DHS (2010)). Innehållet i dessa omfattande planer går ej närmre igenom här, men kan utgöra värdefull information att lyfta in i arbetet med skydd av samhällsviktig verksamhet. För en del av sektorerna (ca 5-6) har DHS huvudansvaret, men arbetet försvåras av att DHS i sitt arbete är inne på andra sektorsmyndigheters arbetsområden och anses ibland lägga sig i arbete som inte "borde" tillhöra DHS.

Viktigt att poängtera är att ingen av de utpekade myndigheterna med huvudansvar inom området skydd av samhällsviktig verksamhet är reglerande (t.ex. är reglerande myndighet för kärnkraftsindustrin Nuclear Regulatory Commission men ligger under DHS inom CIP-området i enlighet med NIPP).

Det finns inga direkta lagar inom CIP-området som går bortom de nationella och statliga nivåerna. Det finns inga lagar eller regleringar som tvingar lokala och privata aktörer att arbeta med skydd av samhällsviktig verksamhet (förutom den normala reglerande lagstiftningen), utan måste genomföras inom ramen för privat-offentlig samverkan. Det var en Executive presidential order under president Bush som slog fast att alla myndigheter skulle arbeta med NIPP. President Obama gav senare en ny Executive order för uppdatering av NIPP. Eftersom NIPP har presidentiell auktoritet och är kopplad till Homeland Security Act så binds de federala myndigheterna till arbetet, men inte de statliga eller lokala myndigheterna eller de privata aktörerna. På nationell federal nivå är arbetet således tvingande medan på alla andra nivåer är arbetet frivilligt. På nationell strategisk nivå finns det även tillgång till finansiering för att stödja NIPP-arbetet genom t.ex. genom FEMA-finansiering. På lokala nivåer finns det mest arbete inom områden såsom evakueringsplanering, planer för räddningsinsatser och planer för återhämtning. Vissa av dessa planer är framtagna i samarbete med myndigheter (t.ex. FEMA) men det finns ingen NIPP eller SSP på statlig eller lokal nivå. Det är dock endast under senare tid som USA har börjat undersöka infrastrukturers resiliens och problem med ömsesidiga beroenden (tidigare mest fokuserat på säkerhetsfrågor). På statlig och lokal nivå finns troligen inga finansieringsmöjligheter för denna typ av arbete.

### 3.3.3 Metoder och verktyg

NISAC har under det senaste decenniet utvecklat och upprätthållit en mängd olika simuleringsmodeller, metoder och verktyg, längre ned återges endast en del av dessa (för olika NISAC modeller, se t.ex. <http://www.lanl.gov/programs/nisac/cipdss.shtml>) men först ges en kort översikt över NISACs modellering och simuleringsarbete. NISACs modeller kan strukturera i tre huvudgrupper:

- 1) Snabba modeller med lägre upplösningsgrad som kan användas i operationellt syfte
- 2) Halvsnabba modeller med högre upplösningsgrad och som kräver längre simuleringstider
- 3) Långsamma modeller som används för att undersöka och förstå problemställningar (kan ta upp till flera månader till år att sätta upp modellen, genomföra simuleringar och analysera resultaten).

Enligt NISAC handlar det om att välja rätt verktyg för problemställning (t.ex. om det är för operationellt syfte, träning eller övning). De är väldigt noga med att understryka att *ett verktyg utgör inte en förmåga*. Människor utanför NISAC och OCIA tenderar att se NISAC som ett "stort datorprogram", som man kan stoppa in frågor i ena ändan och ut kommer ett svar – så är ej fallet. NISAC anser att det är mycket

kraftfullt att ha olika typer av modeller, t.ex. modeller som kan köras med mindre information, och som naturligtvis ger mindre exakta resultat, men kan åtminstone användas för att ge indikativa estimat för att informera operationella beslut.

För att lösa ett givet problem använder NISAC alltid en uppsättning av olika verktyg och modeller samt analytiker som vet hur verktygen och modellerna kan användas (avseende deras styrkor, begränsningar, validitet, etc.). Det är *alltid kombination data-verktyg-analytiker som måste fungera tillsammans* för att lösa ett problem – *inte ett program i en dator*. En modell är endast en pusselbit, en poäng som NISAC ständigt måste upprepa till folk utifrån. Problemet med ”en modell” är att den tenderar att endast passa en frågeställning och om en annan fråga ställs blir modellen ogiltig. Vid tidigare kriser har de varit tvungna att justera och modifiera modellerna för att kunna få ut användbara resultat för beslutsfattande. Vidare, modellerna har dessutom väldigt olika detaljeringsnivåer; t.ex. har infrastrukturmodellerna relativt hög detaljeringsnivå medan de ekonomiska modellerna har väldigt låg detaljeringsnivå.

I början utvecklade NISAC rimliga hotscenario (hazard scenarios) internt men under de senaste åren har de initierat mer samarbete med t.ex. FEMA, andra delar av DHS, samt regional och lokala aktörer för att utveckla scenario som är vettiga för dem och hjälper dem i deras planeringsarbete. Inom detta arbete har de ofta diskussioner kring vilka scenario som bör tas i beaktning, dvs. titta på mer allvarliga händelser med låg trolighet eller scenario med lägre allvarlighetsgrad men högre trolighet. Under senare tiden har de även börjat använda mer ”troliga” scenario, då vid användandet av ”maximala-av-maximala” tenderar att människor resignerar inför problemet. Vidare anser de att det är svårt att adressera resiliens, då system är byggda för en viss hotnivå och det är enklare att gå framåt i mindre inkrementella steg för att gynna den långsiktiga evolutionen.

**CIP-DSS:** Critical Infrastructure Protection Decision Support System är från perioden 2004-2007 när modellen utvecklades med finansiering från DHS. CIP-DSS används inte i lika stor omfattning längre. Det är dock en modell med låg upplösning som kan köras en mängd gånger snabbt och därmed är användbar i ett operativt syfte. Modellen är en system dynamics modell – som passar väl till mer högnivå och mer kvalitativa slutsatser, snarare än kvantitativa slutsatser. Drivkraften bakom modellen är att få till en stor system-av-system modell, som tar en viss begränsad hänsyn till infrastrukturernas funktion och beroenden samt hur kaskaderande effekter kan uppstå. Sedan denna modell togs fram har fokus svängt över till mer detaljerade infrastrukturmodeller och modellering av specifika beroenden (t.ex. deras elkraftsystem- och vattenförsörjningssystemmodeller). Anledningen är att CIP-DSS är ibland för abstrakt och generaliserad, den kan inte användas för att peka ut en specifik kritisk anläggning – vilket är mer den typ av frågeställningar som DHS har ställt från 2008 fram till idag. Därmed behövdes mer precisa modeller – vilket har lett till att de kan i nuläget högst modellera två till tre samberonde system och beroenden sinsemellan. Nuförtiden sätter de i större utsträckning manuellt upp mer högupplösta modeller för att besvara specifika frågor. Det är därmed nödvändigt att ha en analytiker ”i loopen” för att kunna genomföra rimlighetskontroller snarare än att ha mer automatiska modeller (givet den höga graden av osäkerhet som dessa modeller är behäftade med).

**Enskilda ingenjörsmässiga infrastrukturmodeller:** NISAC har modeller för de nationella infrastrukturerna: elkraftsystem, vattenförsörjningssystem, telekommunikationssystem (under utveckling), transportsystem, naturgassystem, finansiella system, kemiska försörjningssystem, livsmedelsförsörjning, och jordbruksmodeller. De ingenjörsmässiga modellerna som NISAC använder kan antingen vara internt utvecklade, kommersiella eller open-source. De försöker få till en ”hävstångseffekt” genom att använda kommersiella programvaror, men generellt finns det stora luckor i dessa programvaror som kräver en del internt utvecklingsarbete. Till exempel för den nationella gasinfrastrukturen finns det en skäligen god, men inte perfekt, kommersiellt modell kallad GPC (Gas pricing competition model) som NISAC använder.

Men för till exempel den nationella petroleuminfrastrukturen (raffinaderier, transmissionsledningar, etc.) finns det ingen kommersiellt modell, vilket lett till att NISAC själv fått utveckla en som de bland annat använt för att analysera konsekvenserna av jordbävningar.

**Finansiella system:** NISAC undersöker även, och försöker förstå, hur störningar kan påverka det finansiella systemet och effekter av sådana störningar. Den här typen av modell är en kombination av flera olika typer av modeller, t.ex. system-dynamic modeller, ingenjörsmässiga modeller, försörjnings-systemsmodeller eller agentbaserade modeller (där agenter agerar utifrån en viss information, eller bristen på information, och hur systemet fungerar i sin helhet kan analyseras).

**Ekonomiska modeller:** NISAC använder både ekonomiska Input-Output modeller (IO) samt General Equilibrium modeller (GEM). För snabba simuleringar använder de IO-modeller (t.ex. för annalkande hot såsom orkaner) och när det finns mer tid tillgängligt använder de GEM-modeller eller en typ av system-dynamics modeller. När de verkligen vill gå in i detalj och förstå hur systemet fungerar använder de även agent-baserade modeller (som är modellerings- och simuleringsmässigt mycket mer kostsamma modeller).

**Hälso- och sjukvårdssystem:** NISAC har även en modell som kan spåra hur människor förlyttar sig genom ett sjukhusystem. Denna modell har använts för att besvara frågeställningar såsom "Hur många patienter kan behandlas vid ett sjukhus och hur kan patienter omdirigeras till andra sjukhus?" (den senare frågeställningen kan besvaras genom att koppla en transportmodell samt inkludera vilka faciliteter de olika sjukhusen har, t.ex. avdelningar för behandling av brännskador). Den används för att utvärdera hur det övergripande sjukhusystemet skulle kunna svara på en katastrof. NISAC har data för de flesta större sjukhusen, t.ex. antal sängar, hanteringsförmåga, etc.

**Beroendemodeller:** Ett angreppssätt för att modellera ömsesidiga beroenden (eng. interdependencies) är att ha väldigt detaljerade infrastrukturmodeller och detaljerad information om beroendena, vilket generellt är svårt att få tillgång till data för. Ingen vet egentligen hur olika kritiska infrastrukturer är sammankopplade på komponentnivå (t.ex. vilken specifik elkraftsstation försörjer ett utpekat vattenreningsverk) och hur buffertkapaciteterna ser ut (t.ex. reservkraftverkskapacitet). Ett annat angreppssätt är en mer system dynamics modellansats där de specifika beroendena inte modelleras utan snarare anges på en mer generell nivå, t.ex. telekommunikationsinfrastruktur generellt beror av elkraftsinfrastruktur – vilket kan användas för att studera storskaliga störningar och hur ett fel i en infrastruktursektor kan sprida sig till andra infrastruktursektorer (dock inte på en anläggnings-/komponentnivå). För den här typen av modelleringsansats är antaganden om beroenden i hög grad baserad på olika anläggningars geografiska närhet till varandra. Huvudproblemet med modeller som tar hänsyn till ömsesidiga beroenden är att få tag i data. Data är definitivt ett stort problem anser de, NISAC har kännedom om hur system generellt är sammankopplade och vilka generella backuplösningar som existerar – det är dock mycket svårt att uttala sig om vilken generator eller anläggning som faktiskt kommer att falla och vilka backuplösningar som då även riskerar att falla.

**Hotmodeller:** Dessa typer av modeller fokuserar på att koppla geospatial anläggningsdata med hot som har geospatiala karakteristika, oftast genom att använda s.k. shape-files (ett GIS-format). NISAC har gjort mycket modelleringsarbete för jordbävningar, orkaner (samt svallvågsmodeller kopplat till orkaner), översvämning och terroristhot som de använder för att simulera olika hots påverkan på infrastrukturer. Dessa verktyg var ursprungligen utvecklade med främsta syftet att få ett grepp om den generella risknivån på den regionala nivån (genom olika myndigheter såsom FEMA) och inte för detaljerade analyser. NISAC har sedan dess utvecklat en del algoritmer för att öka detaljeringsgraden i modellerna i syfte att bättre kunna uttala sig om vilken inverkan ett hot har på olika anläggningstillgångar (t.ex. genom att lägga till

s.k. fragility modeller för anläggningstillgångarna). Dessa hotmodeller kan användas för att analyser hur t.ex. en orkan kommer att påverka infrastrukturerna och sedan koppla en ekonomisk modell för att uttala sig om vilken konsekvenser som kommer att uppstå.

**Situational awareness tool:** Detta är en typ av GIS-applikation som NISAC håller på att utveckla där olika sektorers anläggningstillgångars (t.ex. elkraftsystem och järnvägssystem) geografiska placering kartläggs, dock finns det inga modeller av infrastrukturernas funktion med utan är helt anläggningsbaserad. Verktøget kan användas för att analysera vilka anläggningstillgångar och infrastrukturer som blir påverkade vid geografiskt orienterade hot, t.ex. orkaner eller översvämningar. Verktøget används just nu mest vid NISAC, men DHS har även använt det en del, Vanligast är dock att DHS ber NISAC utreda en specifik frågeställning. Både NISAC och DHS anser att det alltid måste vara en kombination, då det alltid kommer att behövas en viss kunskap och förståelse för att använda verktøget. Själva GIS-gränssnittet kan man lära sig inom 15 minuter, dock krävs det en helt annan kunskapsnivå för att förstå inverkan på t.ex. elförsörjningen. DHS och NISAC utreder vid tillfället för intervjun vilka nivåer av verktøget som är lämpligt på respektive ställe (dvs. vad bör stanna vid NISAC och vad kan användas av DHS utan att det genererar felaktiga resultat). Ibland har en form av "hybrid" använts, där NISAC tar fram hur ett hot kommer att påverka ett geografiskt område och sedan kan DHS använda Situational Awareness Tool för att få en idé om vilka infrastrukturer som kommer att drabbas. Verktøget har ej ännu tagits i bruk, men har potentialen att bli ett kraftfullt verktøget. Ett syfte med verktøget är att mer kraftfullt kunna kommunicera med beslutsfattare (istället för det mer traditionella sättet genom rapporter).

