Bakgrunnsstudie til metode for identifisering og rangering av kritiske samfunnsfunksjoner

Kjetil Sørli, Stein Henriksen, Lene Bogen og Kristin Mørkestøl

Forsvarets forskningsinstitutt/Norwegian Defence Research Establishment (FFI)

23. mars 2007

FFI-rapport 2007/00875

1014

ISBN 978-82-464-1194-1

Emneord

Kritisk infrastruktur

Samfunnsfunksjoner

Risikoanalyse

Beslutningsstøtte

IKT

Godkjent av

Håvard Fridheim	Prosjektleder
Jan Erik Torp	Avdelingssjef

Sammendrag

Denne rapporten er en bakgrunnsstudie til BAS5-prosjektets rapport om en metode for å identifisere og rangere kritiske samfunnsfunksjoner og IKT-systemer. Den ivaretar behovet for dokumentasjon for metoderapporten, og har i tillegg fungert som et arbeidsdokument og en idébank underveis i utviklingen av metoden.

Bakgrunnsstudien har bidratt til at spørsmål har blitt reist og drøftet underveis. For eksempel: Hvilke svar ønsker vi at en norsk metode skal gi? Skal den gi svar på hva som er mest kritisk innen en sektor, innen en funksjon eller innen en viss type infrastruktur. Skal man avgrense seg til objekter eller større systemer? Hva slags beslutningssituasjoner skal den understøtte, for eksempel i forhold til før, under eller etter en krise; i forhold til styring av nasjonale ressurser på et overordnet nivå eller i forhold til prioritering av beredskapsressurser? Skal den bidra til å avdekke områder for videre analyser, for eksempel ROS-analyser? Skal den være et redskap for forvaltningen, eller skal den være et verktøy hvor private og offentlige virksomheter finner egne kritiske punkter?

Det reises videre spørsmål om hvor detaljert og omfattende metoden bør være, hvilke forkunnskaper som må til for å kunne anvende metoden, og om hvordan metoden skal vedlikeholdes og videreutvikles.

Målgruppen for bakgrunnsstudien er snevrere enn målgruppen for metoderapporten, og består primært av BAS5-prosjektgruppen og de som dokumentasjonsbehov ut over det som er dokumentert i metoderapporten.

English summary

The report documents supplementary work done in BAS5 in developing a methodology to identify and rank critical societal sectors and ICT systems. It provides necessary documentation for the work with the methodology, and it has also had the role of an ideas bank as the methodology has been developed.

The report raises and discusses questions, for instance: Which questions should a Norwegian methodology address? Should it aim to provide an answer as to what is most critical within a single sector or an infrastructure? Should it address large systems, or even include singular objects within infrastructures? In what kind of situations should it be used; before, during or after a crisis? Can it be used to direct national emergency preparedness resources? Should it help in identifying areas for further analysis (including risk analysis)? Is it to be a tool for the government, or should it also be a methodology usable for private and public enterprises? Furthermore, how detailed and extensive can the methodology possibly be, what qualifications are needed by its users, and how should the methodology be developed and maintained?

The target group for this report is narrower than the report on the methodology. Primarily, this report is written for the BAS5 project group and others with need for supplementary information on the methodology.

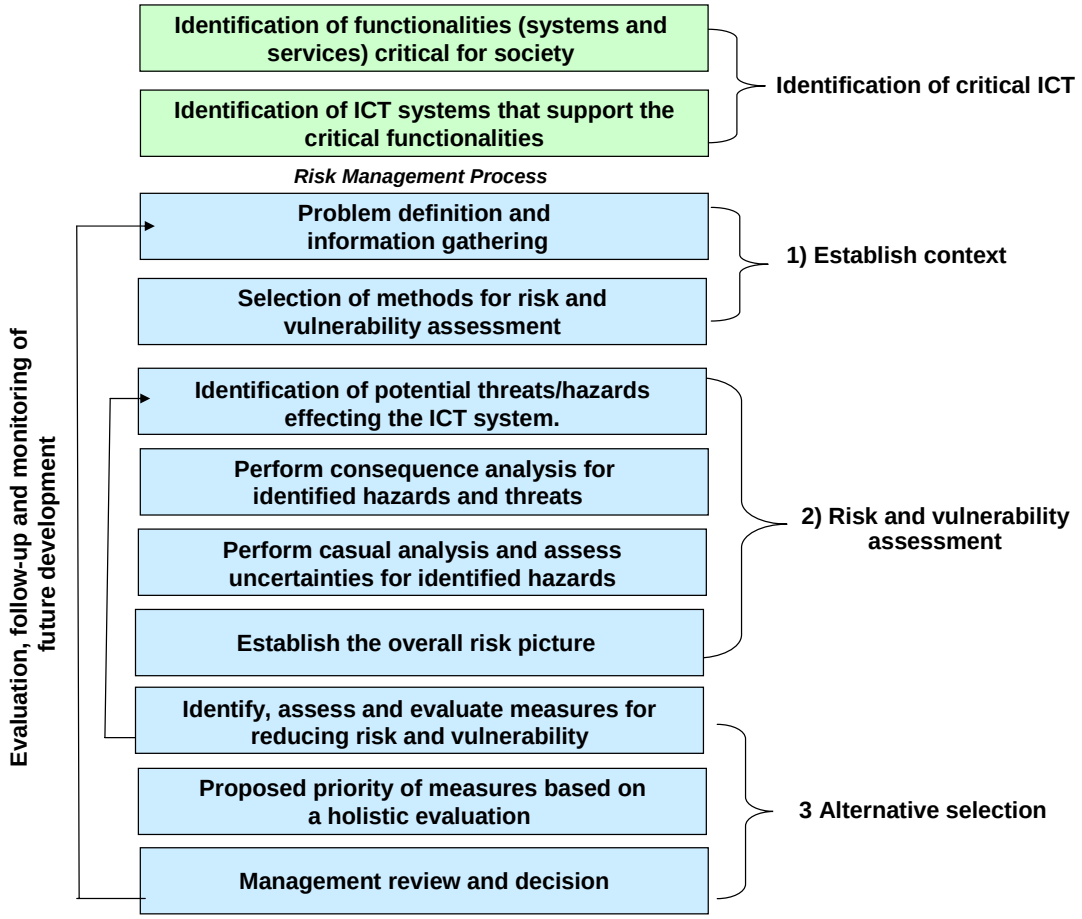
Innhold

1 Innledning

Studien er en del av forskningsprosjektet BAS5 om sårbarhet i samfunnskritiske IKT-systemer. Studien inngår i den tredje av prosjektets opprinnelige hovedmålsettinger:

1. Utvikle og anvende en ROS-metode på samfunnsviktige IKT-systemer
2. Utvikle og anvende en metodikk for å rangere tiltak som reduserer sårbarheten
3. **Utvikle og anvende en metode for å rangere kritiske IKT-systemer og samfunnsfunksjoner**

Arbeidet har bestått av to hovedstudier: En bakgrunnsstudie og en metoderapport. Denne rapporten (bakgrunnsstudien) har som formål å dokumentere og synliggjøre bakgrunnen for metoderapporten.[1] Todelingen er gjort for å rendyrke metoden i en egen rapport, samtidig som at krav til dokumentasjon og drøfting blir ivaretatt.



Figur 1.1. Sammenhengen mellom hovedmålsetting 1 og 3. Hovedmålsetting 3 i grønt øverst, hovedmålsetting 1 nederst i blått

[1] Henriksen, Stein. Sørli, Kjetil. Bogen, Lene. 2007. Metode for identifisering og rangering av kritiske samfunnsfunksjoner. FFI/RAPPORT-2007/00874.

Metoden må ses i sammenheng med BAS5-prosjektets første hovedmålsetting om utvikling og anvendelse av en ROS-metode for samfunnsviktige IKT-systemer. Sammenhengen er illustrert i Figur 1.1., hvor hovedmålsetting tre er markert i grønt, mens hovedmålsetting én er markert i blått. Ved å først identifisere og rangere kritiske IKT-systemer og samfunnsfunksjoner (hovedmålsetting tre), etableres det kunnskap om hvilke IKT-systemer som er så kritiske for samfunnet at det er hensiktsmessig å gjennomføre en ROS-analyse (hovedmålsetting én).

BAS5-prosjektets tredje hovedmålsetting må også ses i sammenheng med et uttalt behov fra myndigheter og private virksomheter om å ha tilgjengelig et verktøy for å identifisere og rangere kritiske objekter, systemer og funksjoner. Det gir myndighetsorganer og offentlige og private virksomheter et bedre grunnlag for å prioritere og å fordele sikkerhets- og beredskapsressurser.

I tillegg til at denne rapporten ivaretar behovet for dokumentasjon for metoderapporten, har den fungert som et arbeidsdokument og en idébank underveis i utviklingen av en metode. Den har bidratt til at spørsmål har blitt reist og drøftet underveis. For eksempel: Hvilke svar ønsker vi at en norsk metode skal gi? Skal den gi svar på hva som er mest kritisk innen en sektor, innen en funksjon eller innen en viss type infrastruktur. Skal man avgrense seg til avgrensede objekter eller større systemer? Hva slags beslutningssituasjoner skal den understøtte, for eksempel i forhold til før, under eller etter en krise; i forhold til styring av nasjonale ressurser på et overordnet nivå eller i forhold til prioritering av beredskapsressurser? Skal den bidra til å avdekke områder for videre analyser, for eksempel ROS-analyser? Skal den være et redskap for forvaltningen, eller skal den være et verktøy hvor private og offentlige virksomheter finner egne kritiske punkter? Det er videre spørsmål om hvor detaljert og omfattende metoden burde være, hvilke forkunnskaper som må til for å kunne anvende metoden, og spørsmål om metoden skal vedlikeholdes og videreutvikles – og i så fall av hvem.

1.1 Målgruppe for rapporten

Målgruppen for bakgrunnsstudien er snevrere enn målgruppen for metoderapporten, og består primært av BAS5-prosjektgruppen og de som dokumentasjonsbehov ut over det som er dokumentert i metoderapporten.

1.2 Målgruppe for en metode

1.2.1 Systemeier

Hvem skal benytte, vedlikeholde og videreutvikle metoden? Det kan tenkes at alle fra den enkelte virksomhet til sektormyndighet eller en tverrsektoriell myndighet har behov for å benytte metoden. For eksempel kan en større privat virksomhet ha behov for å identifisere og rangere virksomhetskritiske systemer og objekter. Det kan også tenkes at et sektordepartement ønsker å identifisere og rangere sektorens mest kritiske objekter ut fra behovet for å prioritere sikkerhets- og beredskapsmidler.

Erfaringsmessig ligger behovet for identifisering og rangering på alle nivåer, alt fra den enkelte

private virksomhet til tverrsektorielle myndigheter. Normalt er det også slik at det er de tverrsektorielle myndighetsorganene og forskningsinstitusjonene som blir bedt om å bistå ulike virksomheter og myndighetsorganer ved behov. I denne sammenheng vil det si Direktoratet for samfunnssikkerhet og beredskap (DSB), Forsvarets forskningsinstitutt (FFI) og Nasjonal sikkerhetsmyndighet (NSM). DSB gjør dette ut fra sine oppgaver og kompetanse knyttet til samfunnssikkerhet og beredskap i samfunnet som helhet, FFI ut fra sin kompetanse fra BAS-prosjektene og NSM ut fra sitt arbeid med å identifisere og verdivurdere skjermingsverdige objekter.

Det kan derfor være naturlig at ansvar for vedlikehold og videreutvikling av metoden ligger hos én eller flere av disse. I tillegg har DSB og NSM som tverrsektorielle myndigheter behov for å bruke metoden på egne problemstillinger. Ansvaret for gjennomføringen av prosjekter som benytter metoden, og eierskap til resultater fra metoden må ligge hos systemeier, men med bistand fra eksempelvis FFI, DSB eller NSM.

1.2.2 Mulig overordnet prosess

Eierskap, drift og videreutvikling av metoden har sammenheng med hvilket ambisjonsnivå man legger seg på. Ved et lavere ambisjonsnivå kan problemstillingene avgrenses til å produsere lister av typen; hvem skal få prioritet i mobilnettet ved større kriser. Ved et høyere ambisjonsnivå kan problemstillingen være av typen; hvordan skal beredskapsressursene fordeles i samfunnet som helhet.

Hvis metoden skal dekke et lavere ambisjonsnivå med avgrensede problemstillinger, kan det tenkes at en eller to tverrsektorielle sikkerhets- og beredskapsmyndigheter sammen forvalter og vedlikeholder metoden. De som har behov kan da henvende seg til disse for bistand. Dette kan omtales som en *bistandsmodell*. Ved et høyere ambisjonsnivå med større problemstillinger, må det gjennomføres en møysommelig byråkratisk prosess som involverer et større antall virksomheter og etater, og hvor én etat blir nasjonal samordningsmyndighet. Oppgavene til den nasjonale samordningsmyndigheten vil være å koordinere, gi råd og sammenfatte. Denne modellen kan omtales som en *byråkratisk prosessmodell*.

I en *byråkratisk prosessmodell* administrerer den nasjonale samordningsmyndigheten prosessen. Prosessen vil bestå av å (1) hente inn informasjon gjennom ansvarlige sektordepartementer, (2) samle informasjonen i et sammenlignbart format og (3) etablere enighet om resultatene.

Innhenting av informasjon (1) kan bestå av en årlig revisjonssyklus i forhold til ansvarlige departementer. Departementene kan delegere oppgaven til samvirkegrupper som igjen involverer sektorens virksomheter, bransjeorganisasjoner, tjenesteleverandører, eiere av kritiske samfunnsfunksjoner og så videre. Informasjonen blir innhentet og rapportert via samvirkegruppene til ansvarlig departement. Departementet tar den endelige prioriteringen innen sin sektor. Ved behov kan fylkesmannen koordinere og innhente informasjons regionalt. Formatet på informasjonen (2) vil være forutbestemt av metoden, slik at det er mulig å sammenligne informasjon innad i sektoren, og på tvers av sektorene. Den nasjonale samordningsmyndigheten

(3) vil sammenstille nasjonal prioritering etter en konsensusprosess. En byråkratisk prosessmodell må utarbeides i større detalj, og vil kunne bli en nasjonal ROS-analyse.

1.3 Avgrensinger og anvendelsesområder

Metoden som utvikles skal i følge målsetningen for BAS5 brukes til å (1) identifisere og (2) rangere kritiske IKT-systemer og kritiske samfunnssfunksjoner. Dette lar seg imidlertid neppe avgrense kun til en snever definisjon av IKT-systemer, i det IKT-systemer griper inn i alle samfunnets områder. I praksis vil en avgrensing av målsettingen omhandle kritiske infrastrukturer og kritiske samfunnsfunksjoner. Studien vil derfor måtte omfatte en identifisering og rangering av alle kritiske infrastrukturer og samfunnsfunksjoner, ikke bare kritiske *informasjons*infrastrukturer.

Ovenfor er det nevnt at det er klart slektskap mellom delmålene i BAS5-studien. En sterkt medvirkende årsak til det er at det knapt er mulig å identifisere kritiske infrastrukturer uten samtidig å gjøre seg opp en mening om hvilke risikoer og sårbarheter de er utsatt for; det vil si at det må foretas risiko- og sårbarhetsvurdering (ROS-vurdering) på sektor- og virksomhetsnivå. Det går et skille i målsetning mellom en slik ROS-vurdering, og identifisering og rangering av den aktuelle kritiske infrastrukturen i sammenligning med andre kritiske infrastrukturer. Hvis dette arbeidet aggregeres til et felles nasjonalt nivå, vil det imidlertid utgjøre et vesentlig aspekt av en nasjonal tverrsektoriell ROS-vurdering.

En metode for identifisering og rangering av kritiske infrastrukturer og kritiske samfunnsfunksjoner, vil ha potensielle anvendelser og implikasjoner som er bredere enn målsetningene for BAS5. En metode vil kunne ha som målsetting å være i stand til å sammenligne en rekke ulike fenomener, sektorer, policyer og for så vidt også nasjoner. Prioriterte lister over diverse funksjoner, infrastrukturer og installasjoner vil være interessante i mange situasjoner og for mange formål. Eksempler på dette kan være å lage begrunnede innspill til svar på følgende:

- Hvem bør ha prioritert adgang til teletjenester i krisesituasjoner?
- Hvem bør få vaksine i en pandemisituasjon og i hvilken rekkefølge?
- Hvilke IKT-systemer skal prioriteres ved kraftmangel?
- Hvilke andre samfunnsfunksjoner skal prioriteres ved kraftmangel?
- Hvor lønner det seg å sette inn investeringer for å forebygge kriser?
- Hvilke installasjoner bør prioriteres for fysisk beskyttelse?
- Hvor er de mest kritiske punktene i norsk olje- og gassproduksjon?
- Hvilke virksomheter bør være underlagt Sikkerhetslovens bestemmelser?
- Hva skal bygges opp igjen først etter en naturkatastrofe?
- Hvilke samfunnsområder bør ha særlig oppmerksomhet omkring ROS-vurderinger?

I tillegg vil tilstedeværelsen av en slik metode ha implikasjoner for alminnelig politisk bevisstgjøring omkring kritiske infrastrukturer spesielt og samfunnssikkerhet generelt.

1.4 Kapittelinndeling

Studien er delt i to deler. Den første delen inneholder gjennomgang og drøfting av relevante begreper og teorier. Del to beskriver ulike metoder som er relevante for å identifisere og rangere kritiske samfunnsfunksjoner.

Studien starter i del I med en gjennomgang av behovet for en metode for å identifisere og rangere kritiske samfunnsfunksjoner i kapittel to. I kapittel tre gis en gjennomgang av begreper som er knyttet til identifisering og rangering av kritiske samfunnsfunksjoner.

I kapittel fire vises det til hvordan begreper knyttet til teorier utviklet av Charles Perrow, og teorier utviklet av Klinke og Renn kan brukes som kriterier. Videre viser studien i kapittel fem, to forskjellige måter å liste kritiske sektorer, samfunnsfunksjoner og kritisk infrastruktur på. Den ene viser til hvem/hva som er kritiske i en krisesituasjon. Den andre viser til hva som blir ansett som sektorer med kritisk infrastruktur. Begge er til dels overlappende, men forskjellene kan gi seg utslag i forskjellige tiltak. I del II, kapittel seks, redegjøres det for forskjellige lands metoder for å identifisere og å rangere.

Del I – Relevante begreper og teorier

2 Hvorfor en metode for å identifisere og rangere?

Samfunnet er avhengig av ulike typer teknologi, systemer og ressurser for å fungere. Enkelte av disse er mer kritiske enn andre, og enkelte er mer sårbare enn andre. I etterkrigstiden førte slike erkjennelser til at det ble bygget opp et apparat for å sikre kvalitet av og tilgjengelighet til det som ble vurdert som helt nødvendig for samfunnet. Rammen for denne satsingen var en permantent tilstedeværelse av kald krig og en overhengende trussel om den totale krig.

Prinsippet om totalforsvar av landet var dimensjonerende. Alle samfunnets ressurser skulle ved sikkerhetspolitiske kriser og krig rettes inn mot å forsvare seg mot en ekstern fiende, og samfunnet skulle i størst mulig grad fungere ved krig. Det var et særlig fokus på forskjellige beredskapstiltak, for eksempel forsyninger av mat og medisiner til Forsvaret og sivilbefolkningen ved krise og krig. Også kraftforsyningen ble ansett som så viktig for driften av samfunnet at det bl.a. ble iverksatt fysiske sikringstiltak ved kritiske installasjoner. Flere andre sektorer iverksatte tiltak. I telesektoren ble det for eksempel gitt prioritet i telefonnettet til personer som ble vurdert som viktige i en krise/krigssituasjon. Sikring av det som er ansett som mest kritisk for samfunnet er derfor ikke noe nytt, og det er en tradisjon i Norge å institusjonalisere beskyttelsestiltak.

Denne tankegangen blir nå kontinuerlig utfordret av endringer i Norges sikkerhetspolitiske rammer, tilgang på nye tjenester, tilgang til og utnyttelse av ressurser og organisatoriske og strukturelle endringer i samfunnet. En drivende endringsfaktor er og har vært videreutvikling og bruk av kjent og ny teknologi. I de senere år har særlig utviklingen av nye IKT-tjenester vært viktig. En annen faktor er endringer i hvordan leveranser av samfunnskritiske tjenester er satt i system. For eksempel er det relativt enkelt å sette opp ett trafikklys, men noe helt annet å regulere lyssignalene i en hel by.[2] På samme måte er det relativt enkelt å forsyne én lyspære med strøm, eksempelvis med et aggregat. Å forsyne en landsdel med strøm gjennom et nettverk er noe annet. Det meste må settes inn i et system av politisk, sosialt, forvaltningsmessig, teknologisk og økonomisk art for å fungere. Disse forskjellige systemene er i kontinuerlig endring.

Økende fysisk sammenkobling, nye styringssystemer og teknisk og organisatorisk sentralisering gjør at det i mindre grad enn tidligere er relevant å snakke om et samfunn bestående av separate systemer. På den ene siden har vi fått bedre tjenester med større kapasitet, på den andre siden øker kompleksiteten på grunn av det voksende antallet kontaktpunkter mellom systemer og mellom systemer og brukere.

Sammen med endringer i systemer, kompleksitet og teknologi, har samfunnets avhengighet endret

[2] Schneier, Bruce. 2003. Beyond Fear. Thinking Sensibly about Security in an Uncertain World. Copernicus Books.

seg. Den har endret seg fordi ny teknologi erstatter eldre. Et eksempel er urbane områders avhengighet av elektrisitet for oppvarming. Når vedovnen kasseres, forsvinner også muligheten for oppvarming ved strømbrudd. Samtidig er gevinsten stor når elektrisitetsforsyningen fungerer. Det er enklere å håndtere, faren for brann reduseres og lokal forurensing i urbane områder blir langt mindre.

Avhengigheten har også endret seg fordi det kommer nye tjenester som det forventes er tilgjenglige. Det gjelder eksempelvis bruken av Internett som informasjonsbærer, hvor virksomheter gjør seg avhengige av nye tjenester som de selv ikke har kontroll over. Også samfunnsviktige brukere gjør seg avhengig av ny teknologi. Et eksempel er økende bruk og avhengighet av mobiltelefoni blant personer som innehar sentrale roller i håndteringen av ulykker og katastrofer.[3]

Tjenester er også mer spesialiserte, og det påvirker vår avhengighet. Hvis noe går i stykker, er vi avhengig av spesialister for å reparere.

Endringene har ført til et samfunn som er sårbart for avbrudd i kritiske infrastrukturer og samfunnsfunksjoner. Endringene har også ført til nye kritiske områder og punkter i samfunnet. Det er naturlig å anta at dette vil fortsette å være i endring.[4] Parallelt så har endringene også ført til et bedre og tryggere samfunn. Antall tjenester øker, tilgjengeligheten til tjenestene øker og de har blitt mer robuste. Samfunnsutviklingen innenfor dette området bærer derfor preg av en tosidighet, med økende sårbarhet og avhengighet på den ene siden, og økende tilgjengelighet og robusthet på den andre siden.

I de siste årene har trekk i samfunnsutviklingen ført til ny oppmerksomhet omkring kritiske infrastrukturer. Det gjelder blant annet i forhold til en økende bevissthet om samfunnets avhengighet av kritiske infrastrukturer, et nytt og diffust terrortrusselbilde, klimaendringer og den eksplosive utviklingen av informasjons- og kommunikasjonsteknologi (IKT). Disse trekkene er deler av et utviklingsbilde som blant annet er beskrevet i Organisasjonen for økonomisk samarbeid og utvikling (OECD) sin rapport *Emerging Systemic Risks*.[5] Her vises det til en rekke utfordringer som dukker opp samtidig over hele verden som en del av globaliseringen. En viktig del av dette er IKT.

I løpet av få år er IKT blitt allestedsnærværende i alle samfunnssektorer. Den tette symbiosen mellom kraftforsyning, telekommunikasjon og informasjonsteknologi begynner å bli allment kjent. Imidlertid har IKT bidratt til omfattende gjensidige avhengigheter, symmetriske og asymmetriske, mellom de aller fleste sentrale og viktige samfunnsfunksjonene og infrastrukturene. Bruken av IKT i styringssystemer har utviklet seg slik at det kan være tvil om

[3] Post- og teletilsynet 2003. *Risiko og sårbarhetsanalyse av mobilnettene i Norge*. Saksnummer: 200205841. (Unntatt off i.h.t. offentlighetsloven § 6.1. ledd nr. 1)
[4] Inn i en slik diskusjon faller også begrepet forventninger, og da sett i forhold til kvalitet, mangfold og oppetid på leveranser av varer og tjenester. En slik diskusjon vil ikke bli foretatt her, ut over å fastslå at forventingene til kvalitet, mangfold og oppetid ikke blir mindre etter hvert.
[5] OECD. 2003. *Emerging risks in the 21st century*. An OECD international futures project.

det er mulig å drifte vitale systemer uten IKT. Den ekstreme sammenkoblingen som blant annet skjer via Internett, aktualiserer spørsmålet om i hvilken grad feil ett sted kan forplante seg gjennom alle kritiske systemer i samfunnet. Ondsinnet datakode er et allment kjent eksempel på slike fenomener.

3 Definisjoner og drøfting av relevante begreper

I dette kapittelet drøftes relevante begreper for metoderapporten.

3.1 Samfunnets verdier, kritiske samfunnsfunksjoner og kritisk infrastruktur

For å få en riktig anvendelse av en metode, må det presiseres hvilket nivå den skal omfatte. I det følgende presenteres ulike begreper som er relevante i en metode for å identifisere og rangere kritiske samfunnsfunksjoner og kritiske infrastrukturer.

På bakgrunn av at dette er en bakgrunnsstudie, er ikke hensikten å konkludere, men å bevisstgjøre og danne grunnlag for diskusjon om hvordan vi med begreper tydeliggjør det som er mest kritisk for samfunnet.

3.1.1 Samfunnskritisk, kritisk og viktig

Begreper som funksjoner og infrastruktur er ofte akkompagnert av ord som ”viktig”, ”kritisk” og ”samfunnskritisk”. Begrepet funksjon blir i denne sammenheng også fremstilt som ”kritisk samfunnsfunksjon”. Som regel blir det ikke gitt noen begrunnelse på hvorfor det ene eller det andre forsterkende ordet blir benyttet. Begrepsbruken varierer også internasjonalt. Også begrepet ”sektor” blir benyttet i slike sammenhenger.

Det er ikke lagt opp til noen diskusjon eller analyse i teksten om bruk av forskjellige forsterkende ord. For å understreke at det er samfunnet som er utgangspunktet for analysen, og at høy grad av kritikalitet er sentralt, vil det for vårt formål bli brukt begrepet ”kritisk samfunnsfunksjon”. For å beskrive infrastruktur som er kritisk for samfunnet, er begrepet ”kritisk infrastruktur” allerede etablert nasjonalt og internasjonalt, og vi vil forholde oss til det.

3.1.2 Definisjoner av kritisk infrastruktur

En tilnærming for å klargjøre hva som er kritisk for samfunnet, er å ta utgangspunkt i begrepet kritisk infrastruktur og definisjonen av den. Internasjonalt eksisterer det svært mange definisjoner. I USA er det sågar identifisert åtte forskjellige definisjoner i perioden 1983-2004.[6]

Felles for de definisjonene som denne studien har sett på, er at det er skapt en helhetlig definisjon ut fra hovedsaklig én setning. Felles er også at fokus i definisjonene er på konsekvensene for samfunnet ved bortfall og at infrastrukturen er vesentlig for at samfunnet skal fungere. Bruken av kriterier er også fremtredende hos en del av definisjonene.

[6] Moteff, John and Parformak, Paul. 2004. *Critical Infrastructure and Key Assets: Definition and Identification.* CRS Report for Congress.

Canada har følgende definisjon:

> *Critical infrastructure consists of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada.*[7]

USA har følgende definisjon:

> *Critical infrastructure are systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*[8]

Danmark har følgende definisjon:

> *[Kritisk infrastruktur] kan forstås som de elementer i et overordnet system (samfund), der er så vitale, at forstyrrelse og nedbrud af bare en enkelt af dem ville kunne true selve systemets funktionsduelighed.*[9]

Sverige har følgende definisjon:

> *Med samhällsviktig infrastruktur avses grundläggande system i samhället som är väsentliga för att samhället skall fungera och som direkt eller indirekt används av flertalet invånare.*[10]

Det regjeringsoppnevnte utvalget for beskyttelse av kritiske infrastrukturer og kritiske samfunnsfunksjoner (Infrastrukturutvalget) kom våren 2006 med følgende definisjon:

> Kritisk infrastruktur er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse.[11]

Det kan hevdes at det er en utfordring å operasjonalisere kritisk infrastruktur, basert på en definisjon. Som begrep er det ment å beskrive at noen typer infrastrukturer er mer kritiske for samfunnet enn andre.

3.1.3 Kritisk infrastruktur og kritiske samfunnsfunksjoner

Kritiske samfunnsfunksjoner kan bli brukt for å beskrive de funksjonene som understøtter samfunnet, og som samfunnet er svært avhengig av for å fungere. Ved bortfall stopper varer og tjenester som befolkningen er avhengig av. På et overordnet nivå er enkelte så kritiske for

---

[7] http://www.ocipep.gc.ca
[8] US Senate. 2001. *US Patriot Act of 2001*. H.R. 3162
[9] Beredskapsstyrelsen. 2004. *National Sårbarhedsudredning*. Udvalget for National Sårbarhedsudredning
[10] Planeringsprocessen. 2003:7. *Samhällets krisberedskap 2005. Planeringsinriktning.* Krisberedskapsmyndigheten.
[11] NOU 2006:6. *Når sikkerheten er viktigst.*

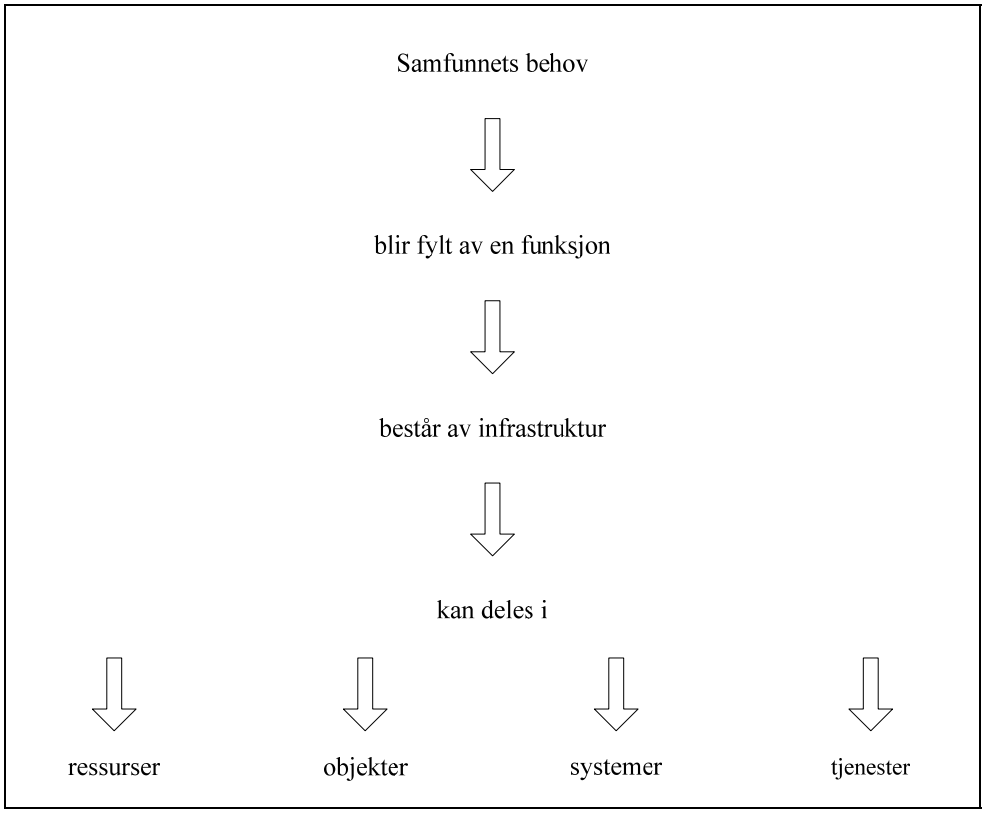
samfunnet at de omtales som bærebjelker. Bortfall av bærebjelkene vil merkes umiddelbart, og omfatter funksjoner som kraftforsyning, telekommunikasjon, ledelse/informasjon og forsyning av rent vann og ernæring.[12] Renovasjon kan også omtales som en kritisk samfunnsfunksjon, men bortfall får konsekvenser først på lengre sikt og blir derfor ikke bli omtalt som en bærebjelke. Hvor kritisk en samfunnsfunksjon faktisk er kan også være situasjonsbestemt, eksempelvis funksjonene territorialforsvar og nasjonale beredskapssystemer. Det er først ved gitte situasjoner slike samfunnsfunksjoner er kritiske for samfunnet.

Leveranse av en kritisk samfunnsfunksjon er avhengig av tilgang til gitte *ressurser, objekter, systemer og tjenester*. Eksempelvis er funksjonen strømforsyning i Norge avhengig av vann (ressurser), damanlegg (objekter), datakontrollsystemer (systemer) og softwareleverandører (tjenester). Ressursene, objektene, systemene og tjenestene kan omtales som infrastruktur og funksjoner som understøtter den kritiske samfunnsfunksjonen. De mest kritiske infrastrukturene som understøtter samfunnsfunksjonen, kan kalles kritisk infrastruktur. En tilsvarende tilnærming blir lagt til grunn i Infrastrukturutvalgets rapport. Der blir det hevdet at kritisk infrastruktur er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner.[13]

Med en slik tilnærming er det samfunnets behov som utgjør utgangspunktet for hva som er kritisk infrastruktur: Samfunnet har behov for rent drikkevann; hvilken infrastruktur sørger for det? Samfunnet har behov for et fungerende regjeringsapparat; hvilken infrastruktur sørger for det? Samfunnet har behov for transport; hvilken infrastruktur sørger for det og så videre. De mest kritiske funksjonene dekker opp for de mest kritiske behovene som samfunnet må oppfylle, og funksjonene er avhengig av infrastruktur i form av ressurser, objekter, systemer og tjenester. Skjematisk kan det fremstilles slik:

[12] Hæsken, Ole Morten. Olsen, Thor Gunnar. Fridheim, Håvard. 1997. *Beskyttelse av samfunnet (BAS) – Sluttrapport.* FFI/RAPPORT-97/01459; Aven, Terje. Boyesen, Marit. Njå, Ove. Olsen, Kjell Harald. Sandve, Kjell. 2004. *Samfunnssikkerhet*. Universitetsforlaget; Fridheim, Håvard. Hæsken Ole Morten. Olsen Thor Gunnar. Balke, T, Ensrud May-Kristin. 1997. *Viktige samfunnsfunksjoner*. FFI/RAPPORT-97/01458 (Begrenset)

[13] NOU 2006:6. *Når sikkerheten er viktigst*.



Figur 3.1. Samfunnets behov som utgangspunkt for hva som er kritisk infrastruktur.

Fremgangsmåten gir en logisk tilnærming for å vurdere hva som er mest kritisk for samfunnet med utgangspunkt i funksjoner og behov. På den annen side gir den ingen helhetlig tilnærming til hvilken av funksjonene som er mest sårbare og utsatte for bortfall. Sluttrapporten etter BAS4-prosjektet ga en illustrasjon på det. Transport er en kritisk funksjon for samfunnet, men på grunn av stort tilbud, ulike transportformer og redundans ble den ikke vurdert som *sårbar*. Derimot ble den vurdert som *utsatt* for enkelte scenarier så som terrorhandlinger.[14]

En tilnærming til hva som er samfunnets grunnleggende behov, er å ta utgangspunkt i Maslows behovspyramide. Den er delt opp i (1) selvrealisering, (2) egoistiske behov, (3) sosiale behov, (4) trygghet og (5) fysiske behov. De grunnleggende behovene som kritisk infrastruktur og samfunnets kritiske funksjoner kan tenkes å dekke, kan omtales å være (4) trygghet og (5) fysiske behov.

3.1.4 Kategoriseringer av kritiske samfunnsfunksjoner[15]

Beskrivelser av kritiske samfunnsfunksjoner er som oftest av teknisk karakter, og tar ikke høyde for at forhold som kompetanse er en kritisk innsatsfaktor for funksjonsdyktigheten. Det kan stilles spørsmål om det ikke også vil være fruktbart å identifisere denne ressursen, og på den måten legge bedre til rette for en presis virkemiddelbruk. Dette kan eksempelvis gjøres ved å omtale de

[14] Hagen, Janne M. Rodal, Gry Hege. Hoff, Erlend. Lia, Brynjar. Torp, Jan Erik. Gulichsen, Steinar. 2003. *Beskyttelse av samfunnet med fokus på transportsektoren.* FFI/RAPPORT-2003/00929

[15] Kategoriseringen av kritiske samfunnsfunksjoner er gjort etter innspill fra Jørn Vatn, NTNU.

funksjoner som må være på plass for at den *primære funksjonen* skal fungere, for *sekundære kritiske samfunnsfunksjoner*. Dette kan være forhold som kompetanse for å drifte og vedlikeholde kraftproduksjonen. En tydeliggjøring mellom primære og sekundære kritiske samfunnsfunksjoner vil kunne bidra til å synliggjøre forhold som for eksempel manglende rekruttering i drifts- og vedlikeholdsoppgaver i kritisk infrastruktur.

I tillegg til å operasjonalisere begrepet kritisk samfunnsfunksjoner ut fra om den er *primær* eller *sekundær*, kan begrepet operasjonaliseres ut fra en tidsdimensjon. En *umiddelbar* kritisk samfunnsfunksjoner omhandler de funksjonene som kreves i en normalsituasjon, og hvor svikt får umiddelbare konsekvenser. Forsyning av elektrisitet er et eksempel på en umiddelbar kritisk samfunnsfunksjon.

En *skadereduserende* kritisk samfunnsfunksjon er en funksjon som først blir påkrevd etter at en uønsket hendelser har oppstått. Brann, helse og politi er eksempler på kritiske samfunnsfunksjoner som i stor grad er skadereduserende.

En *forebyggende* kritisk samfunnsfunksjon er viktig i en generell forebyggende kontekst, uten at funksjonen vil være direkte knyttet til en uønsket hendelse eller en kritisk situasjon. Eksempler på dette er brann, helse og politiets forebyggende funksjoner samt det meste av statlig tilsynsvirksomhet.

En *regulerende* kritisk samfunnsfunksjoner har som formål å regulere aktivitet. Dette kan eksempelvis være forbud mot visse typer aktiviteter som er uønsket fra samfunnets side. Herunder inngår lover, regler og forskrifter.