**Analystyper:** NISAC har genomfört en stor mängd scenariobaserade analyser (dvs. kopplat till ett hot) men också mer sårbarhetsorienterade analyser såsom t.ex. "N-k"-analyser (där k anger antalet fallerade komponenter utav infrastrukturens totala N komponenter). De har också studerat problem relaterade till åldrande infrastrukturer och hur klimatförändringar tillsammans med förändrande användamönster kan ge upphov till ökade påfrestningar på infrastrukturerna (dvs. mer av en framtidsutsikt). Scenarioanalys utgör dock huvuddelen av analyser som NISAC genomför, eftersom de är enklare att kommunicera och förstå för externa parter. För de allra flesta analyserna är fokus kring hur populationen påverkas av störningar (sjukdomar, skadade, etc.), vilket kan användas för att informera t.ex. sjukvårdssektor men även för DHS avseende t.ex. temporärt boende och temporär vattenförsörjning (dvs. mer långsiktiga konsekvenser och i termer av vilka förnödenheter för att täcka människornas basala behov).

**Validering av modeller:** För samtliga modeller som utvecklas är det generellt svårt verifiera och validera dessa, då NISAC generellt inte har tillgång till data (eller ens existerar) för att kunna genomföra verifiering och validering. För t.ex. bränsleförsörjningsmodellen kunde man genom att hämta data från en mängd olika källor komma fram till hur systemet troligen fungerar eftersom antalet frihetsgrader för hur systemet borde kunna fungera blev begränsat – ingen bra validering men ger åtminstone rimlighetsgränser. När storskaliga händelser inträffar så jämför NISAC sina resultat från modellerna med de empiriska data för att förbättra modellerna. De arbetar även med infrastrukturägare för att validera modellerna, speciellt avseende återställning/återhämtning och vad som faktiskt blev skadat i infrastrukturerna på grund av påfrestningen. De poängterar att vid parametrering och validering av modellerna är det viktigt att få så mycket återkoppling med industrin som möjligt.

DHSs åsikt är att det är bättre att ha en modell som är användbar än absolut korrekt, att få en absolut korrekt modell är omöjligt [Intervjuarens kommentar, jämför med: "Essentially all models are wrong, but some are useful" (Box, 1976)].

### 3.3.4 Datainsamling och spridning av resultat

NISAC - Data är vår akilleshäls. Runt 85 % av infrastrukturerna ägs och drivs av privata aktörer, dvs. myndigheterna måste verkligen arbeta med dessa för att kunna få tillgång till data och se till att skapa incitament för de privata aktörerna att arbeta med problemen inom området. Från vissa sektorer är det enklare att få data och samarbeta med, medan för vissa andra sektorer är det svårare - t.ex. den finansiella sektorn (då all data är ägarskyddad).

Det är också riskfyllt att använda reglerande myndigheter för insamling av data, därmed ligger mycket av arbetet under DHS (dvs. i ett försök att hålla isär reglerande och samarbetsmyndigheterna tillräckligt för att få det att fungera). Även om NISAC inte är på något sätt involverad eller stödjer det reglerande arbetet är vissa privata företag ändå rädda för att ge ut data (då det skulle kunna användas mot dem). NISAC har även tydlig känt av "säkerhetsproblemspendeln" under deras år i existens, som har svängt från att all information ska skyddas till ett mer öppnare klimat med att dela och sprida information.

Då NISAC inte alltid får den data de skulle vilja ha, har de fått utveckla algoritmer och uppskattningar baserat på generella ingenjörsmässiga bedömningar och principer. Med detta tillvägagångssätt kan grundläggande frågor besvaras även om data saknas – det är dock inte på den detaljeringsnivå som de skulle önska (men åtminstone kan användbara resultat fås). Generellt har DHS och NISAC lärt sig mycket av tidigare inträffade händelser, såsom orkanerna Sandy och Katrina. Genom att studera dessa typer av händelser har en mängd icke-uppenbara beroenden kunnat identifieras (dvs. sådana som är svåra att identifiera på förhand). Om studier görs av specifika anläggningar är det relativt enkelt att ta reda på kapaciteten för buffertar givet beroendena. Det är dock mycket svårare att generalisera detta till alla andra anläggningar i landet, till och med endast för ett storstadsområde.

Data är generellt enklare att få tillgång till när det gäller transmissionsnivåerna för infrastrukturerna (dvs. den högsta nationella nivån) medan det för distributionsnivåerna är mycket svårare (dvs. den lägsta lokala nivån). Men inte ens anläggningstillgångar på transmissionsnivån är alltid georefererade (dvs. saknar geografiska koordinater för anläggningstillgångarna). En generell trend är att allt fler kommuner lägger in deras data i GIS-format, vilket gör det enklare att få tillgång till (historiskt har denna typ av information arkiverats endast i pappersformat).

Den mesta data som finns tillgänglig via internet, och som NISAC även använder sig av, är ren data och analysmetoderna som då står till buds är rent data-drivna (till skillnad från simuleringsdrivna). NISAC har som mål att kunna koppla denna typ av data med modellerings- och simuleringsmöjligheter för att kunna nå mer kraftfulla resultat.

Resultaten från analyser som NISAC och DHS genomför sprids i nuläget inte till någon större krets. I huvudsak används de för DHS arbete, men de arbetar aktivt med att försöka sprida till en större krets. Utvecklingsresan i det här området har att först säkerställa kommunikationen mellan NISAC och DHS, sedan NISAC till övriga federala myndigheter, medan kommunikationen från NISAC och DHS till publika aktörer fortfarande är omoget. Det är dock inte säkert att denna kommunikation bör ligga under DHS eller NISACs ansvarsområde, en mer naturlig kanal skulle vara att sprida resultat genom de s.k. "private outreach programs" som är definierade i NIPP. NISAC genomför dock visst arbete med privata aktörer angående data och validering av modeller, men även om NISAC uppmärksammar om ett kritiskt beroende som företaget själva inte är medvetna om är det inte säkert att företaget kan göra något åt saken då det kanske inte ligger direkt i aktieägarnas intresse.

### 3.3.5 Lärdomar och framtidsplaner

NISAC och DHS anger att på ena sidan är det en utmaning att effektivt arbete inom ramstrukturen för politiker och beslutsfattare – att arbete med alla intressenterna anser de generellt vara en av de stora utmaningarna. På andra sidan är det en utmaning att få de kontakter som behövs för att få tillgång till nödvändig data. Ytterligare en utmaning är att utforma frågeställningarna och problemen i hanterbara storlekar – dvs. hitta russin i kakan, försök inte göra allt på en gång och börja inte med att bygga modellen som ska fånga allt.

NISAC har gått från att försöka modellera allt till att mer försöka besvara specifika frågor genom mer begränsade studier. Med tanke på datorkraftens utveckling kan det som inte är möjligt idag vara möjligt om bara några år – det är därmed en nödvändighet att bibehålla sin flexibilitet. Det skulle vara utmärkt att ha tillgång till perfekt data och att kunna modellera alla system och ömsesidiga beroenden samtidigt, men det är viktigt att acceptera att frågorna som man har ej säkert kan besvaras med högsta noggrannhet och upplösning. Det är därmed viktigt att försöka hitta vägar för hur man interpolerar och hittar substitut och nöja sig med lägre upplösning när det endast finns mindre än perfekt information tillgängligt. Vidare är det viktigt att förstå inom vilka tidsramar som en fråga måste besvaras, är det inom en timme, en vecka, eller flera år, eftersom detta starkt påverkar vilka typer av modeller och analyser som kan användas. Det är även av stor vikt att inse behovet av kompetens, inte endast vid framtagande av verktygen utan även under själva användandet – det är ett arbete som kräver fackkunniga och skickliga lag.

En lärdom som NISAC dragit, och som varit lyckosam, är att dela in NISAC i tre kluster: 1) Krishanteringsanalyser (analyser med väldigt kort tidsramar), 2) Strategisk analys (planering för framtida troliga händelser såsom orkaner, höjd vattennivå, torka, jordbävningar) samt 3) Utveckling av förmåga (underhålla och utveckla metoder och data för att kunna besvara frågorna som ställs idag och framöver).

Varje sektor har sin egna ansvariga myndighet. DHS har försökt att nå ut till vissa av de sektorsspecifika myndigheter, men de har oftast deras egen agenda och driver deras utveckling av förmåga i en riktning som inte nödvändigtvis överensstämmer med DHS önskemål (även om det kan var förståligt sett ur sektorsmyndigheternas perspektiv). Frågorna som DHS ställer till NISAC är antingen från DHS ledarskap eller från Vita huset (endast ett par lager mellan DHS och Vita Husets national security staff).

En annan nyckelutmaning är att utveckla kommunikationen i form av rapporter eller produkter: Vem ska det distribueras till? Hur ska distributionen gå till? Hur kommer granskningsprocessen se ut – hur säkerställs kvaliteten? Kommunikationen lämnas ofta till slutet, men det är viktigt att förstå mottagaren och det är enklare att få med dem i arbetet och man får med dem i ett tidigt skede (nyckelfaktor för att göra skillnad och nå framgång eller inte). Det är nämligen aldrig samma frågor som ställs, t.ex. var frågorna som ställdes för orkanen Katrina helt annorlunda jämfört med de som ställdes för orkanen Sandy. I någon mening så utkämpar man alltid det sista slaget. Det är därmed av stor vikt att ha en flexibel förmåga, som möjliggör både en reaktiv och proaktiv utveckling mot frågorna som ställs, förändringar av koncept (t.ex. säkerhet, till sårbarhet, till resiliens) och förändringar av beroendena till de tjänster som infrastrukturerna levererar.

Vidare är det viktigt att tillåta sig att gå längs fel väg och hamna i återvändsgränder. Inget som NISAC har gjort har varit helt och hållet slöseri med tid, då de lärt sig från misstagen och omförvandlat deras arbete. Men med nuvarande kunskap och gå tillbaka till åren 2001/2002 hade det definitivt varit beslut som tagits annorlunda (men en naturlig del av inlärningskurvan). I början av NISACs tid var DHS ganska omoget och det fanns ingen att sprida verktygen och resultaten till. Allteftersom DHS har mognat som



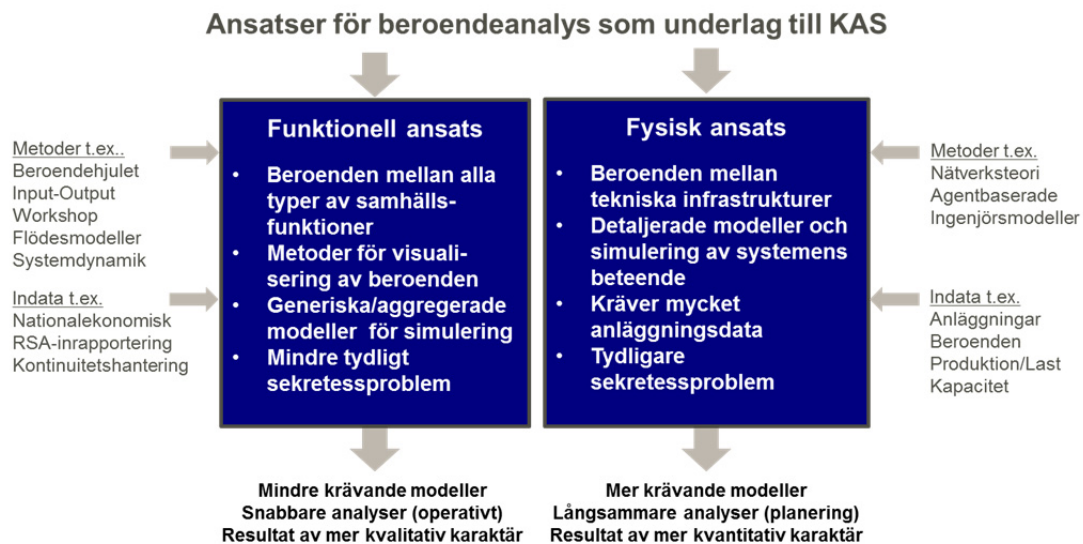
organisation har fokus till del skiftat mot att utveckla web-baserade verktyg. Produkterna från NISAC kommer dock alltid att vara mer kopplat till analys snarare än verktyg.

En annan utmaning att tackla är människorna som kritiserar NISACs och DHSs arbete. Eftersom de, i någon mening, genomför arbete och ställer frågor inom någon annans ansvarsområde. DHS har genomfört uppsökande verksamhet och försökt kommunicera att de har ett något annat fokus och problemformulering (dvs. kriser snarare än normal verksamhet) och att deras arbete ska ses mer som kompletterande än konkurrerande (t.ex. skulle FEMA inte sända ut mat och vatten om det är ett 15 minuter elavbrott, endast om det varar i dagar eller veckor – FEMA ska inte ingripa såtillvida lokala och statliga resurser är uttömda). Det är helt enkelt viktigt att hitta och kommunicera området man verkar inom.

En sista utmaning är att hitta människor med den rätta kunskapen och färdigheterna som kan arbete med frågor som rör skydd av samhällsviktig verksamhet (CIP). Det finns ingen utbildning eller examen i USA med inriktningen mot modellering och simulering inom området skydd av samhällsviktig verksamhet (förutom enstaka kurser som fokuserar mer på hanteringsidan av risk inom området, t.ex. George Mason University). Skydd av samhällsviktig verksamhet (CIP) är dock ett väldigt nytt begrepp, första gången det dök upp var i en Presidential Order från 1996. Det tar lång tid att träna människor så att de dels får de rätta tekniska färdigheterna men också för att de ska förstå området för att kunna utnyttja sina färdigheter, vilket nödvändiggör en stabil arbetsplats. Vid NISAC har de lyckats samla en mängd olika kompetenser med olika färdigheter som behövs för att svar på frågeställningarna inom området, t.ex. ekonomer, infrastrukturingenjörer, matematiker, beteendevetare och riskhanterare.

### 3.4 Diskussion och slutsatser

Med tanke på den stora mängd information som framkom under intervjuerna och komplexiteten som råder inom området skydd av samhällsviktig verksamhet är det inte helt enkelt att dra kortfattade slutsatser utan att riskera att intressant och värdefull information utlämnas. Perspektivet som valts är att försöka dra slutsatser från intervjuerna främst ur perspektivet konsekvensanalys på samhällsnivå. En övergripande slutsats som kan dras utifrån intervjuerna att det grovt finns två olika ansatser inom ramen för skydd av samhällsviktig verksamhet som kan användas som underlag till KAS, vilka vi valt att benämna med en *funktionell ansats* och en *fysisk ansats*, se Figur 3.1.



**Figur 3.1** Två olika ansatser för att genomföra beroendeanalyser som underlag till konsekvensanalys på samhällsnivå. (Metoder och indata som anges till respektive ansats ske ses som indikerande exempel, då t.ex. vissa metoder kan användas i båda ansatser samt att även data överlappar. Ibland används även hybrider av de två ansatserna).