3.1.5 Begrepet ”samfunnets grunnleggende verdier”

Begrepet viser til verdier som er grunnleggende for å opprettholde en normaltilstand i samfunnet. I utgangspunktet det et svært omfattende begrep som er vanskelig å avgrense. Det foreligger heller ingen omforent definisjon som presiserer det. Å fylle begrepet med innhold er derfor en subjektiv vurdering preget av hva man ønsker å bruke det til. Forhold som politikk, ideologi og trusseloppfatning bidrar til å forme det.[16] I denne sammenheng er det naturlig å ta utgangspunkt i begrepet slik det er omtalt i dokumenter knyttet til forsvar og samfunnssikkerhet.

I sårbarhetsutvalgets rapport fra 2000 er samfunnets grunnleggende verdier omtalt flere steder. De blir omtalt som ”sentrale samfunnsverdier”, ”viktige verdier i samfunnet” og ”grunnleggende og viktige samfunnsverdier”. For eksempel:

> Samfunnet skal sikres mot utfordringer mot sentrale samfunnsverdier som liv, folkehelse og velferd, livsmiljøet, det demokratiske system og dets lovlige institusjoner, nasjonal styringsevne og suverenitet, landets territoriale integritet, materiell

[16] Lewerentz, Birgitta. Frost, Christina. Marklund, Anna. Franzén, Göran. Wahlberg, Maria. Ånäs, Per 2005. *Kriteriemodell för identifiering av samhällsviktiga verksamheter och system.* FOI Memo 1283. Totalförsvarets forskningsinstitut.

> og økonomisk trygghet og kulturelle verdier.
> …
> Risiko uttrykker fare for tap av viktige verdier som følge av uønskede hendelser. Viktige verdier kan for eksempel være liv og helse, miljø, økonomi og gjennomføring av kritiske samfunnstjenester.
> ...
> Utvalget legger til grunn at en krise er en hendelse som har potensiale til å true viktige verdier og svekke en organisasjons evne til å utføre viktige funksjoner.[17]

I langtidsmeldingen for Forsvaret for 2005-2008 er verdier knyttet til samfunnet omtalt slik:[18]

> I tillegg til stats-, samfunns- og menneskelig sikkerhet, er det å beskytte velferd, miljø og økonomisk trygghet for det norske folk, grunnleggende norske sikkerhetsinteresser. […] Videre inngår enkelte grunnleggende verdier som viktige komponenter blant Norges sentrale sikkerhetsinteresser. […] Norske sikkerhetsinteresser berøres derfor av utfordringer som kan true den internasjonale rettsorden, menneskerettighetene, demokrati, rettsstatens prinsipper, økonomisk trygghet og livsmiljøet.

De to dokumentene omtaler samfunnets grunnleggende verdier som liv, folkehelse og velferd, livsmiljøet, det demokratiske system og dets lovlige institusjoner, nasjonal styringsevne og suverenitet, landets territoriale integritet, materiell og økonomisk trygghet, kulturelle verdier, gjennomføring av kritiske samfunnstjenester, menneskerettigheter og rettsstatens prinsipper.

Totalförsvarets forskningsinstitut (FOI) i Sverige beskriver samfunnets grunnleggende verdier som respekt for menneskers verdighet, frihet, demokrati, likhet, rettsstatsprinsippet og menneskerettigheter. De grunnleggende verdiene er felles vurderinger som holder samfunnet sammen. Verdiene holdes oppe av og realiseres gjennom det som bli omtalt som samfunnets vitale interesser.[19] De er i følge FOI:

- Bevare fred og nasjonal selvstendighet
- Opprettholde en demokratisk rettsstat
- Opprettholde en god samfunnsøkonomi og beskytte økonomiske verdier
- Beskytte liv og helse
- Beskytte miljøet

I følge FOI er en virksomhet eller et system samfunnsviktig hvis et avbrudd eller forstyrrelse medfører alvorlige konsekvenser for mulighetene til å opprettholde en eller flere av samfunnets vitale interesser.

De tre nevnte dokumentene identifiserer at noen verdier er viktigere enn andre for et samfunn. De

[17] NOU 2000:24. Et *sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*.
[18] St.prp. nr. 42 (2003–2004). *Den videre moderniseringen av Forsvaret i perioden 2005–2008*.
[19] Lewerentz, Birgitta. Frost, Christina. Marklund, Anna. Franzén, Göran. Wahlberg, Maria. Ånäs, Per

er såkalte grunnleggende verdier for et samfunn. Dette for å skille dem begrepsmessig fra andre verdier i samfunnet. Det kan være samfunnsverdier som ikke er like relevante i denne sammenheng, eksempelvis verdien toleranse. De sistnevnte er eksempler på at en diskusjon om samfunnets grunnleggende verdier vil bevege seg i gråsoner og vil være gjenstand for subjektive vurderinger. Det er derfor en utfordring å være presis og relevant. Et forsøk på å avgrense for vårt formål kan være å omtale samfunnets grunnleggende verdier ut fra forsvar av landet og samfunnssikkerhet, selv om også en slik avgrensing vil åpne for gråsoner og subjektive vurderinger, ikke minst sett på bakgrunn av at begrepet samfunnssikkerhet heller ikke er et omforent begrep.

3.1.6 Gjensidig avhengighet

En kompliserende faktor er den sterke integrasjonen og store gjensidige avhengigheten mellom forskjellige samfunnsfunksjoner/kritisk infrastruktur. Moderne samfunnsdrift støtter seg i stadig større grad på noen sentrale funksjoner som blir stadig mer avhengige av hverandre. Alvorlige forstyrrelser i én funksjon kan derfor gi omfattende ringvirkninger gjennom forstyrrelser i mange andre funksjoner.[20] Eksempelvis er både telekommunikasjon og elektronisk betalingsformidling kritisk avhengig av strømforsyning, og i tillegg avhengig av hverandre.[21] Den høye graden av gjensidig avhengighet i det moderne samfunn forteller oss at tilgjengelighet og integritet for et kritisk produkt eller tjeneste også er avhengig av produkter og tjenester utenfor egen sektor.[22]

3.2 Sammenligning mellom epler og pærer

I en rangeringsprosess mellom ulike samfunnsfunksjoner er det knyttet utfordringer til å sammenligne ulike størrelser på tvers av samfunnsfunksjonene. Man kan bli stående overfor problemstillinger lik det å sammenligne epler med pærer. For eksempel kan det være vanskelig å sammenligne og rangere mellom et gitt strømforsyningssystem og et gitt IKT-system, blant annet på grunn av gjensidig avhengighet mellom systemene. For det andre kan man bli stående overfor vurderinger hvor tap av menneskeliv settes opp mot andre verdier. Det er kontroversielt og etisk utfordrende. På den ene siden kan ett liv kvantifiseres ut fra kroner og øre. Det gjør det enklere å sammenligne med andre verdier som også kan prissettes, selv om det er utfordrende å beregne en "korrekt" sum.[23] På den annen side vil det kunne hevdes at de etiske sidene ikke tillater en slik fremgangsmåte. Svaret på verdsetting av liv er avhengig av situasjonen, men i svært mange tilfeller vil verdien av et liv vurderes som så høyt at tap ikke kan kvantifiseres eller aksepteres.

---

[20] Fridheim, Håvard. Hæsken Ole Morten. Olsen Thor Gunnar. Balke, T, Ensrud May-Kristin. 1997. *Viktige samfunnsfunksjoner*. FFI/RAPPORT-97/01458 (Begrenset)

[21] Fridheim, Håvard. Betten, Stian. Hagen, Janne M. Henriksen, Stein. Rodal, Gry Hege. Rodal, Siv Kjersti. Rutledal Frode. 2001. *Sårbarhetsreduserende tiltak i kraftforsyningen – Sluttrapport.* FFI/RAPPORT – 2001/02383 (Begrenset)

[22] Se for eksempel: Ministry of the Interior and Kingdom Relations 2003. *Critical Infrastructure Protection in the Netherlands.*

[23] Prissetting av liv blir brukt i ulike sammenhenger. For eksempel for å beregne erstatning etter tap av liv eller arbeidsevne, og for å illustrere at svært kostnadskrevende tiltak for å redde liv vil svare seg økonomisk i lengden. Hokstad, Per. Jersin, Erik. Rossnes, Ragnar. Steiro, Trygve. Tinmannsvik, Ranveig K. 2002. *Risiko på tvers (RPT). Gjennomgående og helhetlig strategi for risikovurdering på HMS-områd*et. SINTEF Rapport STF38 A01435.

Det vil ofte bare være i de mest ekstreme situasjoner at andre verdier settes høyere. Et eksempel på en slik verdi er verdien nasjonal selvstendighet; hvis landet angripes militært, vil svært mange akseptere tap av liv hvis det er avgjørende for den nasjonale selvstendigheten. Det vil også være dagligdagse situasjoner hvor tap av liv blir akseptert til fordel for en annen verdi; for eksempel "aksepterer" samfunnet flere hundre dødsfall i trafikken hvert år, fordi verdien av å ha egen bil blir vurdert som høyere.

Sammenligning mellom ulike størrelser har flere avskygninger enn det som er drøftet her. I forhold til denne studien er hensikten å understreke viktigheten av å ha et bevisst forhold til hvordan ulike størrelser kvantifiseres og sammenlignes. Eksemplene illustrerer også at det overfor enkelte problemstillinger er mer hensiktsmessig med en styrt diskusjon blant fageksperter og beslutningstagere, enn å forsøke å plassere de ulike størrelsene inn i en matrise. Det er fordi enkelte forhold vanskelig lar seg kvantifisere, andre igjen lar seg ikke sammenligne, mens noen forhold er bundet opp til politiske prioriteringer.

3.3 Risiko

For å identifisere og rangere kritiske infrastrukturer og funksjoner, må risikobegrepet adresseres. På den ene siden må det etableres en forståelse av hvor kritisk en infrastruktur eller en funksjon er for samfunnet. Det har med identifisering å gjøre. Enten er den ulike grader av kritisk, eller så er den det ikke. På den annen side må man også se på hva risikoen for en uønsket hendelse er. Lav eller høy risiko for en uønsket hendelse har betydning for hvilke beskyttelsestiltak som er nødvendige. Det har med andre ord betydning for hvordan vi rangerer. Eksempelvis er både strømforsyning og renovasjon kritiske samfunnsfunksjoner for et samfunn, og da særlig for byer og tettsteder. Konsekvensene av manglende strømleveranser og renovasjon vil være dramatiske. Likevel, risikoer knyttet til svikt eller bortfall er forskjellig fra de to, og intuitivt ser vi at strømforsyning må rangeres høyere basert på hvordan vi oppfatter risiko.

En vanlig tilnærming er å se på risiko som en kombinasjon av *sannsynlighet* og *konsekvens*.[24] Med lav sannsynlighet og lav konsekvens blir risikoen lav. Med middels sannsynlighet og høy konsekvens, er risikoen høyere. For eksempel kan sannsynligheten for et ras i et gitt område bli vurdert som middels. Hvis et eventuelt ras i området vil kunne ramme et boligfelt eller kritiske infrastrukturer er konsekvensen høy, og sammenlagt vil risikoen bli vurdert som høy. Risikoen for ras reduseres ved å redusere sannsynligheten for ras (eksempelvis ved rassikring), og/eller redusere konsekvensen av et ras (flytte de kritiske infrastrukturene eller boligfeltet bort fra de mest utsatte områdene).

En annen definisjon på risiko er: *risiko er en kombinasjon av mulig konsekvens (utfall) og tilhørende usikkerhet* (2). Denne definisjonen brukes både for sikkerhetsanvendelser og i en del økonomiske sammenhenger.[25] Usikkerhet kvantifiseres ved hjelp av sannsynligheter, og dermed

[24] Denne tilnærmingen sammenfaller med ISO standardens definisjon av risiko.
[25] Se for eksempel Aven, Terje. 2003. *Foundations of Risk Analysis. A Knowledge and Decision-Oriented Perspective*. John Wiley & Sons, Ltd 2003.

faller denne definisjonen sammen med definisjon 1 i dette tilfellet. Definisjon 2 er følgelig mer generell enn definisjon 1, i og med at den også har mening uten at usikkerhet kvantifiseres eller uttrykkes ved hjelp av sannsynligheter. For en del situasjoner vil en slik bredere definisjon kunne være formålstjenlig, eksempelvis risikovurderinger knyttet til mulige terrorangrep mot et system. Viktige funksjoner som dette systemet har kan defineres, og mulige konsekvenser av et angrep kan identifiseres. Det er imidlertid usikkerheter knyttet til om et angrep vil skje, og hva konsekvensene vil bli gitt et angrep. Disse usikkerhetene kan være meget store, og de vil kunne variere avhengig av hvem som gjør vurderingene. Usikkerhet knyttet til om et angrep vil skje påvirkes av en rekke forhold, som igjen er beheftet med usikkerhet, for eksempel valget i et land og utviklingen i krigsområder. Vi kan i en del tilfeller ønske å bruke sannsynligheter for å uttrykke usikkerhetene, men ofte vil vi nøye oss med å peke på usikkerhetene. Det er en risiko til stede uavhengig av om en har uttrykt usikkerhetene ved hjelp av sannsynligheter.

En annen tilnærming er å vurdere to ulike innfallsvinkler når risiko for terrorhandlinger skal vurderes. For det første ved et sårbarhetsperspektiv. Utgangspunktet for analysen er da å undersøke hvor lett eller vanskelig det er å forårsake skade, og hvor store konsekvenser det eventuelt vil kunne få. For det andre ved å ha et trusselperspektiv. Utgangspunktet for analysen er da å identifisere mulige aktører som kan ha interesse av å utføre skade, og eventuelt hvilken kapasitet de har til å gjennomføre en skadelig handling.[26]

Ulike tilnærminger til risiko har ulik fokus. Er det et ønske om å redusere sårbarhet eller et ønske om å redusere konsekvens eller sannsynlighet? I sammenheng med *security* er det ofte hensiktsmessig å skille mellom trussel og sårbarhet.[27]

3.4 Sårbarhet

Sårbarhetsutvalget definerer sårbarhet på følgende måte:

> Sårbarhet er et uttrykk for de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet. Sårbarhet er knyttet opp til mulig tap av verdi. System kan i denne sammenhengen for eksempel være en stat, den nasjonale kraftforsyningen, en bedrift eller et enkeltstående datasystem. I stor grad er sårbarhet selvforskyldt. Det går an å påvirke sårbarheten, begrense og redusere den.[28]

En annen vanlig definisjon på sårbarhet er: Et uttrykk for et systems evne til å fungere og oppnå sine mål når det utsettes for påkjenninger.

---

[26] Bjørgo, Tore. 2003. *Norske dammer – i hvilken grad er de sannsynlige terror- og sabotasjemål*. Revidert utgave april 2003. NUPI; NOU 2006:6. *Når sikkerheten er viktigst*.

[27] For en diskusjon omkring bruk av de engelske ordene *security* og *safety*, se Vinje, Finn-Erik 2005. *Sikkerhet – Safety/Security. En begrepsutredning* – i NOU 2006:6. *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastruktur og kritiske samfunnsfunksjoner*. Del 2, vedlegg 5.

[28] NOU 2000:24. *Et sårbart samfunn.*

Sårbarhet handler derfor om en egenskap ved en person, et objekt eller en virksomhet og dets forhold til omverdenen. Av definisjonen går det frem at det er mulig å påvirke sårbarheten, ved å begrense og redusere den. For beredskapsplanlegging er dermed sårbarhetsbegrepet svært aktuelt, ettersom man ved sårbarhetsanalyser vil kunne gå nærmere inn på kontrolltiltak og barrierer som bør være på plass for å begrense konsekvensene av uønskede hendelser.

3.5 Trussel

En trussel avhenger av angriperens intensjon og kapasitet til å gjennomføre handlingen. Siden intensjoner kan endre seg raskt, kan trusselsituasjonen, i motsetning til sårbarheter, være svært dynamisk over et kort tidsrom. Dette tvinger den som vil beskytte seg mot en potensiell trussel, å ha vesentlige deler av oppmerksomheten på kapasiter til å forvolde skade.[29] Dersom kapasitet og vilje er til stede, øker sannsynligheten for at en trussel skal bli realisert.

For eksempel er vestlige demokratiske samfunn sårbare for terrorhandlinger. Så lenge det ikke eksisterer noen trussel som kan utnytte sårbarheter, er det uproblematisk. Bruken av flykapringer for å oppnå politiske mål på 1970-tallet og hendelsene i USA 11. september 2001 avslørte at det forelå sårbarheter som terrorister utnyttet. For å redusere risikoen ble det innført sårbarhetsreduserende tiltak så som strengere kontroll av passasjerer, strengere kontroll av hvilke varer som kan medbringes osv. På denne måten bygget man ned sårbarheter for å imøtegå en konkret trussel, nemlig flykapring. Samtidig ble det arbeidet med å redusere selve trusselen. Sammen skulle det redusere risikoen.

3.6 Krise

Krisebegrepet har etter hvert nærmest blitt et moteord, og blir brukt om et vidt spekter av hendelser. Det er en stor grad av subjektivitet forbundet med krisebegrepet slik det omtales i dag, og det er mange ulike nivåer av kriser. I metoden vil det bli presentert en rekke scenarier som representerer ulike krisesituasjoner og trusler mot det norske samfunnet.[30] Sårbarhetsutvalget definerer krise på følgende måte:

> En krise er en hendelse som har potensial til å true viktige verdier og svekke en organisasjons evne til å utføre viktige funksjoner. En krise kan utvikle seg til å bli en katastrofe. Med katastrofe forstår vi en hendelse med særlig alvorlige skader og tap.[31]

Denne definisjonen gir en vid beskrivelse av krisebegrepet, og åpner for at det kan være virksomhetsavhengig hva som er en krise eller ikke.

I forhold til den tidligere diskusjonen rundt samfunnsverdier, er det mulig å skille mellom verdier

[29] Henriksen, Stein. 2004. Ikke utgitt manus *NSBR04*. Direktoratet for samfunnssikkerhet og beredskap; Mærli, Morten Bremer. 2004. *Crude Nukes on the Loose?* Unipub AS 2004.
[30] Henriksen, Stein. Sørli, Kjetil. Bogen, Lene. 2007. Metode for identifisering og rangering av kritiske samfunnsfunksjoner. FFI/RAPPORT-2007/00874.
[31] NOU 2000:24, Et sårbart samfunn - Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet

som er viktige i en normaltilstand og hva som er de viktigste verdiene i en krisesituasjon. Hvis man forholder seg til kriser og katastrofer på nasjonalt nivå vil det være innlysende at verdier som liv og helse er det første man tenker på. I en normalsituasjon vil funksjoner som rettsvern, selvrealisering, religionsfrihet etc. være viktige, men dersom det oppstår en krise blir slike verdier nedprioritert.

Thomas Ries ved det *Utrikespolitiska institutet* i Sverige, setter et mer konkret skille mellom kriser og katastrofer:

- Krise: individuell død og fordervelse, sørgelig, men livet går videre som før
- Katastrofe: samfunnsrystelse, farlig, varige endringer (ikke nødvendigvis til det bedre), status quo ante er ikke mulig, kvantesprang

Poenget med dette skillet er å illustrere at det finnes små kriser og store kriser (katastrofer). Forskjellen mellom disse ligger i hvilke konsekvenser de får for samfunnet. En krise er alvorlig der og da, men etter en stund fortsetter livet på samme måte som før. De store krisene (katastrofene) kjennetegnes ved at samfunnet som kommer ut i etterkant av katastrofen har endret seg.

3.7 Samfunnssikkerhet, Totalforsvaret og Homeland Security

Som en del av å tolke og definere kritiske samfunnsfunksjoner og kritisk infrastruktur, er en vinkling å se på begrepsapparatet knyttet til utviklingen av risikosamfunnet[32] slik det fremstår i Norge. De siste årene har samfunnssikkerhet etablert seg som et eget begrep i Norge, dels også i andre skandinaviske land, for å definere potensiell risiko mot samfunnet. Begrepet har imidlertid ikke satt seg ennå, noe som har sammenheng med at det finnes flere fortolkninger. Utviklingen av begrepet henger sammen med fremveksten av risikosamfunnet, slutten av den kalde krigen, oppblomstringen av regionale konflikter og sikkerhetsutviklingen etter 11. september 2001. Det finnes i dag minst tre hovedbegreper som bør ses i forhold til hverandre:

- Homeland Security
- Totalforsvar
- Samfunnssikkerhet

3.7.1 Homeland Security

Homeland Security eller ”hjemlandssikkerhet” er et amerikansk begrep og utgjør en ordbruk som ikke benyttes i en norsk sammenheng. Begrepet oppstod ved omorganiseringen av den nasjonale sikkerheten i USA etter 11. september 2001. Begrepet kan ses i sammenheng med at USA tradisjonelt har sikret nasjonale sikkerhetsinteresser gjennom tiltak utenfor amerikansk territorium, mens terrorhendelsen 11. september 2001 ble oppfattet som et angrep på hjemlandet, hvilket var en ny erfaring for USA. Derav en nyorientering mot å sikre eget territorium mot store

[32] Ble introdusert av den tyske sosiologen Ulrich Beck i boken Risikogesellschaft i 1986: Beck, Ulrich. 1986. *Risikogesellschaft: Auf dem Weg in eine andere Moderne*. Suhrkamp Verlag, Frankfurt am Main. Engelsk utgave: Beck, Ulrich. 1992. *Risk Society: Towards a New Modernity*. Sage Publ. 1992.

terrorhandlinger. Definisjon av Homeland Security er:

> *Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur*.[33]

Etter denne definisjonen er begrepet *Homeland Security* fokusert på terrortrusselen. *Department of Homeland Security* (DHS) har imidlertid underlagte etater som også arbeider med andre forhold enn terrorisme. *Federal Emergency Management Agency*[34] (FEMA) har for eksempel prioritet på risiko knyttet til naturkatastrofer, transport av farlig gods, forebygging, beredskapsplanlegging, krisehåndtering og normalisering etter kriser. Det har i ettertid av orkanen Katrina august 2005 kommet kritikk mot at terrorbekjempelse har tatt oppmerksomhet og ressurser vekk fra evnen til å forebygge og håndtere utilsiktede hendelser, eksempelvis orkaner.[35]

3.7.2 Totalforsvar

I Norge har sivile og militære tiltak som er relevante for nasjonal sikkerhet og forsvar blitt gruppert under begrepet totalforsvar. Dette begrepet synes å ha blitt oppfunnet av Forsvarskommisjonen av 1946, og har spredt seg til andre nordiske land. Det faktiske begrepsinnholdet er imidlertid basert på de erfaringer flere nasjoner, både krigførende og nøytrale, fikk i løpet av de to verdenskrigene.

Totalforsvar kan defineres som den totale mobiliseringen av alle mulige sivile og militære ressurser for å opprettholde forsvarsviljen, yte mest mulig motstand mot aggresjon, beskytte liv og helse, opprettholde et organisert samfunn og forebygge skade forårsaket av fredskriser og/eller krig.

De to viktigste formålene med totalforsvaret var å kanalisere så mange ressurser som mulig inn i militært forsvar, for det meste fra sivile kilder, og å sikre fysisk overlevelse for (så mange som mulig av) befolkningen, sivile eller militære. Trusselen om den totale krig rammet inn begrepet. I prinsippet gjaldt målsettingen gjennom hele den kalde krigen og fremstår som en restoppgave den dag i dag. Samfunnssikkerhetsbegrepet er i dag i økende grad foretrukket fremfor totalforsvarsbegrepet. Totalforsvaret består som en del av samfunnssikkerheten, men er av flere omfortolket og gitt det nye navnet sivilt-militært samarbeid. Med dagens sikkerhetspolitiske omgivelser ligger vekten mer på hva Forsvaret kan gjøre for det sivile samfunnet, enn på hva det sivile samfunnet kan gjøre for Forsvaret.[36]

---

[33] Office of Homeland Security. 2002. *National Strategy for Homeland Security*.
[34] Federal Emergency Management Agency Strategic Plan, Fiscal Years 2003 – 2008. *A Nation Prepared.*
[35] Se for eksempel: Dagbladet 8. september 2005. *Krise for krisesjefen*. http://www.dagbladet.no/nyheter/2005/09/08/442716.html
[36] Etter Forsvarsdepartementets syn gjelder totalforsvarsbegrepet fremdeles. For departementet beskriver begrepet gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunn i forbindelse med forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering i hele krisespekteret fra fred til sikkerhetspolitisk krise og krig. Sivilt-militært samarbeid omfatter etter Forsvarsdepartementets syn også øvrig samarbeid mellom sivile og militære myndigheter, som ikke er direkte knyttet til kriser og krig.

3.7.3 Samfunnssikkerhet

Samfunnssikkerhetsbegrepet er nytt, og det foregår fremdeles en prosess med hensyn til å feste begrepsinnholdet. En tilnærming til begrepet er å vise til Stortingsmelding 39 (2003 – 2004) om samfunnssikkerhet og sivilt-militært samarbeid og hva slags temaer som tas opp der:

- Omdefinering av sivilt-militært samarbeid innen totalforsvarskonseptet og en rekke andre områder
- Politi og Forsvar i kampen mot terrorismen – hvem gjør hva?
- Oppgradering av Politiets kapasiteter
- Omdefinering av militære roller, særlig Heimevernet
- Etterretningssamordning
- Samarbeid om internasjonal krisehåndtering
- Nukleært og radiologisk beredskap
- Beredskaps mot pandemisk sykdom og bio-terrorisme
- Beredskap mot kjemiske stoffer
- Informasjonssikkerhet
- Konsekvenser av klimaendring og mulige tiltak
- Skred
- Forsyningssikkerhet for elektrisk kraft
- Transportsikkerhet
- Kystberedskap
- Sikkerhet i petroleumsindustrien
- Matvaresikkerhet
- Sikkerhet i vannforsyningen
- Industriberedskap og -sikkerhet
- Forsyningsberedskap med hensyn til kritiske varer
- Samordning av samfunnssikkerheten
- Nasjonal krisehåndtering
- Store ulykker og farlige stoffer
- Brann-, produkt-, og elektrisk sikkerhet
- Utvikling av redningstjenesten[37]

Det kan ut fra dette hevdes å være en viss bredde i begrepet samfunnssikkerhet, og en tilsvarende avgrensingsutfordring. Det som med sikkerhet kan hevdes, er at begrepet ikke er festet til noe bestemt scenario av typen krig eller terror, men omfatter alle potensielle krisescenarier. Ettersom begrepet knapt kan avgrenses tematisk/fenomenologisk, må det søkes etter en ”terskel”, det vil si man må tilnærme seg et skille for eksempel mellom det som kan betraktes som et samfunnsproblem, som er relevant for begrepet, og det som kan betraktes som et individuelt problem, som er mindre relevant.[38]

[37] St.meld. nr. 39 (2003–2004). *Samfunnssikkerhet og sivilt-militært samarbeid*.
[38] For en lengre diskusjon om samfunnssikkerhet, se NOU 2006:6. *Når sikkerheten er viktigst.*

3.8 Hva betyr å identifisere?

Med å identifisere kritiske samfunnsfunksjoner mener vi å finne frem til en oversikt som vil kunne gi grunnlag for å prioritere i en krisesituasjon eller for å prioritere beredskapstiltak. En liste med identifiserte kritiske samfunnsfunksjoner kan inkludere alle kritiske samfunnsfunksjoner som samfunnet består av. Detaljeringsgraden i en slik liste vil være opp til brukerne å bestemme, og det kan innebære alt fra å liste hvilke virksomheter som er samfunnskritiske, til å liste opp personer som er viktige for å opprettholde infrastruktur.

Identifisering av kritiske samfunnsfunksjoner kan ta utgangspunkt i ulike tilnærminger. De kan eksempelvis være som følger:

1) **Identifisere med utgangspunkt i samfunnets grunnleggende verdier**
   Foreta en inndeling ut fra hvilken samfunnsverdi de er med på å opprettholde.

2) **Identifisere med utgangspunkt i samfunnets grunnleggende behov**
   Foreta en inndeling ut fra hvilke grunnleggende samfunnsbehov som må dekkes.

3) **Identifisere med utgangspunkt i scenarier (beredskap/krisetilnærming)**
   I mange sammenhenger vil avgjørelser være basert på knappe ressurser i en krise. En annen tilnærming er derfor å utarbeide en rekke scenarier og se hvilke sektorer og virksomheter som er mest viktige i disse.

4) **Sektorvis kartlegging: Identifisere ut fra en systembeskrivelse av en sektor eller innenfor en virksomhet**
   Tilsynsmyndigheter/sektorvise etater vil være et naturlig utgangspunkt for å identifisere de viktigste virksomhetene innenfor enkeltsektorer. Følgende spørsmål kan være aktuelle i en kartleggingsfase for å få oversikt over bevissthetsnivået i sektorene:
   - Er det laget en liste over alle virksomheter innen egen sektor?
   - Er noen av disse identifisert som mer viktige enn andre?
   - Hva er dette basert på (antall brukere/ berørte, viktighet for andre funksjoner/sektorer etc.)?
   - Hvilken strategi benyttes for å velge ut virksomheter for tilsyn?
     - Geografisk (virksomheter innen kommune x)
     - Størrelsesavhengig (de største virksomhetene)
     - Hendelsesstyrt (ad hoc når situasjoner oppstår)

5) **Geografisk/regional kartlegging**
   For å komme frem til en oversikt på nasjonalt nivå kan man benytte kommuner til å identifisere hvilke virksomheter som er viktige innenfor egen kommune. På kommunenivå vil det ofte være veldig synlig hva som er de viktige virksomhetene og noen mulige sjekkpunkter i forhold til dette kan være:
   - Er det utarbeidet en oversikt over alle virksomheter innen egen kommune?
   - Er noen av disse virksomhetene kritiske for kommunen?
   - Hvilke kriterier er lagt til grunn for dette (konsekvenser for liv og helse, hva som er økonomiske bærebjelker for kommunen osv.)?

3.9 Hva betyr å rangere?

Å rangere betyr å *ordne i en viss rekkefølge*, som i denne sammenheng betyr det å rangere kritiske samfunnsfunksjoner etter hvilke som er mest kritiske. Som nevnt finnes det mange formål med å rangere, men et av de viktigste vil være å skape et beslutningsgrunnlag for å prioritere.

Det finnes mange fremgangsmåter for å rangere, og to åpenbare alternativene vil være:

- Bruk av ekspertvurderinger (stor grad av subjektivitet)
- Bruk av rangeringskriterier (målbare og mindre subjektive)

Bruk av ekspertvurderinger til å rangere, innebærer at en bredt sammensatt gruppe med fageksperter gjør en vurdering basert på *common sense* over hva de anser som mest kritisk. Lang erfaring i de respektive fagområdene og god kjennskap til sektoren kan være tilstrekkelig til å peke ut hva som er de mest kritiske infrastrukturene, funksjonene eller virksomhetene. Ulempen med en slik fremgangsmåte er at metoden blir lite etterprøvbar, resultatene kan bli lite nøyaktige og gi dårlige muligheter for å kvalitetssikre hvilke kriterier som ligger til grunn. I tilegg vil bruk av forskjellige "eksperter" gi ulike resultater avhengig av deres subjektive oppfatninger.

Alternativet er derfor å utarbeide et felles sett med rangeringskriterier basert på mest mulig objektive kriterier. Fordelen med dette er at fastlagte kriterier vil kunne gjøre det mulig for "hvem som helst" å gjennomføre rangeringen. Utfordringen blir imidlertid å finne kriterier som vil kunne fungere på alle sektorer og innenfor alle scenarier. Det finnes mange kriterier man kan rangere på.

Den følgende listen viser eksempler på påvirkningsfaktorer i ulike scenarier som vil kunne tjene som rangeringskriterier:

- Sted/befolkningstetthet
- Årstid
- Varighet
- Situasjon
- Omfang (f.eks. geografisk)
- Gjensidige avhengigheter/koblede systemer
- Substitusjonsmuligheter: er funksjonen irreversibel? Eller kan man fortsatt gjøre det "på gamlemåten" om noe svikter? Dette er spesielt viktig i forhold til dagens avhengighet til IKT, ettersom det på mange områder ikke lenger finnes alternativer, som for eksempel manuelle betalingstjenester.[39]

For å kunne bruke disse kriteriene mest mulig effektivt, vil det være nødvendig å bryte kvalitative vurderinger ned i enklere og mer målbare score.

I praksis vil en metode bestå av begge tilnærmingsmåtene, både ekspertvurderinger og rangeringskriterier.

[39] Audestad, J. 2005. *E-bomber og e-granater – om IKT og sårbarhet*. FFI/NOTAT-2005/00938.

3.10 Metode

Hva er en metode? En kjent definisjon står omtalt i Ottar Helleviks lærebok Forskningsmetode for sosiologi og statsvitenskap:

> En metode er en framgangsmåte, et middel til å løse problemer og komme fram til ny kunnskap, Et hvilket som helst middel som tjener dette formålet, hører med i arsenalet av metoder.[40]

I BAS5-sammenheng er det utviklet en metode og en fremgangsmåte ut fra ønsket om å hjelpe brukere med å identifisere og rangere kritiske samfunnsfunksjoner på en oversiktelig, systematisk og dokumenterbar måte. Det har videre vært et ønske om å bruke en metode slik at utenforstående kan etterprøve resultatet, og eventuelt justere det. Det er også slik at innholdet i en rangert liste med kritiske samfunnsfunksjoner vil variere fra problemstilling til problemstilling. Ved å ta i bruk en metode, unngår brukeren å legge til grunn en rangert liste som ble laget med et annet formål; en metode gir fleksibilitet i forhold til problemstillingen. Det har også vært ønskelig å bruke en metode for å effektivisere rangeringsprosesser ved at man unngår å starte på nytt hver gang en rangert liste skal produseres.

4 Relevant teori

4.1 Charles Perrow – Normal Accidents

I 1999 utga den amerikanske sosiologen Charles Perrow ut boken *Normal Accidents*.[41] I boken presenteres et begrep som kan være fruktbart som kriterium for å identifisere og rangere kritisk infrastruktur og/eller identifisere og rangere kritiske samfunnsfunksjoner.

I Perrows teori om systemulykker vises det til begrepet *tett koblet system* (*tight coupling*). Begrepet beskriver en prosess som krever sentralisert styring for å fungere. Det viser til prosesser som skjer hurtig, og som ikke lar seg avbryte uten store konsekvenser. En avgrenset forstyrrelse vil umiddelbart berøre resten av systemet og skape negative konsekvenser for hele prosessen. Et tett koblet system er videre tidskritisk. Prosessen kan ikke avvente inngripen, men må håndteres der og da. Et tett koblet system er også avhengig av at de forskjellige delprosessene skjer i riktig rekkefølge. A må inntreffe før B for at det skal fungere. Et tett koblet system tillater i tillegg bare én måte å gjennomføre prosessen på. Det er heller ikke rom for slakk i prosessen. Ressurser som inngår i prosessen er nøye avmålt og kan ikke erstattes av andre ressurser, så fremt det ikke er lagt inn planlagt redundans.

Perrows teorier er langt mer omfattende enn det blir redegjort for her. Perrow benytter begrepet tette koblinger som en del av å beskrive risikoer knyttet til *systemulykker*. Han viser til

[40] Ottar Hellevik siterer samfunnsforskeren og sosiologen Vilhelm Aubert i Hellevik, Ottar. Forskningsmetode i sosiologi og statsvitenskap. 5. utgave, 2. opplag 1993. Universitetsforlaget.
[41] Perrow, Charles 1999. *Normal Accidents. Living with High-Risk Technologies*. Princeton University Press.

karakteristika ved et system for å si noe om risikoen for feil i systemet. I vår sammenheng kan Perrows teori om tett koblede systemer fungere som et verktøy for å identifisere kritiske infrastrukturer og funksjoner hvor toleransen for avbrudd er svært små. Vi har da et kriterium for å identifisere og rangere kritisk infrastruktur og kritiske samfunnsfunksjoner ut fra et sårbarhetsperspektiv. For eksempel er strømforsyning langt mer sårbar enn renovasjon. Begge har en kritisk funksjon i samfunnet, men mens strømforsyning er avhengig av noen få kontrollsentraler for å fungere, er det mulig å drifte renovasjon desentralisert med gode muligheter for å improvisere ved feil. Renovasjon er i Perrows terminologi et *løst koblet system*.

Ved å benytte Perrows teori kan det fastslås at leveranse av strøm må rangeres foran leveranse av renovasjonstjenester, fordi strømleveranse er et tett koblet system, mens renovasjon ikke er det. På samme måte kan vi se på jernbane og lufttrafikk i Norge. Begge er avhengige av styring fra driftsentraler i sanntid. Styringen er tidskritisk, prosessene må skje i en gitt rekkefølge og det er svært små muligheter til å gjøre ting annerledes enn planlagt. Det er heller ikke rom for noe særlig slakk i prosessen. Systemer og personell kan ikke erstattes uten at det på forhånd er lagt opp til det. Busstrafikk kan derimot ses på som et løst koblet system. Det kan fungere uten samme krav til sentralisert styring, eller i hvert fall med langt lavere krav til sentralisert kontroll og styring i sanntid. Potensialet for improvisasjon er stort, og svært mange av leddene i kjeden kan erstattes, omprioriteres eller omrutes, og det er heller ikke knyttet like stor grad av tidskritikalitet for funksjonsdyktigheten i systemet. Ut fra Perrows teori kan det fastslås at styringsfunksjonene til jernbane- og lufttrafikk må rangeres foran styringsfunksjonene til busstrafikk.

Et annet interessant trekk ved Perrows teori, er at virksomheter med tett koblede systemer er mer utsatt for systemulykker enn andre. En systemulykke oppstår når det samlede utfallet av svikt i flere ledd er uventet og ikke mulig å forutse. Dette gjelder særlig når kompleksiteten i prosessene i tillegg er høy. Perrow skiller her mellom *komplekse* og *lineære* tett koblede systemer. Både fly- og jernbanetransport er tett koblede systemer, men fordi jernbanetransport mer bærer preg av å være lineær, vil potensialet for feil være mindre. Det skyldes at antall mulige kombinasjoner som kan gi feil er mindre. Flytransport har et langt større antall mulige kombinasjoner som kan gi feil, og fremstår derfor som mer kompleks. En slik tilnærming vil i vår sammenheng kunne si noe om sannsynligheten for at en uønsket hendelse inntreffer. Jo mer kompleks, jo større sannsynlighet for en uønsket hendelse. Vi har da et kriterium for å differensiere mellom de ulike tett koblede systemene ut fra antall mulige kombinasjoner som kan gå feil.