Den funktionella ansatsen försöker på en mer generisk och aggregerad nivå beskriva och modellera beroenden mellan många olika typer av funktioner i samhället. Metoderna som framkom i intervjuerna var t.ex. TNO:s workshoppar och NISAC:s CIP-DSS, men tydligt att ej så många metoder finns inom denna ansats. Generellt handlar det om antingen identifiering, aggregering och visualisering av beroenden eller modeller som bygger på generisk data och förhållande om beroenden. Därmed är det troligt att sekretessproblematiken ej omnämndes i intervjuerna i samma omfattning i anslutning till denna ansats. Fördelen med denna metod är att det generellt handlar om mindre krävande metoder och datainsamling och som lämpar sig för snabbare analyser (som sedan kan ligga till grund för t.ex. operativa beslut). Resultaten är av mer kvalitativ karaktär, som ger fingervisningar om generella systemsvagheter snarare än användbar för att peka ut konkreta fysiska åtgärder.

Den fysiska ansatsen handlar om att identifiera och modellera beroenden främst mellan olika typer av tekniska infrastrukturer. Metoderna inom denna ansats är betydligt mer vanliga inom området skydd av samhällsviktig verksamhet, vilket även var tydligt från intervjuerna (t.ex. NISAC:s olika modeller av tekniska infrastrukturer och beroenden). Generellt handlar det om att skapa detaljerade modeller av infrastrukturer och deras beroenden. Detta är relativt krävande både modellerings-, kunskaps-, och data-mässigt och lämpar sig för mer långsiktiga analyser (som sedan kan ligga till grund för t.ex. planerings- och åtgärdsbeslut). Den höga detaljeringsnivån för modellerna är troligen också orsaken till varför sekretessproblematiken är större med denna ansats. Resultaten är av mer detaljerad kvantitativ karaktär och kan t.ex. användas för att peka ut fysiska kritiska komponenter och beroenden samt åtgärder riktade mot dessa.

Generella slutsatser och indikationer på viktiga ingångsvärden för arbetet med konsekvensanalys på samhällsnivå kan även dras utifrån intervjustudiens tematiska områden. Nedan återges dessa endast kortfattat i punktform, för djupare förståelse kring kontext och motivering rekommenderas det fullständiga intervjumaterialet i Bilaga 3.

### Lagstiftning, ramverk och riktlinjer

- I USA existerar National Infrastructure Protection Plan (NIPP) samt Sector Specific Plans (SSP) som främst definierar ansvarsområden och samarbetsformer, verkar dock endast på federal nivå och inte på statlig eller lokal nivå.
- I Holland existerar ingen övergripande lagstiftning inom området tvärssektoriella beroenden men Ministry of Security and Justice driver och koordinerar frågan.
- På den Europeiska nivån existerar ingen lagstiftning, ramverk eller riktlinjer kring KAS.
- I USA och Holland genomförs arbete inom ramen för skydd av samhällsviktig verksamhet rörande identifiering av kritisk infrastruktur, nationella och regionala risk- och sårbarhetsanalyser samt inomsektoriellt arbete.
- Infrastrukturers resiliens och inverkan av beroenden är ett relativt nytt synsätt.
- I nuläget finns relativt lite arbete som passar inom ramen för konsekvensanalys på samhällsnivå.

### Metoder och verktyg

- Finns en stor mängd metoder och verktyg inom området skydd av samhällsviktig verksamhet.
- Relativt få metoder existerar dock som adresserar konsekvensanalys på samhällsnivå.
- Ett verktyg inte en förmåga.
- Kombinationen data-verktyg-analytiker krävs, inte endast ett datorprogram.
- Modeller som utvecklas är generellt svåra att verifiera och validera.

### Datansamling och spridning av resultat

- Data är alltid en akilleshäls
- Merparten av samhällsviktig verksamhet ägs och drivs av privata aktörer (i USA ca 85%)
- Det är svårt att samla in data som behövs pga. sekretessproblematik, konkurrenssituationer, rädsla för att data ska användas i reglerande syfte, avsaknad av data samt svårt att hitta incitament och tydliga nyttan för aktörer att lämna ut data.
- Det krävs därmed tydliga incitament och lösning av sekretessproblematiken för både offentliga och privata aktörer att medverka i arbetet med SSV (t.ex. lagar, finansiering, sekretessavtal).
- Former och vägar för spridning av resultat fortfarande i sin vagga.

### Lärdomar och framtidsplaner

- GIS-plattform för informationsdelning och visualisering av resultat verkar vara en framgångsrik väg för att få aktörer intresserade samt ett bra sätt att informera politiker och beslutsfattare.
- Problem med att vissa aktörer inte passar inom systemet för krishanteringsarbetet.
- Acceptera att frågorna man har ej kan besvaras med högsta noggrannhet och upplösning.
- Viktigt att hålla isär reglerande och samverkande myndigheter.
- För en lyckosam privat-offentliga samverkan krävs det förståelse och hänsyn att de har olika mål.
- En viktig del för framtida arbete med skydd av samhällsviktig verksamhet är att undersöka och förstå vilken detaljeringsnivå och kommunikation som behövs inom de olika områdena.
- Brist på människor med rätt kunskap inom området, vilket innebär att utbildningsinsatser behövs.
- Både DHS/NISAC, TNO och JRC ansåg att arbetet fortfarande fragmenterat och det är viktigt att lärdomar sprids bättre mellan länder och sektorer.



## 4 Avstämning av tankar för utveckling av KAS

För att få kommentarer och ingångsvärden kring resultat och tankar i föreliggande rapport från samhällsaktörer genomfördes den 14 januari 2015 en workshop vid MSB i Stockholm. Medverkande vid workshopen var 8 representanter från centrala myndigheter, 2 från landsting, 2 från länsstyrelser samt 3 från kommuner. Nedan presenteras frågeställningar som lyftes vid workshopen och en sammanfattning av de reflektioner och svar som kom in från deltagarna. Vid workshopen presenterade resultat från Kapitel 1 och 3 samt ett utkast till de tankar som återfinns i Kapitel 1 som ingångsvärde till diskussionen kring frågeställningarna.

### Vad är er tolkning av begreppet konsekvensanalys på samhällsnivå (KAS)?

Att beroenden är en viktig utgångspunkt för KAS verkade samtliga deltagarna hålla med om.

Deltagarna tyckte dock att tolkningen av begreppet KAS är något oklart. Vad menas t.ex. med samhällsnivå, är det på lokal, regional eller nationell nivå – eller ges samhällsnivån av analyskontext?

Vidare tyckte de att det var olika tolkning av KAS om det var för ett geografiskt område eller för ett sektoriellt område. Som vi (författarna) ser det kan KAS inte var sektoriell utan måste alltid vara tvärsektoriell i någon mening.

Vidare ansåg deltagarna att begrepps användningen inom området behöver tydliggöras. Det är t.ex. inte enkelt att direkt förstå vad som avses med begrepp såsom ”djupare analyser” eller ”högre ordningens konsekvenser”, vilka användes för att beskriva området.

Deltagarna kopplade även till samhällsviktig verksamhet (SVV) som en delmängd av KAS. Där framkom det åsikter om svårigheten att identifiera vad som är SVV, detta kan ju variera över tid eller vara hotberoende. De såg även behov av kriterier för vad som utgör SVV. På nationell nivå pågår det just nu ett projekt för just kriterier för SVV.

### Finns det behov att genomföra KAS?

Samtliga av deltagarna såg ett tydligt behov och vikten med att genomföra KAS. Deltagarna tog även upp komplexitetsproblemet med KAS, ju längre man går i spridningskedjan desto mer komplext och svårhanterligt blir det. Här uttrycktes ett starkt behov av metodstöd för att kunna analysera dessa komplexa beroendeförhållanden. Vidare behövs det en samordning av begrepp och en röd tråd inom SVV och krishantering i stort, t.ex. hur kopplar olika aktiviteter med varandra och kan de stödja varandra.?

### Till vilken omfattning genomför ni KAS?

Enligt en del av deltagarna görs det en del inom KAS, dock utanför själva RSA-arbetet då det genomförs av andra instanser än där RSA-arbetet genomförs. Sådant arbete borde kanske i förlängningen integreras bättre i RSA. Omfattningen för KAS ansåg en del deltagare bero på vilken samhällsnivå den genomförs men även för vilken aktör.

### Vad skulle krävas av er för att få fram beroendedata för KAS från offentliga såväl som privata aktörer?

*Vilken data har ni?* Det är olika tillgång till data som kan användas till KAS beroende på aktör, vissa aktörer har mycket data som direkt skulle kunna användas men i andra fall handlar det om kunskap hos experter som skulle behöva omvandlas till data. En del verksamheter/sektorer har en mängd data men som av sekretesskäl inte kan spridas eller användas för KAS.

*Vad skulle ni kunna få fram?* Data finns troligen, men utnyttjas kanske inte just nu i RSA-spåret. Här är en problematik sekretess, vilken data går att utnyttja för arbetet. Det kanske kan behövas någon form av sekretessklassning av information (t.ex. behörighetsnivåer) för att kunna genomföra KAS-arbetet.

*Vad är utmaningarna?* Det finns problem med sekretess, även om aktörerna har data och använder den för KAS kan det vara svårt att sprida data och analysresultat vidare på grund av sekretesskäl. Anledning med skralt med beroendeanalyser och KAS i risk- och sårbarhetsanalyserapporterna kan bero dels på att äldre analyser, men kanske även att man anser denna information vara känslig och av sekretesskäl återges det inte i RSA-rapporterna. KAS och beroendeanalyser upplevdes generellt som ett komplext område, där en deltagare såg att ISO-standarden kring kontinuitetshandling kanske skulle kunna användas som stöd. Vidare såg deltagarna det viktigt att kunna ta del av andras resultat för att kunna uppnå KAS, vilket kommer att kräva någon form av system eller infrastruktur för informationsutbyte, vilken även behöver beakta problematiken kring sekretess. En praktisk utmaning är att tillgång till tid och pengar för genomförande är begränsat.

### **Har ni, i form av olika samhällsnivåer, olika behov av stöd för genomförande av KAS?**

Deltagarna gav uttryck för att behovet ser olika ut för olika samhällsnivåer, men att en gemensam grund och begreppsapparat efterfrågas. Vidare efterfrågas ett stöd för hur andra aktiviteter inom systematiskt säkerhetsarbete kan användas inom ramen för KAS. Det fanns även behov av stöd och metoder för att kunna omvandla kvalitativa svar till kvantitativ data. Deltagarna menade även generellt att det kommer krävas en ”top-down” styrning avseende form för data och kriterier för bedömningar, medan själva datainsamlingen bör generellt ske ”bottom-up” – trots allt är det på lokal nivå som konsekvenserna uppstår. En parallell drogs till Styrels-arbetet där en väl definierad systematik användes. Vidare bör KAS kunna användas såväl ur ett riskperspektiv, dvs. mer kopplat till sannolikhet och konkreta hot, som ur ett sårbarhetsperspektiv, dvs. mer kopplat till konsekvens, kontinuitet och resiliens.

Vidare framkom det även önskemål om att få till ett system för KAS där även kvalitetssäkring ingår, t.ex. vem som lämnat information och i vilken roll. Det framkom även ett behov att kunna presentera data och resultat på ett bra sätt, t.ex. visuellt för att kunna användas på ett intuitivt sätt för presentation till beslutsfattare eller i form av olika aggregerade eller beräknade mått för att kunna greppa komplexiteten för de som utför analyserna. Vidare betonades vikten av att informationsflödet inte bara ska gå från lägsta till högsta samhällsnivå, utan det är mycket viktigt att det även finns återkoppling från högre nivåer till lägre – t.ex. kunna upplysa enskilda aktörer inom systemet om deras roll och viktighet i helheten. Vidare uttryckte vissa centrala myndigheter svårigheterna med att uppskatta samhällskonsekvenserna som kan uppstå om de ej kan utföra sin funktion, vilket tenderar att deras fokus inom RSA blir på organisationen snarare än ansvarsområdet. Här skulle ett framtida KAS-system kunna ge värdefull ingångsvärden till deras arbete kring samhällskonsekvenserna som uppstår vid bortfall av deras funktion.

### **Ytterligare inspel från en MSB rapport (MSB 767)**

Under hösten 2014 genomförde MSB en genomgång av 2013 års risk- och sårbarhetsanalyser samt fördjupande intervjuer med utvalda aktörer med syfte att ge återkoppling till myndigheternas redovisningar (MSB, 2104c). Temat för genomgången var samhällsviktig verksamhet vilket gör att en del resultat även är av intresse för diskussionen i föreliggande rapport. Nedan återges en del utdrag från rapporten som kompletterar eller styrker de åsikter som framkom under workshopen och som även tjänar som inspel till diskussionen i kapitel 1.

”Myndigheterna uttrycker olika åsikter avseende hur de upplever arbetet med att identifiera samhällsviktig verksamhet. Några [myndigheter] ser inga större problem med att identifiera [de samhällsviktiga]

verksamheterna men upplever att det är svårare att fortsätta arbetet efter identifieringsfasen. ... Andra myndigheter upplever att arbetet kan vara otydligt, komplext och omfattande.” (sid 14)

”Flera av myndigheterna använder andra analyser och identifieringsarbeten så som Styrel, pandemiplanering, civilförsvarsplanering och den nationella risk- och förmågebedömningen [för att identifiera samhällsviktiga verksamheter].” (sid 16)

”Det finns även länsstyrelser som ser behov av samordning mellan arbetet med skydd av samhällsviktig verksamhet, RSA, Styrel, totalförsvarsplanering och skyddsobjekt. En samordning bidrar till att skapa samsyn i frågorna och minskar dubbelarbete.” (sid 18) samt ”Flera myndigheter lyfter fram kopplingen till kontinuitetsfrågor” (sid 18)

”Därför finns ett stort behov av att fortsatt utveckla systematiken och samordningen av frågorna, samt att beskriva helheten med samhällsviktig verksamhet kopplat till det övriga krisberedskapsarbetet” (sid 23).





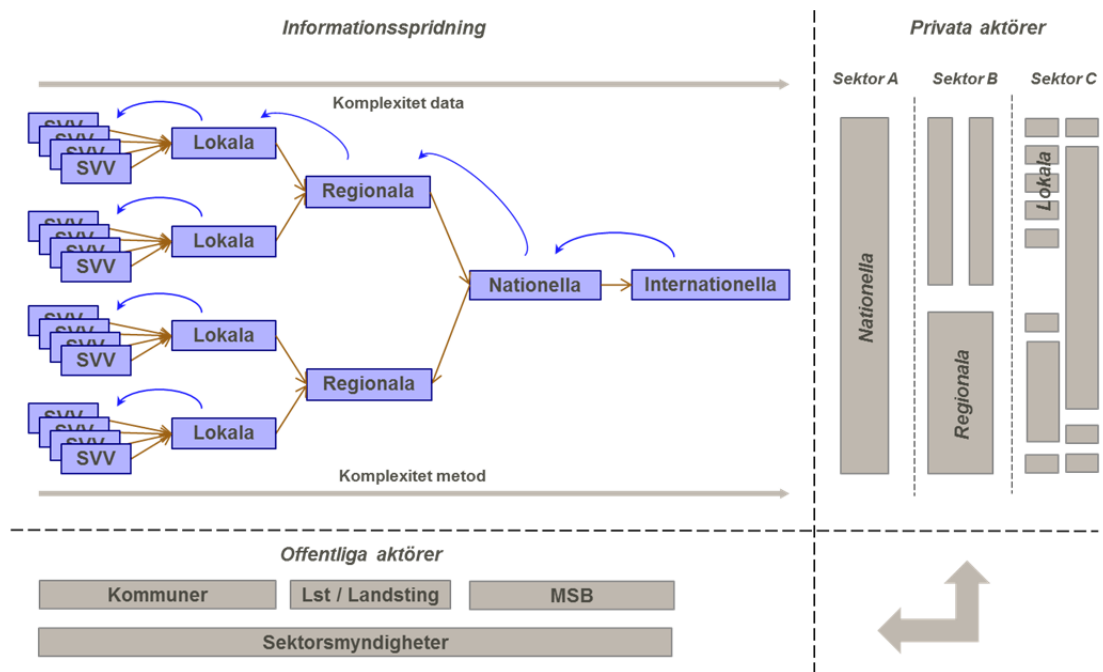
## 5 Utgångspunkter för utveckling av KAS

Syftet för uppdraget är att ge ett underlag för framtagandet av metoder och angreppssätt som behövs för att aktörer inom krisberedskapssystemet ska kunna genomföra konsekvensanalys på samhällsnivå. Följande avsnitt tar utgångspunkt från de tidigare tre kapitlen rörande a) genomgång av offentliga aktörers RSA:er (Kapitel 1), b) erfarenheter från internationella aktörer inom CIP-området (Kapitel 3) och c) ingångsvärden från en workshop med samhällsaktörer (Kapitel 1). I avsnittet presenteras först ett övergripande ramverk kring hur det svenska ”nerifrån-upp”-perspektivet inom krishanteringssystemet skulle kunna användas för konsekvensanalys på samhällsnivå och sedan gås mer ingående igenom vilka aspekter som speciellt behöver beaktas för att åstadkomma en utveckling av metoder och angreppssätt.

*Av vikt att poängteras* är att här tas endast den funktionsorienterade ansatsen upp, i enlighet med avsnitt 3.4, för beroenden mellan samtliga samhällssektorer och funktioner, och inte en ansats för att angripa ömsesidigt beroende kritiska tekniska infrastrukturer och mer fysiska modelleringsansatser. Den senare ansatsen är minst lika viktigt, med tanke på samhällets beroende av denna typ av infrastrukturer som framkom i genomgången av risk- och sårbarhetsanalyserna (se t.ex. Figur 2.14), men behandlas inte djupare här. Anledningen till detta är att det övergripande målet i handlingsplanen (MSB, 2013) är att utveckla metoder och verktyg som kan användas av samtliga samhällsviktiga verksamheter och funktioner, inte endast för de system som är av mer teknisk karaktär. Dock kräver även denna ansats framtagande av tydliga ramverk och riktlinjer för insamling av data samt modeller och metoder för transparenta och korrekta analyser, från enklare aggregerade analyser till simuleringsbaserade. Vidare anser författarna att det inom tidshorizonten för handlingsplanen (fram till år 2020) är möjligt att med denna ansats kunna samla in relevant data, ställa rimliga krav på utveckling av områdesexpertis samt möjliggöra framtagande av konsekvensanalyser på samhällsnivå för aktörer på både lokal, regional och nationell nivå med rimliga och väl avvägda insatser. Vidare skulle den funktionsorienterade ansatsen på ett utmärkt sätt komplettera parallellt arbete med en fysiskt orienterad ansats, t.ex. skulle resultaten från den funktionsorienterade ansatsen kunna användas för att öka kunskapen och förståelsen kring effekterna som uppstår i samhället av sammanbrott i de ömsesidigt beroende tekniska infrastrukturer.

Den övergripande utgångspunkten för att det ska vara möjligt att genomföra konsekvensanalyser på samhällsnivå av god kvalitet i det svenska krisberedskapssystemet är att information om beroenden kan samlas in och spridas mellan samhällets aktörer, se Figur 5.1. För ett sådant system ska vara effektivt bör varje enskild aktör endast ansvara för att kartlägga sina direkta beroenden, där aggregering av beroenden för analys av indirekta beroenden bör genomföras och återmatas ett steg högre i samhällsnivån (t.ex. lokala samhällsviktiga verksamheters aggregeras och analyseras på kommunal nivå). Här förordas således ett system som möjliggör att samhällets alla aktörer med ansvar för krisberedskapsarbete tillsammans kan stödja varandras arbete med konsekvensanalys på samhällsnivå.

Det föreslagna ramverket för informationsspridning utgår från det etablerade ”nerifrån-upp”-perspektivet inom svensk krishantering, strukturen för det offentliga risk- och sårbarhetsarbetet samt hur privata aktörers hanteringsarbete kan integreras i arbetet med konsekvensanalys på samhällsnivå. Den bärande tanken är således att information och analyser, med olika djup och komplexitet, ska kunna genomföras på de olika samhällsnivåerna och sedan kunna aggregeras till en högre nivå samt även återföras till en lägre nivå. Det senare är av mycket stor vikt eftersom det är först då som en enskild aktör kan förstå sin del i helheten och agera utifrån informationen. Av vikt är också att inse att en stor del av de samhällsviktiga verksamheterna drivs och ägs av privata aktörer, varvid en integrering av även dessa i arbetet är av yttersta vikt.



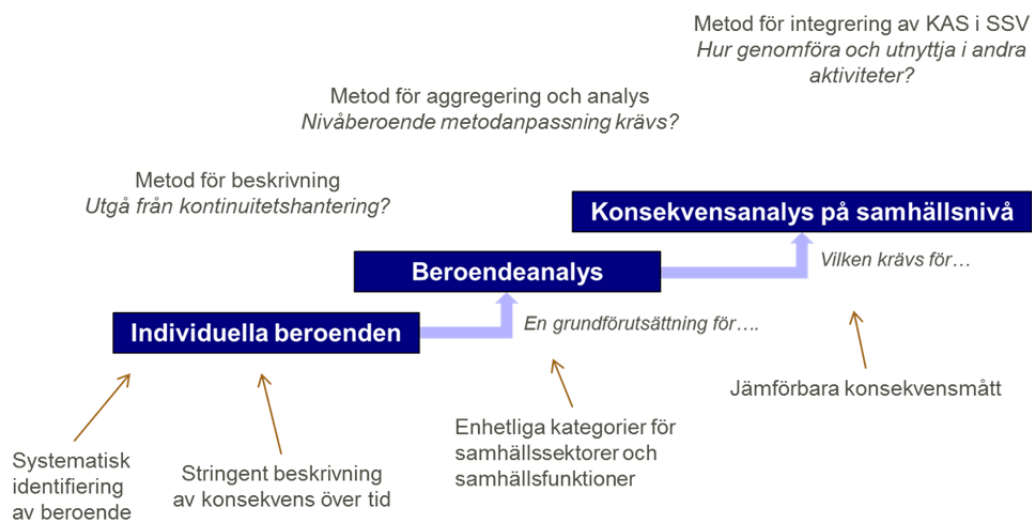
Figur 5.1 Idéskiss över insamling och spridning av information för offentliga och privata aktörer

Det ramverk som skisserats på ovan kommer att kräva adressering och arbete av en del problemområden relaterade till hur information kan samlas in och delas mellan alla aktörer som ingår i hanteringssystemet. Nedan återges sådana områden (oprioriterade) som framkommit utifrån kunskaper från tidigare kapitel. Implementering av ett ramverk för KAS bör ske över längre tid och i samspel med övrigt krishanteringsarbete. Förslagen enligt nedan ska därmed ses som viktiga aspekter att ha i åtanke när ett ramverk för KAS implementeras i inkrementella steg. (dvs. de behöver inte vara lösta för att påbörja arbetet):

- Kräver utredning och förslag avseende integrering av sektorsmyndigheternas ansvarsområden i relation till området skydd av samhällsviktig verksamhet
  - Tydligare koppla sektorernas arbete till det övergripande arbetet med skydd av samhällsviktig verksamhet genom t.ex. s.k. sektorsvisa planer.
  - Hur kan sektorsmyndigheters arbete rörande nationella och regionala aktörer, dvs. aktörer som verkar i flera eller alla regioner och som därmed av praktiska skäl ej kan delta i arbete på regional och lokal nivå, användas och spridas till regionala och lokala aktörer?
  - Hur säkras överensstämmelse mellan sektorsmyndigheternas arbete och MSB:s arbete med sektorerna, t.ex. hur bör skärningar och frågeställningar se ut?
- Kräver arbete kring ansvars- och rolldefiniering mellan MSB, sektorsmyndigheter, andra myndigheter, offentliga aktörer och privata aktörer.
  - Gränsöverskridande samarbetsforum kan vara en möjlig väg för detta arbete.
- Kräver en fungerande privat och offentlig samverkan
  - Tydliga initiativ och incitament för privata aktörer att medverka
  - Förbättrad kommunikation av nyttan och vikten av arbetet till aktörer som inte direkt är involverade i arbetet med konsekvensanalys på samhällsnivå
- Kräver utredning av sekretessproblematiken kring insamling och spridning av information
- Kräver angreppssätt för kvalitetssäkring av informationen som tas fram i systemet
- Kräver vidare arbete med hur infrastrukturen för insamling och analys av data kan se ut
  - Utreda om och hur insamling av KAS-relaterad data kan ske via samma infrastruktur som insamlingen av RSA-relaterad data.

- Undersök om infrastrukturen ska möjliggöra visualisering av beroenden för att aktörer på olika nivåer till viss del ska kunna använda resultatet för eget arbete.
- Utredda om det är lämpligt att integrera någon form av analysstöd i infrastrukturen.
- Undersöka hur och under vilka former delning av information mellan aktörer kan ske.
- Kräver en samordning av och integrering med de aktiviteter som genomförs inom krishanteringsarbetet (t.ex. risk- och sårbarhetsanalyser, kontinuitetshantering, förmågebedömningar, etc.) och hur detta arbete kan utnyttjas och stödja arbetet med konsekvensanalys på samhällsnivå.

Inom respektive samhällsnivå kommer analys- och metodstöd i enlighet med de tre nivåerna i) individuella beroenden, ii) beroendeanalys och iii) konsekvensanalys på samhällsnivå att behöva utvecklas, se Figur 5.2. Troligen kommer det att behövas differentierade analys- och metodstöd för de olika samhällsnivåerna samt utifrån tillgängliga resurser och kompetenser för genomförande av arbetet i enlighet med slutsatser i tidigare kapitel. Nedan ger vi några ingångsvärden till status för och det stöd, i form av till exempel metoder och verktyg, som kommer att krävas på respektive nivå.



Figur 5.2 Översiktliga utvecklingsbehov utifrån de tre nivåerna individuella beroenden, beroendeanalys och konsekvensanalys på samhällsnivå.

### Individuella beroenden

- Identifiering och diskussion av individuella beroenden genomförs av offentliga aktörer i all de tre nivåerna vilket är mycket positivt, dock i varierande omfattning (i enlighet med Kapitel 1)
- För att nå framgång och erhålla data av nödvändig kvalitet bör åtminstone följande aspekter beaktas:
  - Stöd behöver utvecklas för systematisk identifiering av beroenden, t.ex. genom kartläggning och erfarenhetsåterföring av beroenden och konsekvenser i tidigare kriser.
  - Stöd för stringent beskrivning av beroendet för att bl.a. underlätta aggregering, delning av information och möjliggörandet av beroendeanalyser.
  - Stöd för beskrivning av konsekvensen som uppstår över tid för att öka användbarheten av informationen.
  - Stöd för omvandling av kvalitativ data till kvantitativ data för att möjliggöra bearbetning av informationen i en analys.

- Metod för identifiering av individuella beroenden bör tas fram. Här kan det vara lämpligt att utgå från och samsynka med det arbete som genomförs inom ramen för kontinuitetshandling samt att utnyttja empirisk data om beroenden från inträffade händelser.

### Beroendeanalys

- Beroendeanalys genomförs i begränsad omfattning, även då vi var relativt frikostiga med vad som ansågs utgöra en beroendeanalys, av de offentliga aktörerna, då ofta med olika metoder och av varierande omfattning (i enlighet med Kapitel 1).
- För att nå framgång när det gäller att möjliggöra informationsutbyte mellan aktörer och erhålla användbara resultat av bör åtminstone följande aspekter beaktas:
  - Enhetliga kategorier för samhällssektorer och samhällsfunktioner för att möjliggöra aggregering av information från olika aktörer.
  - Undersöka behovet av metod visualisering av indata, som t.ex. kan användas för kvalitetssäkring, kommunikation med beslutsfattare och enklare former av analyser.
- Metod för analys av beroenden utifrån definierade kategorier och definierade format för indata. Det kommer troligen att behövas en metदानpassning utifrån vilken samhällsnivå som avser utnyttja metoden – kan vara allt ifrån stöd för enklare visuella analyser till djupare beroendeanalys utifrån specifika störningar som kan drabba systemet.