Sammenlagt kan vi da både si noe om *sårbarhet* ut fra om det er ett tett koblet system eller ikke, og vi kan si noe om *potensialet for feil* ved at antall mulige kombinasjoner som kan gi feil er lavt eller høyt (lineært/komplekst). Sårbarhet er i denne sammenheng også relevant sett opp mot tilsiktede hendelser, ved at sårbare systemer lettere kan utnyttes av ondsinnede aktører. Et høyt potensial for feil kan på sin side gi indikasjoner på om det er sannsynlig at feil kan oppstå, uten å ha tilgang til statistikk over tidligere hendelser. Dette er særlig relevant fordi statistikk av ulike årsaker kan være utilgjengelig.

Vi kan da beskrive følgende:

- Løst koblet system = lav rangering
- Lineært tett koblet system = medium rangering
- Komplekst tett koblet system = høy rangering

Vær oppmerksom på at Perrows teori i utgangspunktet er tenkt brukt for å beskrive risikoer sett ut fra systemkarakteristika. Perrow skiller i tillegg mellom lineære og komplekse løst koblede systemer, slik at det i praksis er en firedeling, og ikke en tredeling som her. I vår sammenheng er det av mindre interesse å differensiere et løst koblet system. Et løst koblet system vil uansett få en lav rangering, enten det er lineært eller komplekst.[42] Vi forholder oss derfor til en tredeling som vist over.

4.2 Kriterier for å evaluere risiko - Klinke & Renn 2002

I 2002 utgav Klinke & Renn artikkelen *A New Approach to Risk Evaluation and Management: Risk-based, Precaution-based, and Discourse-based Strategies*.[43] Hensikten med artikkelen er å komme frem til en forbedret risikohåndteringsprosedyre. Artikkelen favner derfor bredere enn det som er av interesse i denne sammenheng, nemlig å redegjøre for metoder og kriterier som er fruktbare for å fremskaffe en metode for rangering og identifisering av kritiske samfunnsfunksjoner. Det følgende vil derfor ha fokus på det som kan ha relevans i sistnevnte sammenheng. Det betyr at de ikke blir redegjort for hele bredden i artikkelen

4.2.1 Ni kriterier for å evaluere risiko

I artikkelen blir det vist til ni kriterier for å evaluere risikoen for uønskede hendelser. I BAS5-sammenheng er det ikke kriterier for evaluering av risiko som er i fokus, men kriterier for å identifisere og rangere kritiske IKT-systemer og kritiske samfunnsfunksjoner. Klinke og Renns kriterier kan likevel ha en overføringsverdi i BAS5.

Artikkelforfatterne har følgende definisjon av risiko: Risiko er definert som muligheten for at menneskelige handlinger eller hendelser fører til konsekvenser som skader aspekter av ting som mennesker setter pris på.

Ni kriterier er lagt til grunn for å evaluere risiko, som vist i Tabell 4.1:

[42] Eksempler på løst koblede systemer som er komplekse og lineære er i følge Perrow universiteter og postkontor. Hvis noe går galt i disse systemene er det god tid til gjenoppretting fordi de begge er løst koblet og det er liten sannsynlighet for en systemulykke. Men i kontrast til universiteter så har ikke et postkontor mange uventede gjensidige samhandlingselementer. Det har en oversiktelig og lineær produksjonssekvens, derav begrepet et lineært løst koblet system. Et universitet er langt mer uoversiktlig med svært mange funksjoner som kan samhandle på uventede måter, derav begrepet et komplekst løst koblet system.
[43] Klinke & Renn.2002. *A New Approach to Risk Evaluation and Management: Risk-based, Precaution-based, and Discourse-based Strategies*.

Kriterium	Beskrivelse
Skadens omfang	Skadelig effekt på naturlige enheter (natural units) som dødsfall, personskade, produksjonstap etc.
Sannsynlighet for forekomst	Estimat for den relative frekvensen av en enkeltstående eller kontinuerlig tap av en funksjon
Uvisshet	Generell indikator for forskjellige usikkerhetskomponenter
Allestedsnærværelse (Ubiquity)	Definerer den geografiske utbredelsen og potensiell skade (intragenerational justice)
Utholdenhet	Definerer den tidsmessige utvidelsen av potensiell skade (intergenerational justice)
Reversibilitet	Beskriver muligheten for å gjenopprette/tilbakestille situasjonen til slik den var før skaden skjedde (mulig gjenoppretting kan være rensing av vann, gjenplantning av skog etc.)
Forsinkende effekt	Karakteriserer en lang latens mellom den initiale/utløsende hendelsen og den hendelsen som innbærer skade. Latenstiden kan være fysisk, kjemisk eller biologisk i sin natur.
Krenkelse av rettmessighet (Violation of equity)	Beskriver diskrepansen mellom de som nyter fordelene og de som bærer risiko.
Potensiale for mobilisering	Forstått som krenkelse av individuelle, sosiale og kulturelle interesser og verdier som genererer sosiale konflikter og psykiske reaksjoner hos individer eller grupper som føler at konsekvensene av risikoene går ut over dem. Dette kan også komme som et resultat av oppfattede urettferdigheter i fordelingen mellom risiko og fordeler.

Tabell 4.1 - Klinke & Renn. Ni kriterier for å evaluere risiko

4.2.2 Seks ulike klassifiseringer av risiko

Med utgangspunkt i gresk mytologi klassifiserer Klinke og Renn risiko ut fra seks ulike kategorier. Dette er en systematisk tilnærming mot ulike sammenhenger mellom sannsynlighet og skadepotensialet for å vurderes hva som er kritisk, og hvordan de skal rangeres seg i mellom.

Damokles sverd

Damokles sverd er et symbol på en truende fare i en heldig situasjon. Det skarpe sverdet henger i en tynn tråd over Damokles hode. Trusselen er knyttet til muligheten for en dødelig utgang, selv om sannsynligheten er lav. Myten kan bli overført til risikoer med *stort skadepotensiale med lav sannsynlighet*. Typiske eksempler er teknologi som innebærer stor risiko som bruk av kjernekraft, storskala kjemisk industri og damanlegg. Også naturhendelser som 100-årsflommer og meteornedslag faller inn i denne kategorien.

Kykloper

Kyklopene hadde kun ett øye, og bare én side av virkeligheten ble oppfattet. Det flerdimensjonale perspektivet manglet. Overført viser det til at bare én side av risikobildet kan bli fastslått, mens det andre er ukjent. *Katastrofepotensialet er stort og relativt kjent, mens sannsynligheten for en hendelse er ukjent*. En rekke naturhendelser faller inn i denne kategorien. For eksempel jordskjelv, vulkanutbrudd, ikke-periodiske flommer og værfenomener som El-Niño. Ofte mangler det kunnskap om kausale faktorer. Også former for menneskelig atferd faller inn i klassifiseringen

og gjør dette kriteriet usikkert. Fremkomsten av AIDS og andre infeksjonssykdommer samt tidligvarslingssystemer og NBC-våpen tilhører kategorien.

Pythia

Det mest kjente oraklet i det antikke Hellas var Oraklet i Delfi med den blinde seersken Pythia. I denne sammenhengen er det av interesse at Pythias spådommer alltid var flertydige. I overført betydning er poenget at *både sannsynligheten for en hendelse og skadepotensialet er ukjent*. Usikkerheten er derfor samlet sett stor. Sett opp mot naturhendelser innebærer dette risiko knyttet til plutselige ikke-lineære klimatiske endringer, for eksempel selvforsterkende global oppvarming eller ustabilitet i det vestantarktiske isflaket, altså hendelser med et større katastrofalt potensial enn en gradvis klimaendring vil ha. I forhold til risiko knyttet til bruk av teknologi, kan flertydigheten illustreres ved å vise til genetisk modifisert matproduksjon hvor verken den maksimale grad av skade eller sannsynligheten for skadelige hendelser kan beregnes per i dag. Pythia-klassifiseringen inkluderer også kjemiske og biologiske substanser hvor det er mistanke om at visse effekter kan oppstå, men hvor verken omfanget eller sannsynligheten kan bli fastslått med nøyaktighet. Risikoen for BSE (kugalskap) er et eksempel på dette.

Pandoras eske

I det antikke Hellas kunne farer bli forklart ut fra myten om Pandoras eske. Pandora brakte med seg håp, men også en eske som ikke skulle åpnes. Hvis esken derimot ble åpnet kom all verdens ondskap og plager frem som ikke lot seg stoppe med irreversible konsekvenser. Menneskelige inngripen i miljøet har ved flere anledninger irreversible, vidtgående og vedvarende endringer uten noen klar kobling til spesifikke skader. Ofte oppdages skadene lenge etter at hendelsene har skjedd. For eksempel er bruken av KFK-gasser hovedårsaken til hull i ozonlaget. Spesiell oppmerksomhet må vies til risikoer som kan karakteriseres med høy grad av spredning, motstandsdyktighet og ikke vendbare prosesser. Ved Pandoras eske er både *sannsynligheten for en hendelse og graden av skadeomfanget usikkert*, og bare fornuftige hypoteser om sammenheng er tilgjengelig. Som ved Pythia er usikkerheten stor, men det kausale forholdet mellom faktor (agent) og konsekvens er ikke vitenskapelig bevist på en plausibel måte.

Cassandra

Cassandra var en seerske fra Troja som korrekt forutså farene ved en gresk seier, men som ikke ble tatt på alvor. Det er ved dette paradokset som denne risikoklassifiseringen dveler: *Sannsynligheten for en hendelse og for skadeomfanget er høyt og relativt kjent, men avstanden i tid mellom den utløsende faktor og selve skaden er stor*. Dette leder til en situasjon hvor risikoen blir ignorert eller bagatellisert. Menneskeskapte klimaendringer og tap av biologisk mangfold illustrerer dette. Legg merke til at risikoklassifiseringen Cassandra kun er av interesse hvis potensialet for skade og sannsynligheten for at det skal skje er relativt høy.

Medusa

Medusa var en av de tre fryktede Gorgonsøstrene i klassisk gresk mytologi. Medusa og hennes søstre ble fryktet fordi et blikk på dem forvandlet tilskueren om til stein. I denne sammenhengen

er det *frykten for det som mangler forankring i virkeligheten* som er tema. Nyskapninger blir avvist på tross av de ikke i noen særlig grad er vurdert vitenskapelig som noen trussel, men fordi de har trekk ved seg som gjør de fryktet eller ikke er velkommen. Slike fenomener har et stort potensial for engstelse og sosial mobilisering blant publikum. Risikoklassifiseringen er kun av interesse når det er et særlig gap mellom risikooppfatningen hos legmann og ekspert. Et typisk eksempel er stråling fra elektromagnetiske felt som av eksperter blir vurdert å medføre lav skade, men som publikum oppfatter som utrygg sett opp mot egen helse.

Kommentarer

De seks risikokategoriene er klassifisert som følger i Tabell 4.2:

Navn	Beskrivelse
Damokles sverd	Risikoer med stort skadepotensiale med lav sannsynlighet.
Kykloper	Katastrofepotensialet er stort og relativt kjent, mens sannsynligheten for en hendelse er ukjent.
Pythia	Både sannsynligheten for en hendelse og skadepotensialet er ukjent.
Pandoras eske	Både sannsynligheten for en hendelse og graden av skadeomfanget usikkert, og bare hypoteser om sammenheng er tilgjengelige. Som ved Pythia er usikkerheten stor, men det kausale forholdet mellom faktor (eng.: agent) og konsekvens er ikke vitenskapelig bevist.
Cassandra	Sannsynligheten for en hendelse og for skadeomfanget er høyt og relativt kjent, men avstanden i tid mellom den utløsende faktor og skaden er stor.
Medusa	Et stort gap mellom risikooppfatningen hos legmann og ekspert.

Tabell 4.2 - Klinke & Renn. Seks risikoklassifiseringer

De seks risikoklassifiseringene gir ingen klare kriterier for hva som er kritisk og hvordan man kan rangere dem i mellom. Utgangspunktet for klassifiseringen er å benytte dem til å vurdere risiko for en hendelse. I Klinke og Renns artikkel er klassifiseringen en del av en helhetlig metode, og den skal fungere som en nødvendig kobling mellom risikovurdering og risikoevaluering. Ved å ta de ut av en helhet lik det er gjort her, står en i fare for å bruke klassifiseringen feil. Likevel kan det være fruktbart å ha en systematisk tilnærming mot ulike sammenhenger mellom sannsynlighet og skadepotensialet når det skal vurderes hva som er kritisk, og hvordan de skal rangeres seg i mellom. For eksempel kan en hypotese være at virksomheter som opererer med risiko for stort skadepotensiale, og med lav sannsynlighet for at noe skal skje (Damokles sverd) burde rangeres høyere enn virksomheter med lavt skadepotensiale.

De ni kriteriene for å evaluere risiko er også tatt ut av sin sammenheng, men enkelte kan likevel ha en overføringsverdi. Et eksempel er kriteriet reversibilitet, som beskriver muligheten for å gjenopprette/tilbakestille situasjonen til slik den var før skaden skjedde. Er det fruktbart å legge inn kriteriet reversibilitet eller gjenopprettingsevne? Hvis en funksjon, virksomhet eller tilsvarende har stor gjenopprettingsevne, er det slik at den dermed har liten sårbarhet overfor avbrudd, og derfor kan vektes lavt? Selv om dette er et riktig resonnement, er det ikke sikkert at det er praktisk gjennomførbart å måle reversibilitet på tvers av sektorer, funksjoner, virksomheter og så videre.

5 Lister over kritiske sektorer, samfunnsfunksjoner og infrastruktur

Det eksisterer et større[44] antall lister over kritiske infrastrukturer, kritiske samfunnsfunksjoner og sektorer nasjonalt og internasjonalt. En gjennomgående utfordring er at det ikke er synliggjort hvordan listene er produsert. Vi kan dermed ikke vurdere metoden som ligger bak, ei heller kontrollere resultatet. Ett unntak er Infrastrukturutvalgets oversikt over kritiske infrastrukturer og kritiske samfunnsfunksjoner. Utvalget har utarbeidet et sett med skjønnsmessige retningslinjer som angir hvordan listen er produsert.

Hensikten med det følgende er ikke å forsøke å komme med en uttømmende oversikt over forskjellige lister for deretter å sammenligne dem. En slik øvelse vil i beste fall ende opp med en enda lengre liste som ikke nødvendigvis er relevant i norsk sammenheng. Hensikten er å vise at det er identifisert to forskjellige typer lister som begge er relevante måter å utrykke seg på. Den ene viser til hvem/hva som er kritiske i en krisesituasjon, og som dermed har karakter av å være en skadereduserende kritisk samfunnsfunksjon. Den andre viser til hva som blir ansett som sektorer med kritisk infrastruktur, og som dermed har karakter av å være en umiddelbar kritisk samfunnsfunksjon.

5.1.1 International Emergency Preference Scheme - IEPS

I 2000 presenterte den internasjonale teleunionen (ITU) en anbefaling om prioritet i telenettet internasjonalt. Bakgrunnen var at NATO så behov for en prioriteringsmekanisme på tvers av medlemslandene. Fra før av hadde en rekke av medlemslandene innført nasjonale prioriteringsmekanismer. I Norge var dette kjent som VPT-ordningen i fastnettet.[45] Den norske ordningen ble nedlagt ved årskiftet 2000/2001.[46] I 2006 ble det fremsatt et forslag fra Post- og teletilsynet til Samferdselsdepartementet om å etablere en prioriteringsordning i mobilnettet. Dette forslaget ligger per februar 2007 til vurdering i Samferdselsdepartementet.

ITU ga innspill til NATOs sivile kommunikasjonskomité (CCPC) som på grunnlag av dette presenterte en liste over hvilke grupper som kan være prioriterte.[47] Listen skal kunne benyttes både overfor fast- og mobilnett og går under navnet IEPS - *International Emergency Preference Scheme*:

- Militære formål
- Sivilforsvar/hjemmeforsvar, offentlige varslingssystemer
- Diplomati og andre vitale myndighetsområder
- Statlig sikkerhet inkludert toll og immigrasjon
- Nødhjelpstjenester på lokalt nivå inkludert politi, brann osv.
- Post- og teleleverandører, for å sikre drift til andre viktige brukere

[44] International Telefommunication Union (ITU). E.106 (03/2000). *Description of an international emergency preference scheme IEPS*; ITU er FNs spesialistorgan for telekommunikasjon.
[45] VPT står for Viktig Prioritert Telefon.
[46] St.meld. Nr. 47 (2000-2001). *Telesikkerhet og –beredskap i et telemarked med fri konkurranse*.
[47] Document EAPC(CCPC)D(2003)0007-REV1. 26 april 2004. *Policy on the implementation of the international emergency preference scheme in the EAPC area*.

- Public utilities, inkludert energi, vannforsyning osv.
- Medisinske tjenester
- Luft- og sjøredning
- Industri som er vital i krisesituasjoner
- Nasjonal og internasjonal transport, så som lufthavner og relaterte tjenester, veitjenester, havner, maritime tjenester, togstasjoner og innenlands sjøveg
- Meteorologiske tjenester
- Kringkastnings- og pressetjenester

IEPS-listen danner et utgangspunktet for de som har behov for prioritering ved krisesituasjoner. Den peker ut grupper som skal ha tilgang til internasjonale teletjenester når tjenestene er begrenset av forhold som skade, overbelastning og/eller andre feil. I utgangspunktet får nasjonale prioriterte brukere ikke tilgang til de internasjonale tjenestene. I vår sammenheng er oversikten interessant fordi den viser hva den internasjonale teleunionen (ITU) og NATOs sivile kommunikasjonskomité (CCPC) mener er de mest kritiske samfunnsfunksjonene sett opp mot deres behov for internasjonal telekommunikasjon, men mest av alt illustrerer den én tilnærming til å produsere en oversikt, nemlig hvem som er de mest kritiske brukerne ved kriser.

5.1.2 Canada – nasjonalt kritiske infrastruktursektorer

Canada har identifisert ti kritiske sektorer på grunnlag av landets nasjonale program for sikkerhet i kritisk infrastruktur (NCIAP – National Critical Infrastructure Assurance Program). NCIAP blir utviklet under ledelse av det canadiske sikkerhetsdepartementet (Public Safety and Emergency Preparedness Canada - PSEPC).[48] De kritiske sektorene er listet i Tabell 5.1.

[48] National Critical Infrastructure Assurance Program. *An Assessment of Canada's National Critical Infrastructure Sectors*. July 2003. www.ocipep.gc.ca/critical/nciap/nci_sector2_e.aps

Sektor	(Sample target) Subsektor
1. Energi og hjelpesystemer	Elektrisk kraftproduksjon (generatorer, overføring, kjernekraft) Naturgass Oljeproduksjon og overføringssystemer
2. Kommunikasjons og informasjonsteknologi	Telekommunikasjon (telefon, faks, kabel, satellitt) Kringkastingssystemer Software Hardware Nettverk (internett)
3. Finans	Bank Sikkerhet (securities) Investeringer (investments)
4. Helse	Sykehus Helsevesen og fasiliteter Blodbank og fasiliteter Laboratorier Farmasi
5. Mat	Matsikkerhet Jordbruk og matvareindustri Matvaredistribusjon
6. Vann	Drikkevann Avløpsvannhåndtering
7. Transport	Luft Jernbane Sjø Vei
8. Sikkerhet (safety)	Kjemisk, biologisk, radiologisk og kjernefysisk sikkerhet Risikomaterialer Søk og redning Nødtjenester (politi, brann, ambulanse og andre) Dammer
9. Myndighet	Myndighetsfasiliteter Myndighetstjenester (eks. meteorologiske tjenester) Myndighets informasjonsnettverk Myndighetsressurser Nasjonale nøkkelsymboler (kulturelle institusjoner og nasjonale steder og monumenter)
10. Produksjon/industri	Kjemisk industri Forsvarsindustri (Defence industrial base)

Tabell 5.1 - Canada – nasjonalt kritiske infrastruktursektorer

Canadas liste er interessant i seg selv fordi den viser hvilke sektorer Canada mener er kritiske for samfunnet, men den er også interessant fordi den viser en måte å kategorisere og

underkategorisere på. En lignende tilnærming kan tenkes å være et godt utgangspunkt i en norsk sammenheng. Den er også interessant fordi den viser til en annen tilnærming enn ITUs oversikt, nemlig å liste opp det som er mest kritisk for å drifte et samfunn, i motsetning til å vise hvilke hva/hvem som er mest kritiske for å håndtere en krise.