### Konsekvensanalys på samhällsnivå

- Konsekvensanalys på samhällsnivå verkar ej genomföras av de offentliga aktörerna (i enlighet med resultaten i kapitel 1). Det kan dock nämnas här att MSB har ett pågående arbete på nationell nivå (NRFB med ursprung från ”Faller en – faller då alla?”-arbetet, MSB, (2009)) som till viss omfattning kan komma att uppfylla delar av det som här avses med den nationella nivån av konsekvensanalys på samhällsnivå (KAS).
- För att nå framgång och erhålla användbara resultat av bör åtminstone följande beaktas:
  - Kategorisering och framtagande av jämförbara konsekvensmått för att kunna jämföra störningar som påverkar olika samhällsfunktioner och i förlängningen kunna prioritera åtgärder som riktas mot olika sektorer/funktioner.
  - Undersöka kopplingar till och utnyttjande av KAS i relaterade krishanteringsaktiviteter.
- Metod för konsekvensanalys bör utvecklas och stödja övrigt krishanteringsarbete (riskanalyser, sårbarhetsanalyser, operativt beslutsfattande, övningsverksamhet, etc.) och möjliggöra fördjupade analyser inom området skydd av samhällsviktiga verksamheter.

## 6 Referenser

DHS (2013). NIPP – Partnering for Critical Infrastructure Security and Resilience, Department of Homeland Security, USA.

DHS (2010). Energy Sector-Specific Plan – An Annex to the National Infrastructure Protection Plan, Department of Homeland Security & United States Department of Energy, USA.

Hassel, H., Johansson, J., Petersen, K., Svegrup, L., (2014). Kunskapsöversikt – Skydd av samhällsviktig verksamhet, LUCRAM rapport 3001, Lunds universitet, Sverige.

Johansson, J., Svegrup, L., Hassel, H. (2013). Studie och översiktlig utvärdering kring applicerbara metoder för komplex beroendeanalys på såväl sektoriell som tvärspektoriell nivå, LUCRAM rapport 3177, Lunds universitet, Sverige.

Johansson, J., Svegrup, L., Kihl, M., (2014). Studie avseende komplexa beroenden mellan telekommunikationsinfrastrukturer inom sektorn Information och Kommunikation, LUCRAM rapport 3186, Lunds universitet, Sverige.

MSB, (2009). Faller en – faller då alla?, ISBN: 91-85053-20-1.

MSB, (2011). Ett fungerande samhälle i en föränderlig värld: nationell strategi för skydd av samhällsviktig verksamhet (MSB266), ISBN 978-91-7383-137-6.

MSB, (2012). Konsekvenser av en översvämning i Mälaren (MSB406), ISBN 978-91-7383-253-9.

MSB, (2013). Handlingsplan för skydd av samhällsviktig verksamhet (MSB957), ISBN 978-91-7383-373-8.

MSB, (2014a). Vägledning för samhällsviktig verksamhet: att identifiera samhällsviktig verksamhet och kritiska beroenden samt bedöma acceptabel avbrottsid (MSB620), ISBN 978-91-7383-392-9

MSB, (2014b). Inriktning för MSB:s verksamhet 2015-2018, Utgångspunkt för verksamhetsplanering, Dnr 2014-3042.

MSB, (2014c). Risk- och sårbarhetsanalyser 2013: Återkoppling av myndigheters redovisningar baserade på risk- och sårbarhetsanalyser -Tema samhällsviktig verksamhet (MSB767), ISBN 978-91-7383-501-5.

TNO, (2013). Cross-sector Dependencies: Foreign Methods and Their Potential Applicability in the Netherlands, TNO, Holland. (<http://english.wodc.nl/onderzoeksdatabase/vertaling-afhankelijkheden-van-zweedse-methode-naar-nederlandse-situatie.aspx>)



# Bilaga 1 Samhällssektorer och samhällsfunktioner

Samhällssektorer	Samhällsfunktioner
<i>0. Ingen sektor</i>	<i>0.0 Endast sektor</i>
1. Energiförsörjning	1.1 El 1.2 Fjärrvärme 1.3 Bränsle och drivmedel
2. Finansiella tjänster	2.1 Betalningssystem 2.2 Tillgång kontanter 2.3 Värdepappershandel 2.4 Försäkringar
3. Handel och industri	3.1 Bygg & Entreprenad 3.2 Detaljhandel 3.3 Tillverkningsindustri 3.4 Import 3.5 Export
4. Hälsa- och sjukvård samt omsorg	4.1 Akutsjukvård 4.2 Primärvård 4.3 Läkemedel- & Materialförsörjning 4.4 Omsorg om barn 4.5 Funktionshindrade 4.6 Äldrevård 4.7 Psykiatri 4.8 Socialtjänst 4.9 Smittskydd
5. Information & Kommunikation	5.1 Telefoni (fast) 5.2 Telefoni (mobil) 5.3 Elektronisk kommunikation 5.4 Internet 5.5 Radiokommunikation 5.6 Satellit/GNSS 5.7 Post 5.8 Dagstidningar 5.9 Webbaserad information 5.10 Sociala medier 5.11 Medier 5.12 TV 5.13 Radio
6. Kommunalteknisk försörjning	6.1 Dricksvattenförsörjning 6.2 Avloppshantering 6.3 Renhållning 6.4 Väghållning
7. Livsmedel	7.1 Distribution livsmedel 7.2 Primärproduktion livsmedel 7.3 Tillverkning livsmedel 7.4 Kontroll av livsmedel

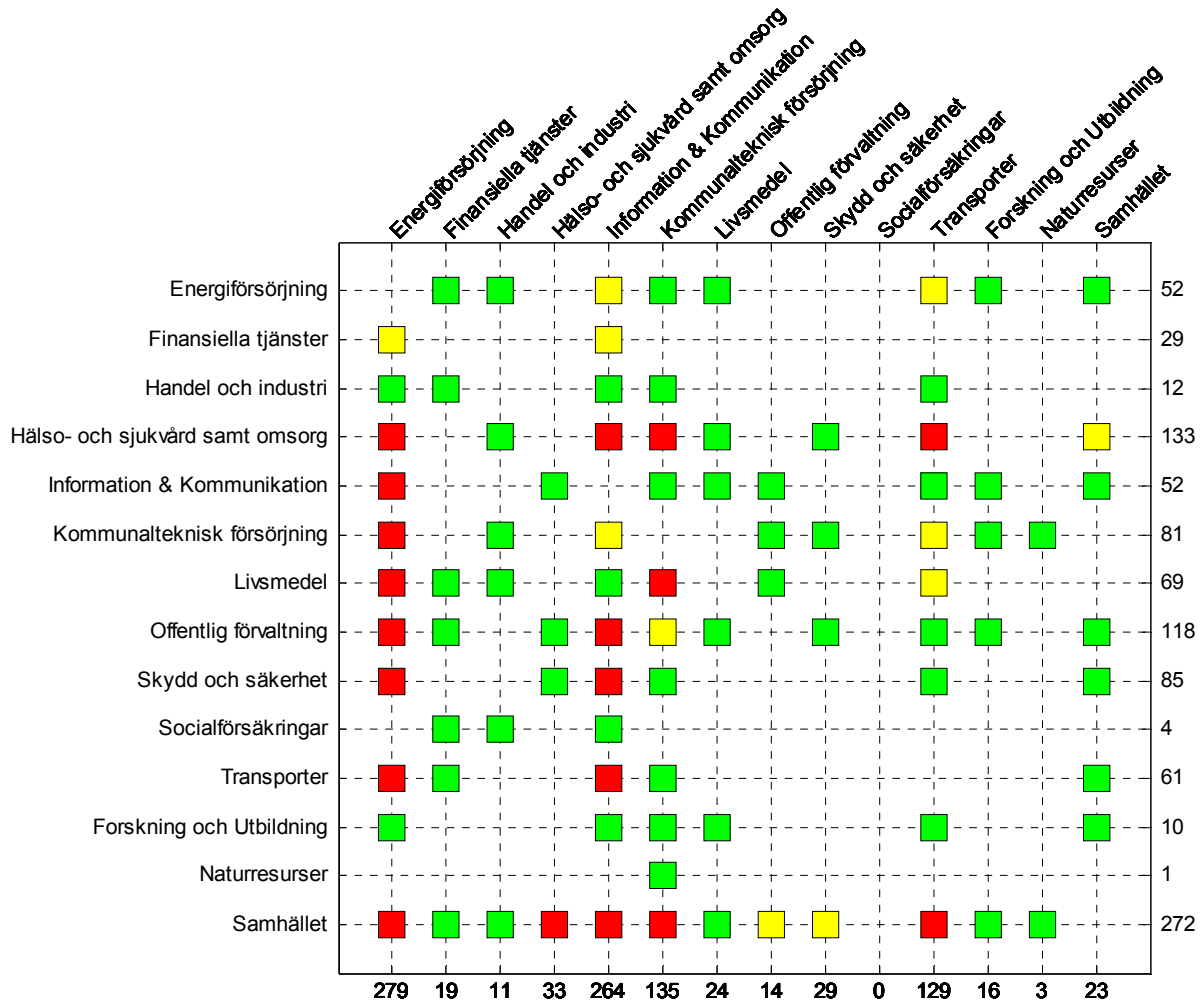
8. Offentlig förvaltning	8.1 Lokal ledning 8.2 Regional ledning 8.3 Nationell ledning 8.4 Begravningsverksamhet 8.5 Diplomatiskt och konsulärt
9. Skydd och säkerhet	9.1 Polis 9.2 Räddningstjänst 9.3 Alarmeringstjänst (t.ex. SOS) 9.4 Tullkontroll 9.5 Kustbevakning 9.6 Gränsskydd & Immigration 9.7 Bevaknings & säkerhet 9.8 Domstolsväsendet 9.9 Åklagarverksamhet 9.10 Militärt försvar 9.11 Kriminalvård
10. Socialförsäkringar	10.1 Allmänna pensionssystem 10.2 Sjuk- & arbetslöshetsförsäkring
11. Transporter	11.1 Flygtransport 11.2 Järnvägstransport 11.3 Sjötransport 11.4 Vägtransport 11.5 Kollektivtrafik
<i>12. Forskning och Utbildning</i>	<i>12.1 Kompetent personal/entreprenörer 12.2 Forskning 12.3 Förskolor och skolor</i>
<i>13. Naturresurser</i>	<i>13.1 Sjö 13.2 Skog 13.3 Hav 13.4 Jordbruksmark</i>
<i>14. Samhället</i>	<i>14.1 Liv och hälsa 14.2 Funktionalitet 14.3 Grundläggande värden 14.4 Samhällsviktig verksamhet 14.5 Teknisk infrastruktur 14.6 Allmänheten 14.7 Personal</i>

*\*Kursiv anger tillagda sektorer och funktioner i jämförelse med de angivna i MSB:s rapport "Handlingsplan för skydd av samhällsviktig verksamhet".*

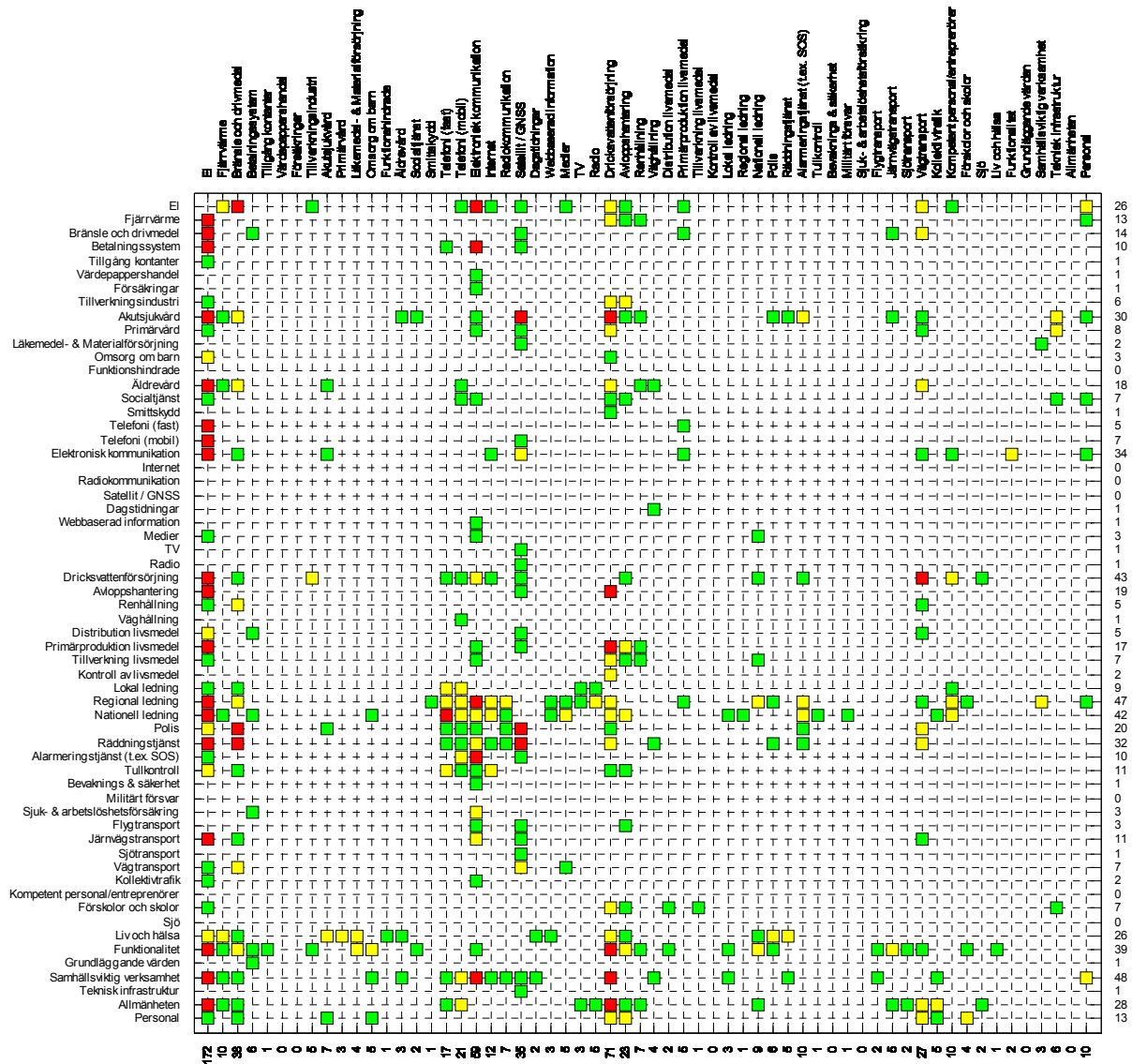


## Bilaga 2 Beroendematriser

Utifrån insamlade data från genomlysningen av de olika aktörernas risk- och sårbarhetsanalyser presenteras här beroendematriser utifrån antalet omnämnande av ett beroende mellan samhällssektorer, se Figur 1, eller samhällsfunktioner, se Figur 2.



**Figur 1** Antalet omnämnande av ett beroende mellan olika samhällsfunktioner. Vertikal axel (y) anger en viss sektors beroende av andra sektorer och horisontell axel (x) anger sektorers beroende av en viss sektor. Färgmarkeringen är utifrån totala antalet omnämnande, där röd  $\geq 20$ , gul  $\geq 10$  och grön  $> 0$ .



Figur 2 Antalet omnämning av ett beroende mellan olika samhällsfunktioner. Vertikal axel (y) anger en viss funktions beroende av andra funktioner och horisontell axel (x) anger funktioners beroende av en viss funktion. Färgmarkeringen är utifrån totala antalet omnämning, där röd  $\geq 4$ , gul  $\geq 2$  och grön  $> 0$ .

## Bilaga 3 Intervjumaterial

Intervjuerna som genomfördes var semi-strukturerade med användning av en tematisk struktur. Innan tidpunkten för intervjun skickades nedanstående frågor till intervjuobjekten för att i möjligaste mån ge en fingervisning om temat för intervjun samt tid till förberedelse inför intervjun. Den kontextuella beskrivningen, tematiska strukturen och de öppna frågorna var enligt texten nedan. Beroende på tillgänglig tid för intervjun och vilken inriktning intervjun tog, varierar omfattning på svaren och även vilka frågor som hanns med. Dock försökte vi i möjligaste mån under intervjun att täcka samtliga tema.

The Swedish Civil Contingencies Agency (MSB) is responsible for coordinating and improving efforts concerning civil protection, public safety, emergency management and civil defence. One of their long term aims is to improve the understanding of how to build a national strategy in the area of critical infrastructure protection. Currently, MSB is interested in how to provide support to various actors in the Swedish society in the form of frameworks, methods, guidelines, etc. regarding the analysis of cascading effects in large-scale disturbances and the societal consequences thereof. The focus is not only on the immediate effect on given infrastructure system but on the totality of societal consequences. The objective with such an effort is to enable the analysis of high consequence and low probability events from a wider societal perspective, at the local, regional and national level. This would then be a basis for improving decision making concerning e.g. prioritization of activities (prevention) and in emergency response (operative).

To support this work, MSB is interested in how other countries and international bodies are dealing with and are planning to deal with the above issues. Hence, if possible, it could be necessary to meet several different persons within or outside your organization to get the broader picture. We would also highly appreciate if you would have the possibility to give an informal overview of current work and experiences within the area of interest. If you know of any facilities / labs that you think a visit would be of benefit to our project, we would be highly interested.

The purpose of our visit is to take an explorative approach to what efforts are made within this context at the local, regional and national (international) level. Overarching themes where we would like to get some insights are:

### **Projects and areas of work (contextual question)**

- *In what areas do you conduct research/work and are you involved in any type projects related to critical infrastructure protection?*

### **Legislation, frameworks and guidelines**

This theme concerns whether there are any frameworks or guidelines for conducting analysis of societal consequences accounting for cascading effects; either that have been developed by your organization or implemented in your country (e.g. as part of some legislation or as an initiative of some governmental agency). If that is the case, we are interested in things like who are using (or are intended to use) the frameworks/guidelines and for what, the essential characteristics of them, etc.

- *Are there any legislations, frameworks or guidelines suggested and/or used in your country?*
- *What is the main content of these?*
- *Who and at which level of the society (local, regional, national) are these used or intended for?*
- *For what and in which context (operative, risk assessments, identification, prioritization, etc.) are they used or intended for?*

### **Methods and tools**

If methods and tools have been developed to support this work, it would be of interest to get an overall picture of the type and use of these methods and tools. For example engineering driven (i.e. modeling of critical technical infrastructures), economically driven (i.e. economical couplings between societal sectors), empirically driven (i.e. inference of couplings through past events), expert assessment driven (i.e. couplings based on expert assessments). What types of decisions/activities are they supporting? For what level is the method intended (local, regional, national)? What measures of consequence are used? Are the method/tool designed for a specific sector or does it have

more of a general all-sector approach? Are different methods/tools used in different sectors? Are the methods voluntary or obligatory?

- *Are there any methods and tools used by you or other national bodies to support the above work?*
- *Are the methods voluntary or obligatory (connecting back to previous theme)?*
- *What type of methods/tools are they? E.g. are they engineering driven (i.e. modelling of critical technical infrastructures), economically driven (i.e. economical couplings between societal sectors), empirically driven (i.e. inference of couplings through past events), expert assessment driven (i.e. couplings based on expert assessments)?*
- *Who is using the method/tool (i.e. actually conducting the analysis)?*
- *For what level (local, regional, national, all?) and sectors (specific, all?) is the results of the method/tool intended?*
- *What measures of consequence are used?*
- *What types of decisions/activities are they intended to support?*

#### **Data collection and dissemination**

For the methods and tools used, of what type and extent is the input data? How is this data gathered? At what level in the society is the data gathered and, if from different levels, how is the data aggregated? From a data output point of view, how is the results disseminated? How is the results used to inform decision and activities at the different societal levels? Is the data limited in accessibility to certain agents or certain use?

- *For the methods and tools used, of what type and extent is the input data?*
- *How is this data gathered? Is the data limited in accessibility to certain agents or certain uses?*
- *At what level in the society is the data gathered?*
- *How is the results disseminated? E.g. is the data limited in accessibility to certain agents or certain uses? Is the results used to inform decisions and activities at the different societal levels?*

#### **Lessons learned and plans ahead**

We would also like to take part of “lessons learned” regarding all of the above themes. This could be e.g. challenges with respect to constructing a framework, enabling private-public cooperation, setting up a system for data collection, confidentiality issues, data collection and dissemination of results, etc. Finally, it would also be of high interest for us to get a picture of the road ahead. In what direction will the work in this area continue? What are the drivers and challenges?

- *Do you have any “lessons learned” regarding all of the above themes?*
- *What direction will the work in this area continue?*
- *What are the drivers and challenges?*

## I. TNO

Country: Netherlands

Organization: TNO

Name: Eric Luijff & Marieke Klaver

Interviewer: Jonas Johansson & Henrik Hassel

### I. Projects and areas of work

TNO started with CIP in the domain of Cyber security in 1995. Since 2004 they have been working broader with CIP in general. Both Eric and Marieke have a background in mathematics. Mainly their research focus has been on CIP and CIIP including the identification of CI in the Netherlands and dependency analysis as well as on cyber security. Their research is both focusing on national, regional and EU-perspectives.

TNO is trying to support the government and is involved in many EU-projects on Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP). TNO was founded in 1932 and is an independent non-profit body established by law (not a company and not a government). The idea was to take fundamental issues and use it in an applied setting. TNO is partly government funded, partly project funding where part of the funding is through consultancy.

They are currently or have been working on EU-funded projects such as PREDICT, INTACT, CIPRnet and SEGRID.

### II. Legislation, frameworks and guidelines

The Ministry of Security and Justice "owns" the problem of CIP and dependencies between CI in the Netherlands and coordinates the national CIP program. There is no comprehensive/all-encompassing legislation in the area of CIP. However, there are sector-specific legislations within some of the critical sectors. For example for private actors in the telecommunication sector there is some cyber security and business continuity legislation which is mainly EU-driven.

The work in the CIIP area gets a lot of attention in the Netherlands. There is for example a National Security Board and an Incident Response Board in that area. The government is pushing on the private companies to report cyber security breaches, even more than EU requires.

The Ministry of Security and Justice coordinates the work to identify national critical infrastructures. However, each individual ministry is doing the actual assessments for the sectors they are responsible for. Another relevant activity is the National Risk Assessment that is carried out.

Risk assessments are also performed on a regional level by each of the 25 Safety Regions, but nothing is done at the local level. On the other hand, authorities from municipalities, especially the large cities, are part of the Safety Region decision-making bodies.

For what and in which context (operative, risk assessments, identification, prioritization, etc.) are they used or intended for?

The National Risk Assessment is used for setting policies and make prioritizations concerning what sectors/risks to direct efforts to (funding, etc.) on a national level. Only used on the national level and then pushed down although at the regional level a derived method for risk analysis is being used.

### III. Methods and tools

1. Identification of National Critical Infrastructures - Currently the Ministry of Security and Justice is developing a new approach where e.g. additional levels of criticality will be added<sup>4</sup>. This is done because everyone wanted to be called a “critical infrastructure” which gave rise to a need for a more nuanced way of describing criticality. This work, however, does not encompass a method as such but rather based on workshop discussions. How this work is used depend on which sector is considered. But typically it is used to identify what is important to protect, what level of protection is needed and if additional measures must be taken. Exactly how the new method of CI identification looks, however, is not yet open to the public.
2. National risk assessment - There is a specific structure/method (workshop based with persons from different sectors) and so far some 50 scenarios have been analysed; however, these only include first-order effects and not cascading effects. The method was developed by several agencies and focuses on multiple impact categories such as, economic, environmental, casualties, injured, territorial integrity and societal impacts. Dependencies are not formally included in the national risk assessment but this is currently considered. One step towards strengthening the Dutch approach is that TNO has performed an overview for the Dutch Ministry of Security and Justice on how other countries, including Sweden, have worked with cross-sector dependencies.
3. Regional risk assessments – Have to be performed by the Safety Regions. The same method as in the National Risk Assessment is recommended but it is not mandatory to use it.
4. PREDICT – The project is focusing on developing methods to identify CI and assess dependencies and possible ways is a structured way focusing on the regional level. There are three cases/end users (1: Safety region focusing on flooding and the physical, evacuation, economic etc. consequences; 2: Railway incident in a tunnel with a cross-border and HazMat; 3: Finish maritime incident with HazMat and risk of gas cloud across populated area and a shipping channel blockage in international waters). In all cases dependencies are addressed and what type of information tools can support the decisions that need to be taken during an incident. The end users are different for the different cases (safety regions and CI operators, etc.). The tools are intended to be used primarily in the planning, preparation phase and to some extent in the incident phase.
5. CIPRnet – a network of excellence project focusing on modelling and simulation. The idea is to create an equivalent to NISAC in the US although not being a single center but rather be a set of nodes which shares methods and coordinate approaches. The modelling and simulation should be able to provide prediction support to countries, for example predict how a hurricane would strike. One focus is also standardisation of terms since it is easier to use data from different countries then.
6. TNO’s critical infrastructure incident database (CIID) – data is being collected in a systematic way (see more below) to e.g. form basis for analyses and provide a facts-based input to scenario discussion
7. Quick-scan method – was the method that originally was used to identify CI in the Netherlands and was developed by TNO. How similar this is to the method used currently is unclear.

Are the methods voluntary or obligatory (connecting back to previous theme)?

CI identification is obligatory in the sectors and regional risk assessments are obligatory for the regions, and then there are various sector-specific requirements.

---

<sup>4</sup> Publication expected before mid of May 2015.

Who is using the method/tool (i.e. actually conducting the analysis)? For what level (local, regional, national, all?) and sectors (specific, all?) is the results of the method/tool intended? What measures of consequence are used? What types of decisions/activities are they intended to support?

The National Risk Assessment looks at where vulnerabilities are located and provides a list of the main and less critical assets which is used to indicate assets of high criticality and if something happens this could lead to that military/police is directed to the site.

Data from the TNO-database is being used by TNO during workshops and scenario analyses with e.g. infrastructure operators to show potential cascading effects and support the discussion.

#### IV. Data collection and dissemination

TNO has built a database where they look at two different things. First, a database from media reports has been created and secondly looking incident evaluation reports which provide many learning lessons when translated to a national context. Earlier TNO had a project on trying to automate the process of collecting the data but all data right now are collected and coded manually (maybe it would be possible to find "hotspots" automatically but right now it seems to be difficult to automate the process). Since looking at media reports there is a bias in what type of information you get (more high impact on the societal side).

10340 incidents have been collected in database through e.g. Google search in nine languages every day as well as using official incident evaluation reports. They also use the daily CIP reports from DHS in the USA. Characteristics that are being coded are amongst others affected sector, sub-sector, which operator, start and end time, location type, impacted area, human deliberate actions, people affected by consequences, customers or households, common cause, interesting for scenario selection, recovery period, measures, source, nation.

Insurance companies have to some extent collected data but they tend not to focus on cascading effects.

In the early CI-project researchers asked for CI-specific data without getting any. This was mainly due to not asking specific-enough questions, not describing the added value for the CI operators in providing the data. The problem is that most data is security-sensitive or sensitive for business reasons so just asking "give us the data" is not fruitful. In certain projects it has been possible to get reasonably good data, although when asking for geographical data exact locations are not provided due to the sensitivity of that information.

There are some efforts from a R&D-perspective to build and collect the type of data that is needed for modelling and simulation. In the beginning of the TNO research there were hardly any data available; however, now it is getting better. A lot of data is available from open access, especially since exact locations are seldom needed. In general it is enough to draw a bit more "global" conclusions (in certain cases it shows the potential of the approach when detailed information would be available).

For prototype building real data is not needed at all. Rather, realistic data is enough which is easier to get or even can be constructed or derived (e.g. average power consumption per capita).

Much less data exist on "soft infrastructure" – such as food supply, health sector, etc. Also transportation is somewhat difficult to get data on. Some steps have been made in the transportation sector but more to do though.

TNO uses a GIS platform to show data as a way to get interest and get people to share data which seems to be successful.

## V. Lessons learned and plans ahead

We would also like to take part of “lessons learned” regarding all of the above themes. This could be e.g. challenges with respect to constructing a framework, enabling private-public cooperation, setting up a system for data collection, confidentiality issues, data collection and dissemination of results, etc. It would also be of high interest for us to get a picture of the road ahead. In what direction will the work in this area continue? What are the drivers and challenges?

A problem is that the organisational structure of private actors do not map well against the area of responsibility of e.g. the Safety Regions. Some CI operators act on a national level which means they typically only want to have one or a few counterparts rather than e.g. 20 regions. KPN (major telco) and TenneT (electric transmission operator), for example, are such examples. On the other hand in some regions there might be multiple CI operators active, e.g. water boards, but not all can be included in the emergency management decision taking processes which means someone has to represent a set of (even competitor) CI operators which is challenging. But the work is progressing, trust and confidence is being built but it is still much work in progress. Another issue is the differences in goals between private and public actors. It is critical that each side understand the other side. Finally, another concern that is raised by the private CI operators is that they are afraid of a tool that diminishes their own decision ability, i.e. they want to be in control of their (often business driven) decisions.