I samme studie presenteres en sammenlikning av lister fra ni forskjellige land.[49] Sammenlikningen er fra 2003, og blir ikke gjengitt i helhet her. Av interesse er at det fremkommer at alle ni land er identiske på fem punkter. De er:

- Energi og/eller hjelpesystemer
- (Tele)kommunikasjon
- Helse
- Bank og finans
- Transport

Med unntak av Sverige har de andre landene også definert de følgende to som kritisk infrastruktursektorer:

- Myndighet/Regjering og/eller Forsvar
- Nød- og redningstjeneste og/eller *safety* og *security*

Oversiktene fra ITU og Canada illustrerer at vi må være bevisst på hva en metode skal produsere. Selv om de til dels er overlappende, er det en grunnleggende forskjell. ITUs oversikt er ment brukt til å identifisere brukere som har en rolle ved krisehåndtering. Canadas oversikt viser til de sektorene/samfunnsfunksjonene/infrastruktur som er mest kritiske for samfunnet. Forskjellen kan gi seg utslag i forskjellige tiltak, selv om det i praksis vil bli noe overlapping også her.

5.1.3 Norge – Infrastrukturutvalgets liste over kritisk infrastruktur og kritiske samfunnsfunksjoner[50]

Infrastrukturutvalgets oversikt skiller seg fra andre oversikter ved at den er eksplisitt på skillet mellom infrastrukturer og samfunnsfunksjoner. Skillet er brukt for å tydeliggjøre at enkelte kritiske samfunnsfunksjoner i mindre grad har en egen infrastruktur som kan omtales som kritisk, og som i hovedsak er avhengig av eksterne kritiske infrastrukturer for å fungere. Dette er hensiktsmessig blant annet ved valg av virkemidler for å sikre funksjonsdyktighet. Skillet er også hensiktsmessig for å bevisstgjøre avhengighet av anlegg og systemer utenfor egen kontroll.

[49] Listene som er sammenliknet kommer fra følgende land: Canada, Storbritannia, Australia, USA, Tyskland, Sverige, Norge, Nederland og Sveits. For alle detaljer, se: National Critical Infrastructure Assurance Program. *An Assessment of Canada's National Critical Infrastructure Sectors*. July 2003. www.ocipep.gc.ca/critical/nciap/nci_sector2_e.aps

[50] NOU 2006:6. *Når sikkerheten er viktigst*

Kritiske infrastrukturer	*Kritiske samfunnsfunksjoner*
Elektrisk kraft	***Bank og finans***
Elektronisk kommunikasjon	***Matforsyning***
Vann og avløp	***Helse-, sosial- og trygdetjenester***
Transport	***Politi***
Olje og gass	***Nød- og redningstjeneste***
Satellittbasert infrastruktur	***Kriseledelse***
	Storting og Regjering
	Domstolene
	Forsvar
	Miljøovervåkning
	Renovasjon

Tabell 5.2 Infrastrukturutvalgets oversikt over kritiske infrastrukturer og kritiske samfunnsfunksjoner

Utvalget viser til at kritisk infrastruktur er de anlegg og systemer som *understøtter* elektrisk kraft, elektronisk kommunikasjon, transport, olje og gass, vann og avløp og satellittbasert infrastruktur. I dette ligger det at funksjonsdyktigheten til de kritiske samfunnsfunksjonene i stor grad er avhengig av den eksterne kritiske infrastrukturen som er listet til venstre i Tabell 5.2. Eksempelvis er politiets egen infrastruktur lite kritisk i forhold til funksjonsdyktigheten. Funksjonsdyktigheten til politiet sett under ett opprettholdes i første rekke ved at de får adekvat ekstern leveranse av elektrisk kraft, elektronisk kommunikasjon og transport.

DEL II – Relevante metoder

6 Oversikt over eksisterende metoder

Ved å se på utenlandske erfaringer når det gjelder rangering av kritiske infrastrukturer og samfunnsfunksjoner kan vi sammenlikne fremgangsmåter, selv om ikke alle landene er sammenliknbare med Norge med tanke på teknologisk utvikling og størrelse. Dette regnes likevel som nyttige innspill, fordi det gir informasjon om metoder som er benyttet eller er under utvikling. Metodene som presenteres er i hovedsak valgt ut fra at de foreligger på et tilgjengelig språk, og at informasjon er gjort tilgjengelig.

Rangering av kritiske infrastrukturer og samfunnsfunksjoner har åpenbare fellestrekk med arbeider som ligger til grunn for nasjonale risiko- og sårbarhetsanalyser. Derfor presenteres også metodikker for dette.

Infrastrukturutvalget har utarbeidet et sett med skjønnsmessige retningslinjer for å identifisere kritisk infrastruktur og kritiske samfunnsfunksjoner. Det blir redegjort for disse til slutt i kapittelet.

6.1 USA

6.1.1 NIPP

Amerikanske metoder for identifisering og rangering av kritiske samfunnsfunksjoner og kritisk infrastruktur er relativt lite tilgjengelig på Internett. Arbeid på området pågår i *Department of Homeland Security* (DHS), *Directorate for Informations Analysis and Infrastructure Protection*.[51]

Som en direkte følge av den amerikanske presidentens direktiv av 2003 (HSDP-7)[52], utarbeidet DHS i februar 2005 en midlertidig plan for videre arbeid, nemlig *Interim National Infrastructure Protection Plan* (Interim NIPP). Interim NIPP ble etterfulgt av *National Infrastructure Protection Plan* (NIPP) som er et mer detaljert dokument. Første utkast ble publisert 2. november 2005, og utkast til revisjon nummer 2.0 i januar 2006.

NIPP gir rammeverket for identifisering av kritiske infrastrukturer og nøkkelressurser, evaluering av trussel og sårbarhet samt for finansiell prioritering basert på en kost/ nytteevaluering. Overordnet mål med NIPP er:

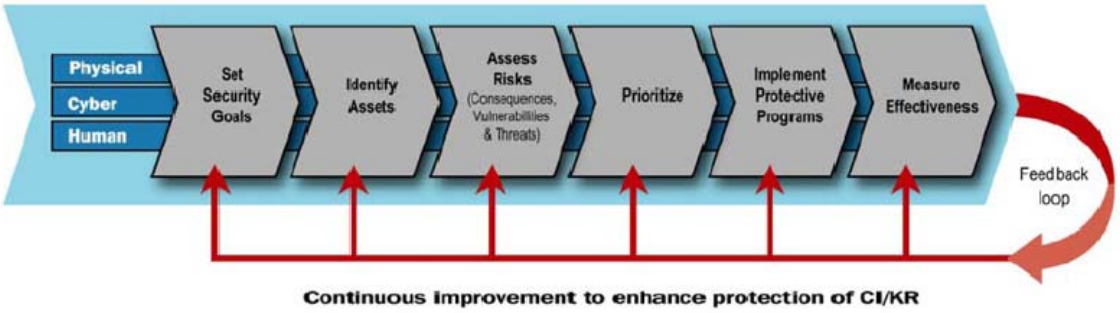
[51] For relevant litteratur, se DHS' hjemmeside på følgende adresse: http://www.dhs.gov/
[52] Homeland Security Presidential Directive (HSPD)-7 2003. *Critical Infrastructure Identification, Prioritization, and Protection*.

Enhance protection of the Nation's CI/KR in order to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and enable national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.[53]

Et eller flere av følgende elementer inngår i følge DHS i enhver kritisk infrastruktur og nøkkelressurs: Personer, fysiske elementer samt cyberelementer.[54] Den menneskelige faktoren omfatter også kunnskap, menneskelige evner og ekspertise. Betegnelsen fysiske elementer brukes om for eksempel bygninger, dyr og produkter, mens cyberelementer er soft- og hardware, informasjon og nettverk som støtter funksjonene i en kritisk ressurs. Kriteriene for å vurdere hva som er kritisk infrastruktur og nøkkelressurser er:

- Antall skadede og døde
- Materiell skade og økonomisk innvirkning
- Påvirkning på nasjonal sikkerhet

NIPP er rettet mot de 17 sektorer av kritiske infrastrukturer og ressurser identifisert i HSDP-7. NIPP identifiserer fem spesifikke aktiviteter som en del av rammeverket:



Figur 6.1. The Protection Program Strategy: Reducing Risk. NIPP Rammeverk Draft NIPP v. 2.0 (2006).

For å oppnå en sikker infrastruktur må man basere seg på felles nasjonale og sektorspesifikke sikkerhetsmål. Sikkerhetsmålene varierer fra sektor til sektor, og nasjonal målsetting kan være annerledes enn sektorspesifikke mål. På nasjonalt nivå er man kommet langt i å bestemme mål for risikoreduksjon. Det er utarbeidet en nasjonal risikoprofil som oppdateres kontinuerlig, der DHS i samarbeid med sektorspesifikke byråer (SSA) bestemmer risikoreduserende tiltak, og man utarbeider beskyttelsesprogram for kritiske sektorer basert på risiko. Sikkerhetsmål på sektornivå definerer hva slags rolle/element (fysisk, menneskelig eller cyberelement) som man ønsker å beskytte. Sektormål omhandler spesifikke elementer, systemer og prosesser, og tar for seg ulike

[53] Draft NIPP v.2.0 2006. Kapittel. 1.6. *Goal and objectives of the NIPP*. Tilgjengelig fra *The Infrastructure Security Partnership (TISP)* http://www.tisp.org/news/newsdetails.cfm?&newsID=704
[54] Draft NIPP v.2.0 2006. Kapittel. 1.8. *Special Considerations*.

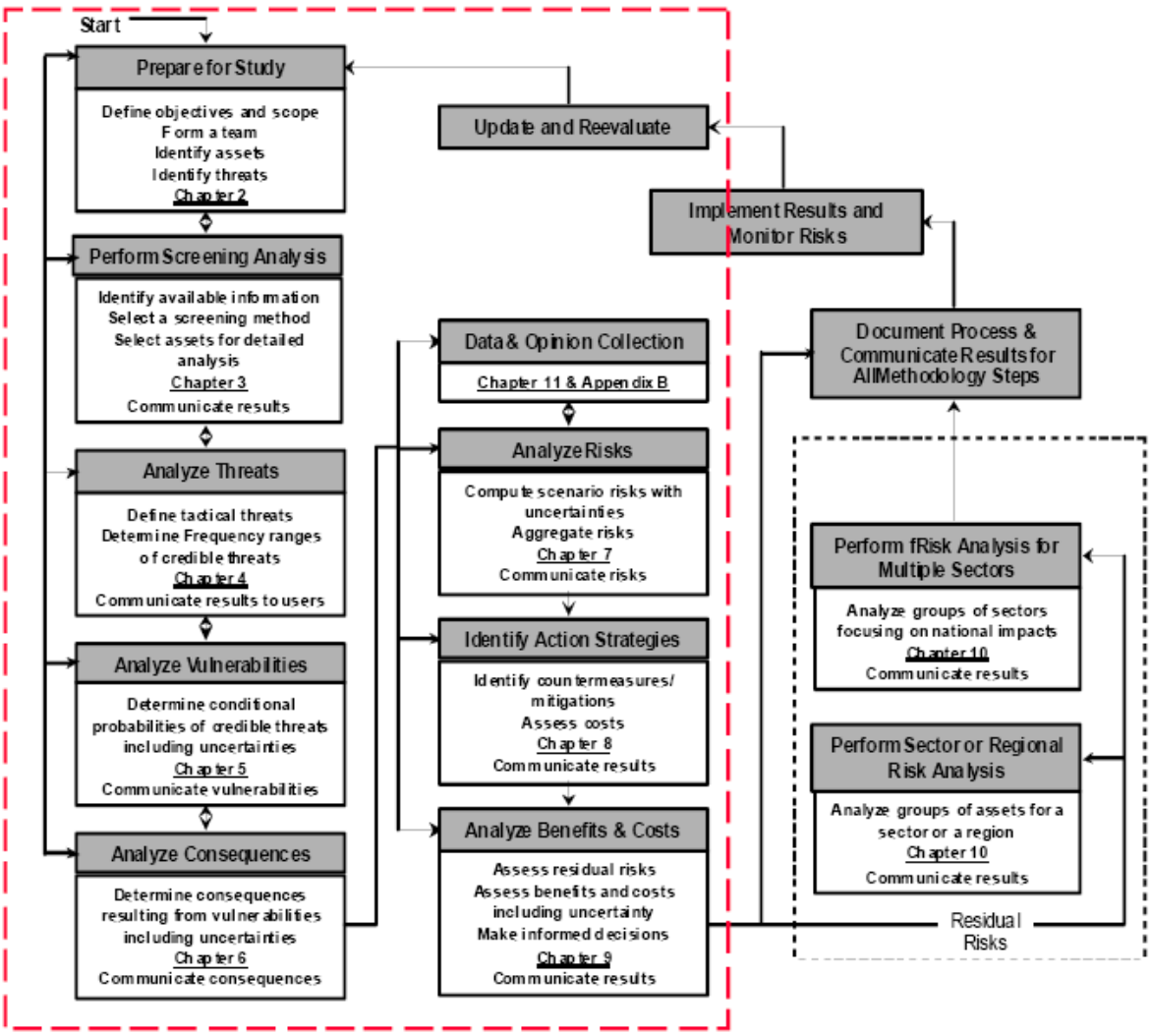
tilnærminger til risikohåndtering.[55]

Det neste steget er å utvikle en nasjonal database (*National Asset Database*, NADB) for nasjonal kritisk infrastruktur og nøkkelressurser. Denne inneholder data fra sektorspesifikke kataloger, datainnsamling fra partnere, frivillig overlevering fra eiere og operatører samt resultat av analyser. Tilgang til data fra NADB er kun gitt utvalgt DHS-personell av sikkerhetsmessige årsaker. Andre kan bli gitt tilgang etter forespørsel, men da kun på en *need to know* basis.

For å evaluere risiko utarbeider DHS en metodologisk verktøykasse kalt *Risk Analysis and Management for Critical Asset Protection* (RAMCAP). Risikoanalysene foregår både sektorvis og på nasjonalt, tverrsektorielt nivå. Risikoanalyser, der sårbarhet og trusselvurdering sammenstilles, gir sammen med kostnadseffektive hensyn muligheten til å se hvilke sektorer som må prioriteres med tanke på blant annet allokering av midler til forebygging og beskyttelse. Måling av effektivitet og ytelse gir grunnlaget for tilbakemeldinger.

American Society of Mechanical Engineers (ASME) ble i september 2003 tildelt et stipend fra DHS for å bidra i arbeidet for å oppnå en enhetlig risikobasert metode. ASMEs generelle RAMCAP metodeoversikt er gjengitt under i Figur 6.2.

[55] Draft NIPP inneholder bl.a. en liste over målene for cybersikkerhet (Draft NIPP v.2.0 2006. Anneks 1A.3).



Figur 6.2. Samlet RAMCAP metodesett (American Society of Mechanical Engineers, ASME)[56]

RAMCAP videreutvikles i DHS, blant annet med det som mål å gi eiere og operatører standardiserte data for å ivareta kompatibiliteten når risikoanalyser skal sammenliknes innen og mellom sektorene. Elementene som inngår i dette metodesettet kan oppsummeres i fire faser som kan benyttes på tre nivåer; (1) innenfor en virksomhet [fase en og to], (2) innenfor en sektor [fase tre], og til slutt (3) avdekke avhengigheter for hele nasjonen [fase fire].

- Første fase innebærer
    1. Identifisere kritiske elementer eller grupper av elementer.
    2. Identifisere trusler mot disse elementene og estimere angrepshyppighet.
    3. Kommunikasjon med de ansvarlige for risikoanalyse for kritiske elementer er også en del av fase én.
- Andre fase:
    4. *Screening* for å skille ut infrastruktur og ressurser som behøver ytterligere

[56] http://www.bfrl.nist.gov/PSSIWG/presentations/NSTCPresentation_0917041.pdf

fokus, samt utvelgelse av hvilken kombinasjon *kritisk element vs. trussel* som skal evalueres.

5. Risikoanalyse (evaluering av trussel, sårbarhet og konsekvens) gjennomføres for den valgte kombinasjonen, og det tas hensyn til kort- og langtidskonsekvenser av realistiske angrepsscenarier. Skade på omgivelsene vurderes også i denne fasen.
6. Det foretaes en gjennomgang av screeningen og risikoanalysen for å vurdere hensiktsmessigheten av metodevalget og for å evaluere og sjekke resultatet.

- I en tredje fase:
    7. Analysere sektorrisiko ut fra individuelle aktørers rapportering om bortfall av kapasiteter. Denne fasen består av flere trinn:
        a. Definisjon av analyseobjekt og grenser.
        b. Samle relevante resultat av individuelle aktørers risikoanalyser.
        c. Benytte computersimulering for å få frem økonomiske og sosiale kort- og langtidskonsekvenser av de samlede kapasiteter som faller bort, basert på gjensidige avhengigheter.
        d. Benytte eksperter til å se på de bredere konsekvenser; endrede vaner i befolkningen vedrørende for eksempel reising eller konsum.
        e. Illustrere den individuelle risikoanalysen ved hjelp av computermodeller (*event trees*) som inkluderer regionalt og nasjonalt nivå i risikoanalysen, og som inkluderer gjensidige avhengigheter.
        f. Risiko for individuelle angrep bestemmes, sammen med den samlede risiko for gjentatte angrep.
        g. Mottiltak og konsekvensreduserende initiativ utvikles.
        h. Evaluering av de foreslåtte mottiltak og konsekvensreduserende initiativ ved hjelp av kost/nytte- og andre analyser.
- I fjerde og siste fase:
    8. Samme form for risikoanalyse gjennomføres for multiple sektorer:
        a. Definisjon av analyseobjekt og grenser.
        b. Samle relevante resultat av sektorvise risikoanalyser.
        c. Evaluere gjensidig avhengighet mellom sektorene.
        d. Mottiltak og konsekvensreduserende initiativ utvikles.
        e. Formålstjenlig bestemmelse taes.
        f. Dokumentering, implementering, overvåkning, oppdatering og kommunikasjon med alle aktører gjennom alle fasene.

Metoden er scenariobasert fremfor verdibasert (*asset-based*), og fungerer som utgangspunkt for en standardmetode. Det er ikke konsensus om denne metoden, og enkeltsektorer benytter ulike verktøy for å evaluere risiko. Det legges likevel opp til at man skal følge grunnlinjen/ minstestandarden (*baseline*) som er lagt frem i NIPP anneks 3A, for å sikre at resultatene kan sammenliknes, og man går ut fra at RAMCAP på sikt vil utgjøre et eksempel også for andre evalueringsmetoder. NIPP grunnlinje følger klassiske risikoanalyser og benytter numeriske data der det er mulig, med den hensikt å forenkle sammenlikning på tvers av sektorer, og synliggjøre

gjensidige avhengigheter.

NIPP grunnlinje består av sju kriterier fordelt på to kategorier. Den første kategorien gir indikasjon på om metoden er troverdig, mens den andre kontrollerer at metoden som benyttes er kompatible med andre standardmetoder for nasjonale og sektorspesifikke risikoanalyser. Troverdighet innebærer integritet, fullkommenhet og forsvarlighet. Kompatibilitet innebærer at metoden må være dokumentert, åpen, reproduserbar og nøyaktig. Dersom metoden tilfredsstiller kriteriene kan den fortsatt benyttes sammen med RAMCAP. I motsatt fall må den modifiseres eller erstattes med RAMCAP.

Innen cyberinfrastruktur er DHS i ferd med å utarbeide en tverrsektoriell metode for å vurdere og identifisere elementer som er avhengig av Internett og IKT-relaterte tjenester. En slik metode baserer seg på NIPP grunnlinjekriteriene i anneks 3A, og innebærer å bestemme nasjonale kausale funksjoner, produkter og tjenester, utvikle en sektormodell samt benytte et "IKT-avhengighetsfilter" for å identifisere cyberelementer og systemer. Prioritering evalueres ut fra kost og effektivitetshensyn som sikrer at risikoreduksjonen blir størst mulig i forhold til investering.

Et sett retningslinjer og veiledninger vil bli laget for å lette implementeringen av RAMCAP. På overordnet nivå kommer en generell veiledning i RAMCAP samt en RAMCAP anvendelsesguide. For de ulike sektorene kan det bli produsert en standard veiledning for RAMCAP sårbarhetsanalyser (RAMCAP *security vulnerability assessments*, SVA) samt en RAMCAP sektorspesifikk veiledning.[57]

Amerikanerne benytter ikke én omforent metode i arbeidet med å identifisere og rangere kritisk infrastruktur. DHS er kritisert for ikke å samarbeide tilstrekkelig med privat sektor i utarbeidelsen av NIPP, spesielt fordi 85-90 % av amerikansk kritisk infrastruktur er eid av private. Kritikere hevder videre at utkastet til ny NIPP er best egnet til å pulverisere ansvar og til å unnvike vanskelige problemstillinger.[58]

6.1.2 VAM

VAM (*The Vulnerability Assessement & Mitigation Methodology*) er en metode for å vurdere og redusere sårbarheter i elektroniske informasjonssystemer.[59] Metoden er utgitt av Rand – *National Defense Reasearch Institute*. VAM består av en tekstelig gjennomgang av metoden og et dataverktøy i form av et Excel-ark for å understøtte gjennomføringen av metoden.

VAM er i utgangspunktet mer interessant for BAS5s første hovedmålsetting, nemlig å utvikle og

[57] DHS er ment å publisere *best practice* for evaluering av cyberrelatert sårbarhetsanalyse 120 dager etter at NIPP godgjennes. Draft NIPP v.2.0 2006. Kapittel 1A.3.3. *Assess Risks*.
[58] Federal Computer Week. 5.12.2005. *DHS issues infrastructure protection plan.* http://www.fcw.com/article91589-12-05-05-Print
[59] Antón, Phillip S. et al. 2003. *The The Vulnerability Assessement & Mitigation Methodology. Finding and Fixing Vulnerabilities in Informasjons Systems.*Rand National Defense Research Instiute.

anvende en ROS-metode på samfunnsviktige IKT-systemer. Målsettingen til VAM faller også sammen med den originale målsettingen til BAS5-prosjektet, nemlig å utvikle en ROS-metode for å redusere sårbarheter mot høykapasitetstrusler så som dataangrep fra andre nasjoner eller ressurssterke terrorgrupper. Den er likevel omtalt her, fordi en rekke av kriteriene for å måle sårbarhet, i utgangspunkter også er gyldige i denne sammenhengen

Fordi metoden er arbeidskrevende og omfattende, er den ikke testet i form av et *case* i BAS5-prosjektet. Det følgende gir derfor kun en kort oversikt over hensikt og metodisk tankegang samt bruken av sårbarhetskriterier.

Metoden tar utgangspunkt i seks steg:

1) Identifisering av virksomhetens viktigste informasjonsfunksjoner
2) Identifisering av de informasjonssystemene som er avgjørende for å implementere disse funksjonene
3) Identifisering av sårbarhetene i disse systemene
4) Identifisering av relevante sikkerhetsteknikker for å redusere disse sårbarhetene
5) Valg av og bruk av teknikker basert på begrensinger, kost og nytte
6) Test av motstandsdyktighet og faktisk gjennomførbarhet under trusler

Steg 3-6 kan repeteres ved behov.

VAM tar hensyn til andre sårbarheter enn de rent systemtekniske når sårbarhet i informasjonssystemet skal vurderes. Det gjør metoden blant annet ved også å ta hensyn til fysiske og menneskelige/sosiale forhold. Den tar også hensyn til avhengighet av eksterne infrastrukturer. Metoden har en *top-down* tilnærming, og søker å avdekke sårbarheter som ikke bare er kjente eller utnyttet, men også potensielle sårbarheter som ikke er kjente eller utnyttet.

Følgende sårbarhetsmatrise viser bredden i VAM:

		Object of Vulnerability			
		Physical	Cyber	Human/Social	Enabling Infrastructure
	Attributes	Hardware (data storage, input/output, clients, servers), network and communications, locality	Software, data, information, knowledge	Staff, command, management, policies, procedures, training, authentication	Ship, building, power, water, air, environment
Design/Architecture	Singularity				
	Uniqueness				
	Centrality				
	Homogeneity				
	Separability				
	Logic/ implementation errors; fallibility				
	Design sensitivity/ fragility/limits/ finiteness				
	Unrecoverability				
Behavior	Behavioral sensitivity/ fragility				
	Malevolence				
	Rigidity				
	Malleability				
	Gullibility/ deceivability/naiveté				
	Complacency				
	Corruptibility/ controllability				
General	Accessible/ detectable/ identifiable/ transparent/ interceptable				
	Accessible/ detectable/ identifiable/ transparent/ interceptable				
	Hard to manage or control				
	Self unawareness and unpredictability				
	Predictability				

Figur 6.3. VAMs sårbarhetsmatrise.

På den horisontale skalaen vises det til ulike systemkomponenter i informasjonssystemet i forhold til om de er fysiske, *cyber*, menneskelige/sosiale eller eksterne infrastrukturer. Med fysiske menes

ulike *hardware*komponenter i systemer. Med *cyber* menes *software*, data, informasjon og kunnskap. Med menneskelig/sosial menes brukere, utviklere, ledelse, organisasjonsstruktur, *policies* etc. Med eksterne infrastrukturer menes de infrastrukturene som er nødvendig for å opprettholde drift, så som elektrisitet, bygningsmasse, vannforsyning og så videre.

På den vertikale skalaen vises det til ulike sårbarhetskriterier. Disse er delt opp i tre hovedbolker. For det første en som omhandler design og arkitektur, for det andre en som omhandler oppførsel og for det tredje en generell del. For en større detaljering av den vertikale aksen, se drøfting under. Matrisen danner rammer for sårbarhetsvurderingen, og rammen for sårbarhetsreduserende tiltak. Selve metoden er mer detaljert og omfattende enn det denne matrisen viser.[60]

6.1.3 Drøfting

Selv om BAS5-prosjektet ikke har gått i dybden i VAM, kan en enklere gjennomgang gi informasjon med overføringsverdi. For det første er det en overføringsverdi ut fra VAMs seks steg. De gir rammene for en overordnet prosess i forhold til å identifisere og rangere kritiske samfunnsfunksjoner. Ved å foreta en enkel modifisering av stegene, kan de overføres til vårt formål:

1) Identifisering av virksomhetens*/sektorens/samfunnets* viktigste ~~informasjons~~funksjoner[61]
2) Identifisering av de ~~informasjons~~systemene som er avgjørende for å implementere disse funksjonene
3) Identifisering av sårbarhetene i disse systemene
4) Identifisering av relevante sikkerhetsteknikker for å redusere disse sårbarhetene
5) Valg av og bruk av teknikker basert på begrensinger, kost og nytte
6) Test av motstandsdyktighet og faktisk gjennomførbarhet under trusler

Avhengig av hvilket nivå man befinner seg på (en virksomhet, sektor, samfunnet etc.), må de viktigste funksjonene identifiseres. Videre må man operasjonalisere funksjonene ned til konkrete systemer. Man må identifisere sårbarhetene i de konkrete systemene, så vel tiltak for å redusere sårbarhet og øke robustheten. Det må så foretas et valg om sårbarhetsreduserende tiltak på bakgrunn av begrensinger og kost/nytte, og til slutt må implementerte tiltak testes ut.

For det andre er det en overføringsverdi ut fra VAMs sårbarhetskriterier. Dette gjelder sårbarhetskriterier som:

- Særegenhet
- Unikhet
- Sentralitet
- Homogenitet
- Atskillelighet

[60] For en videre drøfting av VAM, se Føli, Anja Elisabeth 2006. Hovedoppgave: *Utvikling av verktøy for evaluering av risiko- og sårbarhetsanalyser*. Universitetet i Stavanger 22. juni 2006.
[61] Det som står i kursiv er lagt til, det som er overstreket, er trukket fra VAMs seks steg

- Feilbarhet
- Design sensitivitet / -skjørhet / -grenser / -endelighet
- Uoverkommelighet
- Atferdsmessig sensitivitet / -skjørhet
- Uvilje
- Rigiditet
- Tilpasningsevne
- Lettroenhet / lett å bedra / naivitet
- Selvtilfredshet
- Korruptbarhet / kontrollbarhet
- Tilgjengelig / oppdagbar / identifiserbar / transparent / evne til å fange opp
- Vanskelig å styre eller kontrollere
- Ikke være bevisst og uforutsigbar
- Forutsigbarhet

Uten å gå i dybden på hver enkelt, kan det hevdes at listen identifiserer et sett med sårbarheter som er nyttige i forhold til å få med seg bredden i de sårbarhetsutfordringene eksempelvis en virksomhet står overfor.

6.2 Danmark – Beredskapsstyrelsens model for risiko- og sårbarhedsanalyse av samfundets kritiske funktioner

Den danske Beredskapsstyrelsen (BRS) har utviklet en modell for risiko- og sårbarhetsanalyser som er tilgjengelig på deres nettsider.[62] ROS-modellen er et verktøy for å identifisere og vurdere trusler, risiko og sårbarheter, og er i utgangspunktet tiltenkt danske *myndigheter*. Beredskapsstyrelsen åpner imidlertid for at også andre kan ta metoden i bruk.

ROS-modellen benytter et brukervennlig word-basert skåringssystem som innebærer både en risikovurdering og en sårbarhetsanalyse. Ut fra en skala fra 1 til 5 vurderes sektoren som mindre eller mer risikoutsatt og sårbar. I tillegg til en introduksjon og brukerveiledning, består modellen av følgende fire deler, som er realisert i hvert sitt skjema tilgjengelig på Beredskapsstyrelsens hjemmeside:

- Utgangspunkt for analysen
    - Identifisering av aktøren (bakgrunnsopplysninger), de kritiske funksjoner og aktørens beredskapsansvar
- Oppstilling av trusselscenarier
    - Identifisering og beskrivelse av trusler som kan ødelegge eller forstyrre de kritiske funksjonene
- Analyse av trusselsenariet
    - Scenariobasert vurdering av sårbarheter og risiko
- Risikoprofil

[62] Beredskapsstyrelsen 2005. *ROS-modellen. Beredskabsstyrelsens model for risiko- og sårbarhedsanalyse af samfundets kritiske funktioner*. http://www.brs.dk/folder/nationalsaarbarhedsrapport2005/ros.htm

- Oppstilling av risiko- og sårbarhetsprofil for hver av de kritiske funksjonene

Hver del er bygget opp som et dynamisk word-dokument med en kombinasjon av fastlagte lukkede alternativer og åpne felter. I det følgende vil det bli gitt en gjennomgang av de fire delene den danske ROS-modellen inneholder.

6.2.1 Utgangspunkt for analysen

Denne første delen danner utgangspunktet for analysen og inkluderer følgende punkter:

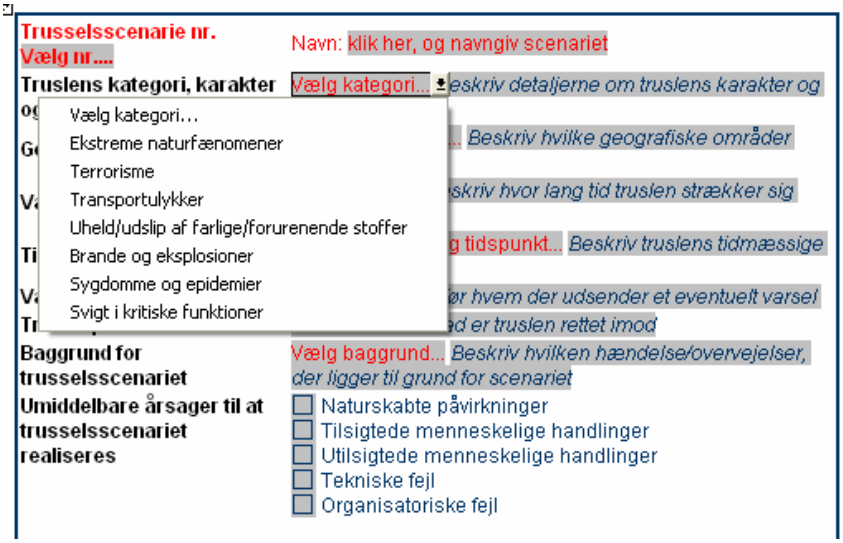
- Bakgrunnsopplysninger: Fastlegge hvilken aktør/myndighet som står bak analysen og hvem som er deltagere i analysearbeidet.
- Identifisering av beredskapsansvar:
    a. Hvilke av samfunnets kritiske funksjoner har myndigheten/aktøren ansvaret for å opprettholde og videreføre i tilfelle større ulykker og katastrofer?
    b. Hvilken kritisk funksjon omfatter denne risiko- og sårbarhetsanalysen? (ROS-modellen er utformet med tanke på at det skal gjennomføres separate analyser av hver av de kritiske funksjonene som myndigheten/aktøren har ansvar for å opprettholde i tilfelle større ulykker og katastrofer).
    c. Hvorfor gjennomføres risiko- og sårbarhetsanalysen?
    Her skal det krysses av for om det gjelder: 1) ny analyse, 2) rutinemessig analyse/oppdatering, 3) lovmessig krav, 4) større endring i trusselbildet, 5) større endringer i egen organisasjon eller ansvarsområde, 6) eller om det er andre årsaker til at ROS-analysen gjennomføres.

6.2.2 Identifisering av trusler

Denne delen har som formål å identifisere relevante trusselscenarier. Metoden tar høyde for at man kan inkludere så mange trusselscenarier som er relevante eller man har kapasitet til. Figur 6.3 viser et utsnitt fra del 2 av ROS-analysen.

Figur 6.3. Eksempel fra den danske ROS-modellen, del 2: Identifikasjon af trusler

Enkelte av feltene har fastlagte alternativer, slik at brukeren enkelt kan velge det alternativet som passer for det aktuelle trusselscenariet. Figur 6.4 viser hvilke alternativer man har for feltet "trusselens kategori, karakter".



Figur 6.4. Eksempel på svaralternativer for feltet "truslens kategori, karakter"

I tillegg til trusselens kategori ligger det også fastlagte alternativer for de følgende fem kriteriene, se Tabell 6.2.

Geografisk utbredelse	Varighet	Tidsmessig plassering	Varsel	Bakgrunn for trusselscenariet
Lokal **Regional** **Nasjonal** **Internasjonal** **Ikke relevant**	**0-1 dag** **2-7 dager** **1-4 uker** **1-6 mnd.** **6-12 mnd.** **>12 mnd.** **Ikke relevant**	**Årstid: vår/sommer/ høst /vinter** **Tid på døgnet:** - **hverdag innenfor normal arbeidsdag** - **hverdag utenfor arbeidstid** - **Helg, ferie, helligdag** - **Tidspunktet er ikke relevant**	**Ingen varsel** **Kort varsel** **Lengre varsel**	**Observert hendelse innen egen sektor** **Observert hendelse i Danmark** **Observert hendelse utland** **Tenkt hendelse som vil kunne påvirke egen sektor**

Tabell 6.1 Fastlagte alternativer for ulike kriterier

Som det også står beskrevet i del 2 av ROS-modellen gir den tilhørende veiledningen en oversikt over noe relevante trusselkategorier. Disse strekker seg fra naturkatastrofer, ulykker, epidemier til terrorisme, og skal være til inspirasjon når den enkelte aktør skal velge trusselscenario.

6.2.3 Analyse av trusselscenarier

Del 3 av analysen inneholder samme oppsett som de to foregående delene, men er inndelt i fire avsnitt som vil bli gjennomgått i det følgende.

Vurdere sårbarheten til den kritiske funksjonen

Dette avsnittet inneholder 8 spørsmål som ser på tilgjengelig kapasitet innenfor områdene ”forebygging og skadebegrensning”, ”beredskapsplanlegging”, ”innsats og hjelpearbeid” og ”reetablering”.

For å vurdere kapasitetene er det laget følgende hjelpetabell, Tabell 6.2:

	Overordnet sårbarhetsnivå		Forebygging og skadebegrensning	Beredskapsplanlegging, innsats og hjelpearbeid, reetablering
1	Meget lav sårbarhet	≈	Avverger alle skader	Tilstrekkelig
2	Lav sårbarhet	≈	Avverger hovedparten av skadene	Overveiende tilstrekkelig, få mangler
3	Middels sårbarhet	≈	Avverger noen skader	Noen alvorlige mangler
4	Høy sårbarhet	≈	Avverger få skader	Mange alvorlige mangler
5	Meget høy sårbarhet	≈	Avverger ingen skader	Helt utilstrekkelig

Tabell 6.2 Fastlagte alternativer for ulike kriterier

På bakgrunn av denne tabellen kan man tilegne verdier til sårbarheten innenfor de ulike områdene.

Vurdere sannsynligheten

Neste trinn i analysen innebærer å fastsette sannsynlighet for at hendelsen kommer til å inntreffe. Tabell 6.3 er til hjelp i denne fasen:

	Sannsynlighetsnivå		Hyppighet/frekvens (hvor ofte det forventes at hendelsen inntreffer)	Plausibilitet (muligheten for at hendelsen inntreffer innen en gitt 12 mnd. periode)
1	Meget usannsynlig	≈	Mindre enn 1 gang i løpet av 100 år	Vil nesten helt sikkert ikke inntreffe innen 12 mnd.
2	Overveiende usannsynlig	≈	Mellom 1 gang i løpet av 50 år og 1 gang i løpet av 100 år	Vil neppe inntreffe innen 12 mnd.
3	Mindre sannsynlig	≈	Mellom 1 gang i løpet av 10 år og 1 gang i løpet av 50 år	Kan, men vil ikke nødvendigvis, inntreffe innen 12 mnd.
4	Sannsynlig	≈	Mellom 1 gang i løpet av 1 år og 1 gang i løpet av 10 år	Kan meget godt inntreffe innen 12 mnd.
5	Meget sannsynlig	≈	Mer enn 1 gang i løpet av 1 år	Vil nesten helt sikkert inntreffe innen 12 mnd.