It is important to be clear in understanding that the researchers that ask for data and perform the analyses but that the decisions should be left to the operators. This e.g. makes it easier to get hold of data.

Many of the building blocks are there but what is needed is to use the lessons identified by research to feed into policy and CI-owners and to provide the tools that the stakeholders (authorities and CI operators) can use. Connecting and selecting what information to provide to the users is crucial. In addition, there are many operational and R&D based advances made in different countries and in different sectors. The question is how to bring this information together and integrate it. as Another question is how to learn lessons from each other.

We also need to figure out at what level of granularity we should apply the models and simulations that we develop. Is it important to only get a feeling of the consequences or do we need to be precise down to the last comma?

When the Netherlands is to take the EU Presidency in 1H2016, CIP is being considered as a theme. That will be an opportunity but will also require some joint international development steps.



## II. JRC

Country: EU  
Organization: JRC Ispra  
Name: Georgios Giannopoulos  
Interviewer: Kurt Petersen

### I. Projects and areas of work

JRC is doing research on critical infrastructure protection at the Institute for Protection and the Security of Citizens. They have developed an ICT-Power model linking the control with the power grid, giving the dispatcher information on disturbances and interruptions. They are developing a platform for illustrating cascading effects, GRASP, based on input-output modelling. The platform is intended for European or national analyses. Finally, they are supporting a project in cooperation with Politecnico di Milano and the Lombardo region who are mapping interdependencies between assets, but it does only include the direct linkages and do not consider cascading effect into secondary assets or activities.

### II. Legislation, frameworks and guidelines

There are no legislations, frameworks or guidelines at European level and JRC has no information on similar activities in any member country. The DG ECHO has the 2011 risk mapping for all member countries, but it does not explicitly consider consequences for all societal sectors.

### III. Methods and tools

At European level one activity is ongoing. An European grid for air traffic management, but it does not address consequences, neither any direct consequence of disturbances nor any cascading effects.

### IV. Data collection and dissemination

No data are collected or available. The DG ECHO national risk mappings are at high level and confidential to the member countries. Only disturbances and accidents at industrial plants under the Seveso directive are collected and available for member countries. The data do not address cascading effects in general.

### V. Lessons learned and plans ahead

No lessons learned are available. The only exception is the MARS database describing accidents at Seveso plants throughout Europe. The data do not include descriptions on the consequences at the societal level.

### III. DHS and NISAC

Country: USA

Organizations: DHS/OCIA & NISAC (Sandia National Lab and Los Alamos National Lab)

Names: DHS: Marilee Orr, Kara Buckley and Christina Saari (Division Chief of the Prioritization and Modelling branch)  
NISAC: Dan Pless (Sandia National Lab. Computer science background - 11 years at Sandia and NISAC. Started with risk analysis, was later detailed for 1.5 years to DHS)  
Alan Berscheid (Los Alamos National Lab. Background in electrical engineering, power system analysis, communication, interdependencies between sectors and infrastructures. 20 years working with CIP)

Interviewer: Jonas Johansson

#### I. Projects and areas of work

DHS and more specifically the Office of Cyber and Infrastructure Analysis (formerly the Homeland Infrastructure Threat and Risk Analysis Center) has lately been focusing more towards the consequences of all-hazard disruptions to critical infrastructures rather than the earlier focus on threat/terrorism, although still working within more "plausible" scenarios. In general they perform: 1) steady state analysis (like Hurricane scenarios that they sent to me) 2) broad cross-sector infrastructure analyses trying to capture the effects of interdependencies at a more granular level 3) More quick-turn analyses, e.g. if there is a Hurricane coming NISAC does pre-analyses with respect to expected infrastructure disruptions and cascading consequences (e.g. power outages). Use it for posting to people to what they can expect. They also have a critical infrastructure prioritization program - try to identify infrastructures that meets critical thresholds, e.g. if this fails it will cost so much money or affect so many. It is a very high level approach where different states nominate infrastructures and then NISAC and other labs helps them figure out the consequences of loss. DHS then assembles lists which are used for funding grants etc. for securing them. Also do prioritization per organization/function during an event to try and figure out the critical components specific to the US. DHS realizes that the criticality depends on context (e.g. for some events, e.g. terrorism, large sport stadiums are important while at steady state it could be an important power station). Underlying all of that is the capabilities that NISAC provide – the work is organized more or less divided in different sectors and some cross-sectorial interdependencies analyzes. DHS also tries and work at an operational level and work with other federal agencies to help them to understand risks and specific questions regarding national security coupled to their area of expertise. About 240 000<sup>5</sup> people work at DHS (effectively larger than the entire Canadian government).

The National Infrastructure Simulation and Analysis Center (NISAC) predates DHS's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), which was formed in 2006). HITRAC was initially focused on terrorism due to 9/11, but shifted to a more all-hazard approach in the aftermath of Hurricane Katrina in 2005 (Katrina was really a major sea-change). Before that, NISAC ran Hurricane events but more in order to be prepared for a terrorist event - fortunately they had the capabilities and could support during the Katrina event – which lead to the realization that the really needed to be an all-hazard and not only looking at terrorism. They also did some analyses during the BP oil-spill in the gulf of Texas - which lead to adding Industrial accidents into the portfolio. They also have some capabilities with respect to pandemic modelling and analysis (however not the epidemiology portion of that, handled at the

---

<sup>5</sup> <http://www.dhs.gov/about-dhs>

Center for Disease Control under the Department of Health and Human Services, but more towards infrastructures/ transportations). NISAC believe that it is powerful to have models that can run with less information, which of course leads to less accurate results, but at least can get some estimations, which are useful for informing operational decisions.

In essence there have been two main shifts (not a big change about what NISAC is doing and their capabilities but how rather how DHS talk and use the results):

- 1) From terrorism to all-hazards
- 2) From protection/security to resilience (mitigate impacts, adapt to disruptions and recover quickly)

In the past the analyses done by NISAC were always more focused towards a threat and questions like "What are we doing two days after the Hurricane?". Now a days it is more forwardly leaning, e.g. aging infrastructure and climate change - which can that potentially lead to a shift in what work they are asked to do (fitting well into what NISAC always wanted to do). NISAC has gone from a more operational/tactical level to a more strategically level over the years. NISAC has also experienced the "security issue pendulum", swinging from protecting information (earlier) to sharing information (lately).

NISAC consists of people from both Los Alamos and Sandia, which are effectively national laboratories for the Department of Energy (DOE) (i.e. federal laboratories). They however have private contractors that manage them. As such people working at the Labs are not federal employees but private employees. In essence they are contractors that can only work for the federal government. About 20 fulltime persons work at NISAC, plus support from co-workers in related areas (each lab have about 10 000 employees).

NISAC started out as collaboration between Sandia and Los Alamos in 1999, was later designated by Congress (through the Patriot Act in 2001) to be the center of excellence within their area of expertise (modelling and simulation of critical infrastructures). NISACs work fall into three buckets:

- 1) Interdependency analysis and cascading consequences
- 2) Supply chains analysis
- 3) Economic analysis, i.e. what are the impacts on the economy if infrastructures fail

NISAC also provides continuity of expertise as oppose to the high turnaround of staff at DHS. In order to give value to the nation NISAC cannot just work in isolation but needs to be the bridge between the industry and the government. It is a very tough communication gap to over bridge to policy and decision makers - and also understanding the timelines you need to hit (e.g. during the H1N1-pandemic the HHS modeling results came in too late and almost contradicted the decisions that had already been made). Having the analysis matching the timeline the decision makers are working on is critical, and it is also important to communicate in a form that is less academic (i.e. not the scientific journal form). Here DHS serves a necessary bridge between NISAC and other governmental bodies.

NISAC can go 24/7 if requested to (the do not like it...). DHS is posing the questions and leading NISAC, there is a specific NISAC only building at Sandia. It is about a 2 hour drive between the two Labs. About 40-50 people working at NISAC part- and fulltime (about 20-30 fulltime), but the part time employees usually work in related fields, which is of use for NISAC, and they are also using the knowledgebase of the Labs for specific questions.

NISAC really has to pick and choose the questions to work with, and it is important that it is clear what type of questions the center should work with. NISAC started with looking within the borders of USA,

lately however they have been working more with cross-border problems, e.g. within supply chain and energy.

In total they have 16 sectors in the US. DHS is only considered with the civilian sectors, not the military such as the defense industrial base (belongs to Department of Defense, DoD), i.e. prioritizing those 5-6 sectors that are considered lifeline infrastructures (transportation, communication, power, water, healthcare, emergency services, commercial facilities). Finance is sort of a lifeline infrastructure and sort of not (it is a weird one...). From some sectors it is easier to get data from and cooperate with while other sectors it is harder, e.g. the financial sector (all data proprietary).

*Why is NISAC not part of DHS?* Hard to maintain a stable federal workforce that can do the type of work that NISAC does (however there have been some failed attempts, like the Risk management and analysis group that was cancelled by congress). It has to be an ongoing capability and it kind of naturally falls in the federal funded research and development organizations - private not an option. Further, DOE laboratories have the technical expertise regarding modelling and simulation of infrastructures prior to the forming of NISAC (which was initiated in 1999). All work is federally funded. Universities could do some of it; however the continuity might be a problem as more of a transient workforce (i.e. students). NISAC can work at all levels of classification levels and handle sensitive information. National labs are also not competing with public industries - make it possible to get information and function as a bridge and neutral broker between industry and government (as they are only semi-government and industries is more willing to share information as they have non-disclosure agreements that NISAC will not give the information to other companies or the government - which could otherwise be used negatively either by competitors or from regulatory bodies). DHS (through the Homeland security act) do have a program to protect critical infrastructure information that they get from the private sector, but some companies still worries about giving out information. It would be more or less impossible to have a NISAC at DHS as it would require a lot of staff, with difficulties of maintaining the workforce and that many of the people at NISAC work only part time there and can draw from a wider set of skills, to cover all the capabilities that DHS can draw from NISAC.

*Are there similar initiatives as NISAC also at state level?* Not really, some initiatives have e.g. been taken by the Louisiana state (through the NIMSAT center at the U of Louisiana) towards Hurricane vulnerability. New York did recently stand up the "The center for Urban Science and Progress" with some infrastructure interest. However, there is really not much at the state or local level that NISAC or DHS are aware of that does similar work as NISAC. If there is something it is more towards more traditional hazard modelling and address more specific local issues.

*How much is NISAC collaborating with universities and how much is it a "stand-alone"?* They have some collaboration with some centers of excellence, e.g. CREATE (economic at USCE), food folks at Minnesota, Cornell for transportation/railway, and University of Utah. There are informal collaborations as the employee at NISAC tends to maintain relationships with their former advisors from university etc. There is however no mechanism that brings this in, but rather ad-hoc. DHS does sponsor summer-students from universities to go to e.g. NISAC.

## II. Legislation, frameworks and guidelines

Critical infrastructures are divided into sectors and then there is "this elaborate plan" (i.e. the National Infrastructure Protection Plan (NIPP)) on how to organize within sectors and between sectors, with sector councils etc. and which agency that has the lead in respective sector. For some of the sectors it is the DHS (8 sectors), but it doesn't really matter as they are always in some "others lane" (i.e. are seen to interfere

with some other authority). The responsible organizations within CIP are not regulatory agencies (e.g. the nuclear industry has the agency “Nuclear Regulatory Commission” but falls in CIP under DHS).

*Are there legislation supporting the National Infrastructure Protection Plan (NIPP) and the Sector Specific Plans (SSP)? E.g. demands on risk analyses etc.? How is it enforced? Mandatory or Voluntary?* It stops basically at the National and state level. No real legislation enforcing local level and private companies. For private companies there is no legislation other than the normal regulatory legislation. It was an Executive Order under President Bush that stated that that all agencies should work with the NIPP. President Obama then gave an Executive Order to update the NIPP, and as this has presidential authority behind it that kind of ties it to the Homeland Security Act - it then really binds the federal government but it does not bind the state and local governments or the private industries. Once passing the "federal fence", everything is voluntary. At the state levels there are however some grants to act as carrots in this area. With private industry it is a lot harder, other than the carrot “if you work with us we can make sure that down the line some regulation will not show up” (kind of a complicated dance). The local levels have mostly evacuation planning, emergency response planning, recovery plans and so forth - Some of these plans are worked with in collaboration with the government (e.g. FEMA) - but there is not really any NIPP or SSP at state or local level.

### III. Methods and tools

NISAC have during the last decade developed and maintained many different models and tool. Here only brief overviews of some of these methods and tools are given (for different NISAC models, see e.g.: <http://www.lanl.gov/programs/nisac/cipdss.shtml> and <http://www.sandia.gov/nisac/>. NISAC did not, by the time of the interview, have a compiled list with good description of their models.). For all CIP-models NISAC tend to structure them into different layers:

- 1) Quick models that allow for operational use
- 2) Semi-quick having higher fidelity but also requires longer time
- 3) Slow models to understand the problem (i.e. can take months to set up the simulation, run the simulation and analyze the output)

It is about picking the right tool for the problem (i.e. operative, exercise, training, etc.). Important a tool does not constitute a capability! Outside people tend to see NISAC as this big computer program where you put in the question in one end and out comes an answer - not the case. They always use a suite of tools and analysts who know how to use the tool. Always the combination data - tools - analysts that has to work together to solve a problem - not a program in a computer. A model is only a piece of the puzzle. NISAC constantly has to make this point to outside parties. The problem of having "one model" is that it tends to fit one question/problem and if another question is asked the model becomes invalid. In previous crises they have had to tune/change the models in order to get useful results for decision making. Furthermore, there are a lot of different granularity levels of the models, e.g. the physical infrastructure models have relatively high resolution while the economic models have rather poor resolution.

PLANNING SCENARIOS: In the beginning they developed reasonable hazard scenarios in-house but lately (the last few years) they have done a lot more outreach to e.g. FEMA, other parts of DHS, regional and local folks to develop scenarios that make sense to them and help them in their planning phases. Within this frame they often have discussion of what actual scenario to look at, i.e. look at more severe scenarios (HCLP) or look at more likely scenarios (LCHP)? Lately they have also been looking at more moderate hazards, as always using the maximum of the maximum tends lead to people just "throwing up

their hands/giving up” as the scenarios become overwhelming. It is tough to address the resilience, as systems are built for a certain hazard level it is easier to do smaller incremental steps for further evolution.

**CIP-DSS:** Critical Infrastructure Protection Decision Support System - From the 2004-2007 time frame when the model was developed by funding from DHS. CIP-DSS is not used as much any longer compared to earlier, although use it as a quick low resolution model that can be run a lot of times quickly. It is a system dynamics model - good for high level and more qualitative conclusions rather than quantitative. The drive behind the model is to get a bigger system-of-system model, there is some high level of modelling regarding infrastructures, including some interdependencies and how things can cascade. Since then, the focus has been on models with higher resolution and modelling specific interdependencies (e.g. their electric power and water supply models). They are using the model less frequently now because it was too generalized, it could not pinpoint the impact on a specific facility which was the type of questions NISAC was asked during, about, 2008 until now. They needed more precise models - which have meant that they model at most two to three systems and interdependencies between systems (it varies with questions being asked). Now they are more "manually" setting up more higher resolution models to answer specific questions. It is nice and necessary to have the analyst "in the loop" to make a sanity check rather than having more automated models (given the amount of uncertainty in the models).

**Single engineering infrastructure models:** Electric power and water, actively developing telecommunication, transportation, natural gas models, financial system models, chemical supply chain models, food industry supply chains models, agricultural models, economic models (IO, CGE, REMI). The models NISAC use within this area can be in-house, commercial or open-source. They try to leverage on commercial tools but there are generally gaps that require some in-house development. For example with national natural gas simulations there is a reasonable good, but not perfect, commercial tool called GPCM (Gas pricing competition model) which NISAC use. But for petroleum (refineries, transmission pipelines, etc.) there does not exist any available model for the national infrastructures, hence NISAC have had to build up their own model. NISAC have the complete infrastructure of the national petroleum pipeline system (with crude oil and refined product pipelines), used e.g. for analyzing the effects of earthquakes.

**Financial systems:** NISAC also looking and trying to understand how disruptions could affect the financial system and the effects of such disruptions. For these types of models they use several different methods, such as system-dynamics, engineering models, supply chain models or agent-based approaches where different agents acts upon certain information (or lack of information) and try to study the system effects.

**Economic models:** NISAC are using both Economic Input Output Models (IO) and General Equilibrium Models (GEM) and REMI. For fast simulations they use IO-models (i.e. for approaching threats such as hurricanes). When they have more time they use CGI [GEM] models or system dynamics sorts of models. When they really want to go into detail and understand what is going on, they also use agent-based models (much more expensive model though).

**Health-care systems:** NISAC have models that can trace how people move throughout the hospital system. Have been used to answer questions like “how many patients can be treated in a hospital and how to reroute patients to other hospitals?” (by connecting a transportation model and the capacities these hospitals have, e.g. burn units). It is used to evaluate how the overall health-care system could respond to a disaster. They have data for most of the hospitals, like number of beds, occupation rate, etc.

**Models of dependency/interdependencies:** One approach is to have very detailed infrastructure models and interdependencies, which are hard to get data to. No one really knows how different critical infrastructures are connected to each other at a component level (e.g. what specific substation provides power to a water treatment plant) and also understanding the availability of backup capabilities (e.g. backup generators). Another approach is more of a system dynamics approach where you do not have the specific dependencies but rather know on a more general level how for example telecommunication relies on power supply - used for looking at high level impacts and how a failure in one infrastructure sector can propagate to other infrastructure sectors (although not on an asset/component level). A lot of it is based on geographical proximity of assets. The main problem for the models is to get hold of data. Data is definitely a big problem, they know how the systems are generally connected and they know that backup solutions exist - however it is hard to assess which generator or asset that will actually fail and which backup solution that may also fail.

**Hazards models:** Focused on linking geospatial assets data and hazards geospatial characteristics using shape-files. Done a lot of earthquake, hurricane (+ surge modelling), flooding and terrorism threat modelling, capabilities that they use to simulate hazards impact on infrastructures. These tools were developed more towards getting a grip of the general risk level at a regional level (by different authorities such as FEMA) and not for more high granularity analyses - NISAC has then developed some algorithms to fill in the gaps in order to better assess the impact on individual infrastructure assets, including adding fragility models for the infrastructure assets. Can be used for looking at how the impact of e.g. an approaching hurricane and how it will hit the infrastructure and then couple economic models to assess the consequences that arise.

**Situational awareness tool:** It is kind of a GIS-application with assets in different sectors mapped (such as electric power and railway). It can be used to see e.g. what assets that will be affected by a Hurricane or flooding. It is mostly a depiction of assets and does not include models of the infrastructures. It is used currently mostly at the labs, but DHS have used it a bit. Most of the time however, DHS is scoping a question to NISAC. NISAC and DHS feels that it is always going to have to be a mixture depending on the skill set necessary. This type of tool is easy to use within 15 min, but e.g. electric power simulation tools require a whole different skill set. Right now NISAC and DHS are working through which levels that are appropriate (i.e. what should stay at NISAC and what can be used by DHS without erroneous results). Sometimes a kind of "hybrid-approach" is used where NISAC does e.g. a shape file (i.e. how the threat hits an area and its infrastructure) and then DHS can use the situational awareness tool to get an idea of what infrastructures that will be affected (i.e. what particular e.g. port that will be hit and the commodities and goods that wouldn't be able to be transported). The tool itself is not deployed yet, although seems to have the potential to become a powerful tool [interviewer's reflection]. One of the reasons for the tool is to more effectively be able to communicate to decision makers (instead of the traditional report type of reporting). Most what has been uploaded to the internet has been data and is hence data-driven, NISAC however also want to couple it with modeling and simulation capabilities.

**Type of analyses:** NISAC have done a lot of scenario-based analyses (i.e. coupled to a hazard) but also "vulnerability" oriented studies such as "N-k"-analyses (where k denotes number of failed infrastructure components). They have also looked into the problem with aging infrastructures and how climate change and changing demand patterns could give rise to additional stress, i.e. a more future outlook based approach. However, scenario analysis is the main bulk of the type of analyses NISAC carries out, as it is much easier to communicate and understand for external parties. For most of the analyses the focus is on the population getting affected (diseases, injured, etc.). Can be used to inform e.g. the health sector but also DHS for e.g. temporary housing and water - i.e. more long term supplies you have to bring in for covering the basic need of people.

**Validation of models:** For all models developed it is generally hard to do verification and validation as NISAC does not generally have the information and data to actually do verification and validation. In the transportation fuels model, pulling data from different sources, made it possible to determine how the system should work as there isn't really many degrees of freedom of how the system could work - not as good validation but gives you some reasonable bounds. When there are large scale events, they compare with their model outputs and use the empirical data to improve the models. They have also worked with utilities to validate their models, especially towards restoration/recovery and what actually got damaged of the infrastructure (e.g. working right now with a power distribution company and looking at outage data from the last twenty years and how quickly they managed to restore supply).

When trying to parametrize and validate models it is important to try and work and get feedback as much as possible with the industry. The main DHS viewpoint: it is better to have a model that is useful rather than absolutely correct (which is impossible, c.f. Box (1976) statement "Essentially all models are wrong but some are useful").

#### IV. Data collection and dissemination

Data is our (NISACs) achilles heel. Roughly 85% of the infrastructure is privately owned (off-quoted ref), i.e. the government really has to work with the industries in order to get hold of data and give incentives for the public industries to work with the issues. There is also a "tricky thing" with using regulatory agencies for this kind of work; hence much of it falls under DHS (i.e. trying to keep the regulatory people and the cooperators sufficiently separated to get it to work). Even if NISAC is not involved or support the regulatory environment, working with private companies they are afraid to give out data to the government as it could be used "against them".

As NISAC does not always get the data they would like to have, they have also developed algorithms/estimations of the impact based on general engineering practices and principles. Although missing data, some basic questions can be answered - however not to the level of detail as they would like to (but still reasonable results).

The general trend is that more and more municipalities are putting their data in GIS-format - i.e. making it more accessible (Historically it was made on papers - and not electronically which made alterations hard to follow up).

In general getting data for the transmission level for any infrastructure (e.g. power, gas, etc) is usually doable however getting it for the distribution level is much harder. But even at the transmission level they may not be georeferenced (i.e. no geospatial information about the assets).

Results are not really disseminated at the moment to a larger audience. Mostly towards DHS, but working on disseminating it to a larger groups.

We also had some discussions regarding the problem of determining the risk of aging infrastructures, sometimes age is not a good precursor of probability of failure (also DHS take on the issue after done some projects).

Hurricane Sandy was the last large event that activated DHS. DHS was lacking high granularity information from utilities of the impact it had on their systems (e.g. in general they knew roughly how many customers they lost but not where). There was also a lot of critical interdependencies that arose that they had not identified beforehand (e.g. there was a big chemical plant that had co-generation, but it needed the electricity grid to shift out there produced power - when the grid faltered the could no longer shift out their power production and the plant had to shut down for a couple of weeks). In general DHS



and NISAC has learned a lot from past events, such as hurricane Sandy and Katrina. Looking at this past events a lot of non-obvious dependencies can be found (i.e. not possible to sit behind the desk and figure out). Looking at specific asset/facilities, it is generally quite easy to figure out their backup capabilities, how much water they need, etc. But generalizing this to all other facilities in the country or even a metropolitan area is quite difficult.

*Are you using the tools to communicate with private companies to raise the issue of their importance and raise the understanding of interdependencies?* At the moment DHS are not doing it as much as they would like to for a broader audience. The development has been first communication from NISAC to DHS, then NISAC to also other federal agencies, while NISAC/DHS to public companies is still immature. It is still however not necessarily DHS or NISACs responsibility, rather a more natural channel would be through the private outreach program in accordance to the NIPP. NISAC do however some work with private companies regarding data and validation, but even if they find some critical dependencies that the company themselves are not aware of, they may not be able to do something about it due to economic reasons (e.g. might not be in the interest of the stakeholders). However, there is some grant money through the FEMA grant-program - but then it must be at a larger national strategic level. It has only been recently that US has started at looking at the resilience of infrastructures and dependency issues (earlier it was mostly a security focus). At state or local level it is likely that there are no funding possibilities for making more resilient infrastructures.

## V. Lessons learned and plans ahead

On the one side it is a challenge to effectively work in the way of the policy making and the decision making structures - working with all the stakeholders is one of the big challenges. On the other side it is a challenge to get the connections you need in order to get the necessary data. Another challenge is to frame the question and the problem in manageable sizes - i.e. Pick the small piece of the pie, do not try to do everything and do not start by building the "uber"-model.

NISAC has gone from modelling everything - to more specific questions and studies. Given the development of computers what is not feasible now might be so further down the line - hence it is important to stay flexible. It would be nice to have perfect data and to model everything together, but it is important to accept the questions you have might not be able to be answered with the highest fidelity and granularity and hence it is important to find ways of how to interpolate and find proxies and to make due when you have less than perfect information. It is also important to know the time frame for answering a question, is it one hour, several weeks or even years, as that defines what type of models and analyses you can use. It is also important to realize that you need competences, not only when building the tools but also during deployment - it is a work that requires skilled teams.

Something that has worked very well was to divide NISAC into 3 cluster areas 1) Crisis action analysis (look at things at a very short time frame), 2) Strategic analysis (Hurricane scenarios, sea-level rise, drought, earthquake etc. - i.e. planning for future plausible events), and 3) Capability development (maintaining and develop models and data to be able to answer the questions posed - during the years NISAC have been able to increase and automate some of their capabilities and questions that earlier took days to answer can now be answered within hours).

Who is posing the questions? Each sector has its own responsible authority. DHS have to reach out to some of the sector-specific agencies; they may have their own agenda and drive their development of capability in a certain direction that does not necessarily make sense for DHS (however understandable from their standpoint). The questions that DHS poses are either from DHS leadership or from the White House (only a couple of layers between DHS and White House national security staff).

Another key challenge is to develop reports or products: who are you going to distribute it to? How are you going to distribute it? And also what are going to be the review process - how do we assure the quality?

Communication usually is left to the end, but it is important to understand the audience and it easier to pull them in as early as possible and get them integrated in the process (the difference between making a difference or not). It is never the same questions being asked, e.g. the questions asked for Hurricane Katrina was completely different than those asked for Hurricane Sandy. In some respect you are always fighting the last war. Hence it is important to have a flexible capability, to accommodate both reactive and proactive development towards the questions asked, changing environment (e.g. from security, to vulnerability, to resilience) and changes in the demands of the infrastructures. It is also important to be able to go down the wrong path and hit some dead ends. Nothing that NISAC has done has been a complete waste of time, as they have learned and repurposed their work. But if with current knowledge going back to the years 2001/2002 there are definitely decisions that had been made differently (but part of the learning curve). In the beginning of NISAC, DHS was quite immature and there was no one to deploy the tools to. As DHS has matured the focus has shifted towards deploying web-based tools. The products from NISAC will always be more coupled to analysis, rather than tools.

Another challenge is to tackle the people criticizing what NISAC and DHS are doing. Since they, in some respect, are carrying out work and doing inquires at someone else's turf (e.g. sector specific agency) - competing interests. DHS have done some outreach and trying communicate that they have a slightly different focus and problem formulation (Crisis rather than steady-state) and that their work should be viewed more complementary than competing (e.g. FEMA wouldn't deploy food or water if there is a 15 minute power outage, only if it lasts during days or weeks - FEMA is not supposed to step in until local and state resources are depleted). It is important to find an area where you fit in.

Another problem is to find people with the right skill set to work with CIP-questions. No real education or degrees towards modelling/simulation within the area of critical infrastructure protection exist (except some courses more towards the management and risk side, e.g. at George Masons university). CIP is however a very new term and a new area of expertise, the first time it appeared was in the Presidential order from 1996. It takes a long time to train people with the right technical skills but also understand the domain in order to utilize their skills, which necessitates a stable work force. The Labs also have more flexible hiring routines and can target recruitment in specific subject matters, which is not as easily done at DHS. The Labs have a very extensive student programs with different universities that brings students in (e.g. Sandia brings in about 1000 students every year from June to September). At NISAC they have managed to pull together a variety of people with different skill sets, e.g. economists, infrastructure engineering, mathematicians, behavioral scientists, risk managers, etc.

Myndigheten för samhällsskydd och beredskap

651 81 Karlstad Tel 0771-240 240 [www.msb.se](http://www.msb.se)

Publ.nr MSB906 – september 2015 ISBN 978-91-7383-595-4