Tabell 6.3 Hjelpetabell for å fastsettes sannsynlighetsnivå

Hyppighet er ment å brukes dersom man kan ta utgangspunkt i egne erfaringer eller historiske eller statistiske data. Dersom en hendelse aldri er inntruffet kan man heller gi en kvalifisert

gjetning på hvor plausible hendelsene er.

Vurdere konsekvenser

Konsekvensene vurderes i to trinn:

a) Konsekvenser for opprettholdelse av den kritiske funksjonen
   - Nøkkelpunkter (vesentlige bygninger, fysiske installasjoner)
   - Medarbeidere og ledelse
   - IT-systemer
   - Tilgang på energi (el/gass/olje)
   - Tilgang på nødvendige materialer/varer/tjenesteytelser
   - Transport/distribusjon av den kritiske funksjonen
   - Informasjon og kommunikasjon
   - Annet

b) Konsekvenser for det øvrige samfunn
   - Direkte konsekvenser av hendelsen:
     - Tap av liv og velferd
     - Tap av aktiva (materielle, finansielle, miljømessige etc.)
     - Angst, utrygghet eller sinne hos befolkningen
     - Politisk indignasjon
   - Avledete konsekvenser som tap/ødeleggelse av den kritiske funksjonen vil ha for samfunnets evne til å fungere, dvs. konsekvenser for kritisk infrastruktur: Energi, Kommunikasjon og IT, Transport, Finans og økonomi, Fødevarer, Vann, Farlige stoffer, Beredskap, Sunnhet, Offentlig forvaltning, Nasjonal sikkerhet.

Innenfor alle disse områdene skal det gis en beskrivelse av hvilke konsekvenser som kan oppstå, samt en fastsetting av konsekvensnivå. Konsekvensene er gitt ved følgende indeksering, se Tabell 6.4:

1	Meget begrensede	≈	Få og små skader/tap på kort sikt
2	Begrensede	≈	Moderate skader/tap på kort sikt
3	Alvorlige	≈	Betydelige skader/tap på kort eller lengre sikt
4	Meget alvorlige	≈	Meget store skader/tap på lengre sikt
5	Kritiske/katastrofale	≈	Ekstremt alvorlige skader/tap på lang sikt, eller permanente skader

Tabell 6.4 Hjelpetabell for å fastsette konsekvensnivå

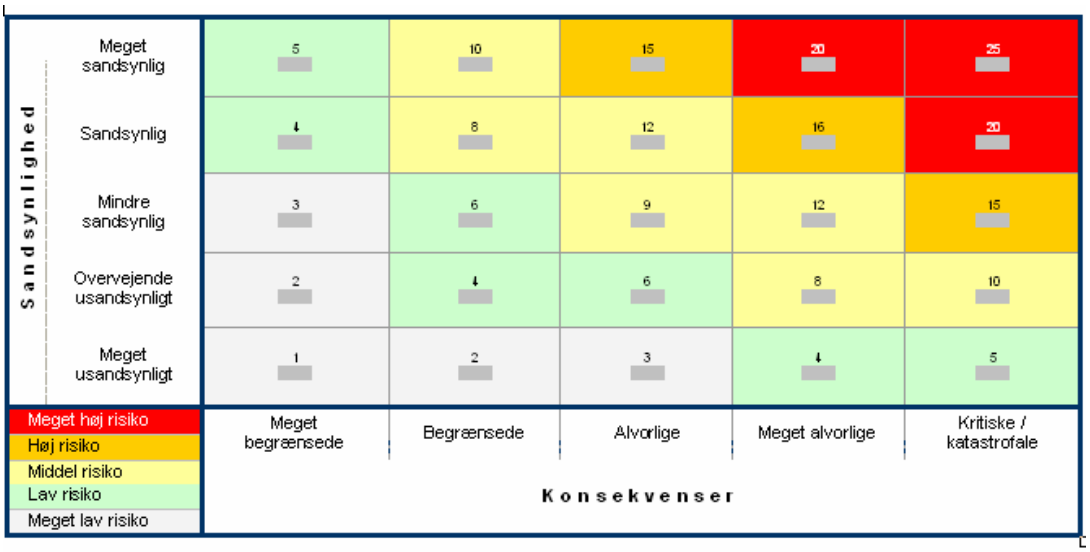
Fastsette risikonivå

Til slutt skal det overordnete risikonivået for det analyserte scenariet fastsettes, ved at man multipliserer sannsynlighet og konsekvens som er funnet gjennom trinnene over.

Sammenstilling av risiko og sårbarhet

Resultatene fra de tre første delene/skjemaene oppsummeres til slutt i to tabeller. Den ene representerer risiko uttrykt ved sannsynlighet og konsekvens, og den andre representerer sårbarhetsnivået for trusselscenariene.

I matrisen under (Figur 6.5) kan man plassere de gjennomgåtte scenariene på bakgrunn av de verdiene man har kommet frem til i avsnitt 6.2.3:



Figur 6.5 Risikomatrise, uttrykt ved sannsynlighet og konsekvens

På samme måte kan man plassere sårbarhetsnivået for hvert trusselscenario i en oversiktlig tabell, som i Tabell 6.5.

Meget høj sårbarhed Høj sårbarhed Middel sårbarhed Lav sårbarhed Meget lav sårbarhed	Vurdering af sårbarhedsniveau			
Trussels-scenarier	Forebyggelse og skadesbegrænsning	Beredskabs-planlægning	Indsats og afhjælpning	Reetablering
Anfør nr. og navn	...	...	...	...
Anfør nr. og navn	...	...	...	...
Anfør nr. og navn	...	...	...	...
Anfør nr. og navn	...	...	...	...
Anfør nr. og navn	...	...	...	...
Anfør nr. og navn	...	...	...	...
Anfør nr. og navn	...	...	...	...
Anfør nr. og navn	...	...	...	...
Anfør nr. og navn	...	...	...	...
Anfør nr. og navn	...	...	...	...
Anfør nr. og navn	...	...	...	...
Anfør nr. og navn	...	...	...	...

Tabell 6.5 Sårbarhetsnivå for ulike trusselscenarier

Ut fra disse tabellene kan man dermed si noe om hva som er mest kritisk ut fra risiko og sårbarhet og følgelig foreta en prioritering.

Den danske metoden gir nyttige innspill til metodikk for BAS5 ettersom den presenterer et helhetlig rammeverk. Metoden er enkel, brukervennlig og klar til bruk. Ved at metoden ligger tilgjengelig på Beredskapsstyrelsens hjemmesider kan alle som vil benytte den, og de ulike word-dokumentene er selvforklarende og enkle å navigere seg rundt i. Dersom man har behov for ekstra støtte underveis i prosessen, kan man benytte en kortfattet veiledning som gir nærmere beskrivelse av de ulike trinnene i metoden.[63] Metoden presenterer også sluttproduktet av ROS-modellen, som består av en risiko- og sårbarhetstabell som oppsummerer gjennomgangen fra de foregående trinnene. Dette gir dermed et strukturert og presentabelt sluttprodukt som gir et godt sammenligningsgrunnlag.

Vi har ikke sett metoden anvendt i praksis, og kan dermed ikke si noe om hvor fornøyde brukerne er med den. De på forhånd definerte påvirkningskriteriene for scenarier i metoden gjør det mulig å skille scenariene fra hverandre og tilpasse dem etter de ulike virksomhetenes behov. Metoden egner seg derfor godt til å gjennomføre detaljerte analyser av scenarier som kan ramme ulike samfunnsfunksjoner.

6.3 England

I England har *Civil Contingencies Secretariat* (CCS)[64] utviklet noe som ligner på den danske

[63] Beredskapsstyrelsen 2005. *ROS-modellen. Beredskabsstyrelsens model for risiko- og sårbarhedsanalyse af samfundets kritiske funktioner*. http://www.brs.dk/folder/nationalsaarbarhedsrapport2005/ros.htm

[64] UK Resilience internettside mai 2006. *Introduction to the Civil Contingencies Secretariat*. http://www.ukresilience.info/ccs/index.shtm

metoden, hvor også resultatene av analysen ender opp i en risikomatrise.[65] Fremgangsmåten for å komme frem til risikomatrisen er noe annerledes, ved at britene har utviklet over 100 fare- og trusselscenarier. For hvert scenario er det foretatt en vurdering av sannsynlighet og konsekvens som ender opp i en tallfestet risiko*rating* (skåringsystem). Denne *ratingen* gir dermed et grunnlag for å rangere scenariene og si noe om hvilke som er mest kritiske. Omtrent halvparten av fare- og trusselscenariene er offentliggjort.

Et dokument på over 300 sider gir en veiledning til den engelske *Resilience Act*[66], men av spesiell interesse for vårt tilfelle er anneks 4 a-f. Metoden er forankret i lov, og politidistriktene i England har fått ansvar for å følge opp metoden. Ut fra dette kan det sies at England har kommet frem til en prosess som er en blanding mellom *top-down* og *bottom-up* tilnærming. Metoderammeverket er forankret på nasjonalt plan, men gjennomføringen foregår ute i politidistriktene hvor spesialkompetansen er størst.

Som støtte for gjennomføring av metoden har CCS fastsatt følgende hjelpetabeller:

- liste over innvirkningskategorier (konsekvenser)
- sannsynlighetskriterier
- risikomatriser

I det følgende blir det gitt en kort gjennomgang av disse hjelpetabellene og hvilke kriterier som ligger til grunn, før det i avsnitt 6.3.4 blir vist eksempel på en metode anvendt i praksis.

6.3.1 Innvirkningskategorier/konsekvenser

Britene har laget en kvalitativ liste over innvirkningskategorier, dvs. konsekvenser, fordelt på fem nivåer. For hvert konsekvensnivå fra 1-5 er det gitt en nærmere beskrivelse og synliggjøring av hva det aktuelle konsekvensnivået har å si for de fire kategoriene helse, samfunn, økonomi og miljø. Dette er skissert i Tabell 6.6:

[65] HM Government (Udatert). *Emergency Preparedness. Guidance on Part 1 of the Civil Contingencies Act 2004, its associated Regulations and non-statutory arrangements*. Annex 4F.
http://www.ukresilience.info/ccact/eppdfs/emergprepfinal.pdf
[66] Office of Public Sector Information. *Civil Contingencies Act 2004*. Chapter 36. Internettside mai 2006.
http://www.opsi.gov.uk/acts/acts2004/20040036.htm

Nivå/ beskrivelse	Innvirknings-kategori	Beskrivelse av konsekvens
1/ Ubetydelige	Helse	Ubetydelig antall skader eller konsekvenser for helse
	Samfunn	Ubetydelig antall personer må forflyttes og ubetydelig behov for personlig assistanse Ubetydelige forstyrrelser i velferdstjenester, inkludert transporttjeneste og infrastruktur
	Økonomi	Ubetydelig innvirkning på lokal økonomi
	Miljø	Ubetydelig innvirking på miljøet
2/ Liten	Helse	Et fåtall personer berørt, ingen dødsfall, et fåtall småskader med behov for førstehjelp
	Samfunn	Mindre skader på eiendom Mindre forflytning av et lite antall mennesker i < 24 timer og lite behov for personlig assistanse Mindre lokaliserte forstyrrelser i velferdstjenester og infrastruktur < 24 timer
	Økonomi	Neglisjerbar effekt på den lokale økonomien og kostnadene dekkes lett
	Miljø	Liten effekt på miljøet uten langvarige skadevirkninger
3/ Moderate	Helse	Moderat antall dødsfall og noen skader som krever sykehusinnleggelse, medisinsk behandling og aktivering av MAJAX; det automatiske intelligente varslingssystemet, prosedyrer i et eller flere sykehus.
	Samfunn	Skade som er avgrenset til et spesifikt område, eller til et antall områder, men trenger ytterligere ressurser. Forflytning av > 100 personer i 1-3 dager Lokal sammenbrudd av infrastruktur og velferdstjenester.
	Økonomi	Begrenset effekt på lokal økonomi med noe tap av produksjon på kort sikt, med mulige opprydningskostnader i tillegg.
	Miljø	Begrensede konsekvenser for miljøet med kort- eller langtidseffekt.
4/ Betydelige	Helse	Betydelig antall mennesker i det rammede området er rammet av mangfoldige dødsfall, mangfoldige alvorlige eller omfattende skader, betydelig mengde sykehusinnleggelser og aktivering av MAJAX prosedyrer ved flere sykehus.

	Samfunn	Betydelig ødeleggelse som krever eksterne ressurser i tillegg til lokale hjelpearbeidere 100 til 500 mennesker i fare og må forflyttes i mer enn 1 uke. Lokale hjelpearbeidere trenger eksterne ressurser for å kunne yte personlig assistanse. Betydelig innvirkning på og mulige sammenbrudd i leveringsevne til enkelte lokale samfunnstjenester
	Økonomi	Betydelig innvirkning på lokal økonomi med tap av produksjon på "medium term" Betydelige tilleggskostnader til opprydning og gjenoppretting
	Miljø	Betydelig innvirkning på miljøet med mellomlang til lang varighet
5/ Katastrofale	Helse	Veldig stort antall mennesker i det berørte området med et betydelig antall dødsfall, stort antall personer behov for sykehusinnleggelse med alvorlige skader med langtids skadevirkninger
	Samfunn	Omfattende ødeleggelser på eiendommer og menneskeskapt miljø i berørt område krever stor opprydning Omfattende forflytning av mer enn 500 mennesker i lang varighet og stort behov for personlig assistanse Alvorlige ødeleggelser på infrastruktur som forårsaker betydelig forstyrrelse i, eller tap av, nøkkeltjenester i lang tid. Samfunnet ute av stand til å fungere uten betydelig assistanse.
	Økonomi	Alvorlige innvirkninger på lokal og regional økonomi med noen langtidseffekter, og mulig permanent tap av produksjon, med noen bygningsmessige skader Omfattende kostnader til opprydning og gjenoppretting
	Miljø	Alvorlige langtidseffekter for miljøet og/eller permanente ødeleggelser

Tabell 6.6 Beskrivelse av ulike konsekvenser for helse, samfunn, økonomi og miljøet

Ved å bruke en 5-trinnsskala og spesifisere hva som menes med de ulike trinnene, vil det være relativt enkelt for brukerne av metoden å tilegne riktig verdi til hvert scenario.

6.3.2 Fastlegging av sannsynligheter

Ved å bruke en 5-trinnsskala er det laget en hjelpetabell som viser ulike konsekvensnivåer, se Tabell 6.7.

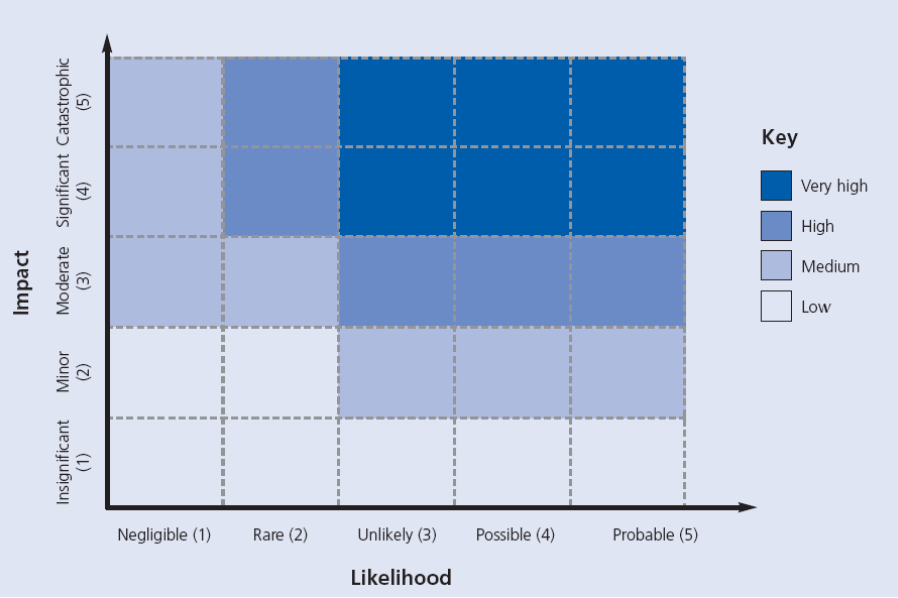
Nivå	Beskrivelse av nivå	Sannsynlighet over 5 år	Sannsynlighet over 5 år
1	Neglisjerbar	>0.005%	>1 av 20,000
2	Sjelden	>0.05%	>1 av 2,000
3	Usannsynlig	>0.5%	>1 av 200
4	Mulig	>5%	>1 av 20
5	Sannsynlig	>50%	>1 av 2

Tabell 6.7 Beskrivelse av sannsynlighetsnivåer

De to kolonnene som illustrerer sannsynlighetene viser at et scenario som havner i kategori 3, ”usannsynlig”, har en sannsynlighet på 0,5% for å inntreffe over en tidsperiode på 5 år.

6.3.3 Oppstilling i risikomatriser

Resultatet av arbeidet vil man få ved å kombinere sannsynlighet og konsekvens for de ulike scenariene i en risikomatrise, se Figur 6.6:



Figur 6.6 Risikomatrise - England

Som matrisen viser, inndeles risikoene i fire ulike klasser: ”veldig høy”, ”høy”, ”medium” og ”lav risiko”. For hver av de fire klassene er det gitt en beskrivelse av hva slags tiltak som er nødvendige.[67] Disse varierer fra umiddelbare ekstratiltak som må iverksettes for de med høyest

[67] HM Government (Udatert). *Emergency Preparedness. Guidance on Part 1 of the Civil Contingencies Act 2004, its associated Regulations and non-statutory arrangements*. Annex 4F. http://www.ukresilience.info/ccact/eppdfs/emergprepfinal.pdf

risiko, til risiko med lavest sannsynlighet som kun må behandles som en del av det generelle planverket (med mindre det oppstår nye forhold som kan påvirke risikoen).

I risikomatrisen er det verdt å legge merke til asymmetrien, ettersom matrisen klassifiserer hendelser med både lav og høy sannsynlighet som kritiske risikoer, dvs. "veldig høy" risiko. Årsaken er at konsekvensene av hendelsene vil bli så store at de må behandles med høyeste prioritet.

6.3.4 Metoden anvendt i praksis: Avon and Somerset

Et eksempel på et politidistrikt som har fulgt veiledningen til CCS er Avon and Somerset. Resultatet av analysen har blitt en liste med farer/trusler, der omtrent halvparten er offentlig tilgjengelig. Ved å følge metoden til CCS har Avon and Somerset kommet frem til det er 13 (av de 84 som er offentlig tilgjengelig) av farene/truslene som havner i kategorien "veldig høy risiko", 18 blir kategorisert som "høy", 50 havner i kategorien "medium" og 3 farer i kategorien "lav"[68]. På denne måten har de kommet frem til en rangering av de identifiserte farene/truslene.

Skjemaet under (Figur 6.7) viser hvordan Avon og Somerset har satt opp de ulike farene og truslene, og fargene indikerer hva slags prioritet de ulike truslene har, avhengig av hvilken risikoklasse de havner innenfor:

[68] Resultatene fra Avon and Somerset kan leses i Avon and Somerset Local Resilience Forum. 2006. *Community Risk Register*. Version 2.1 January 2006. http://www.avonandsomerset.police.uk/information/documents/CachedDocuments/677_20060224135314.pdf

3 Community Risk Register

(Note: ***Outcome description codes:*** *'H' – hazard which will require a national as well as a local response (nationally defined); 'HL' – hazards which would not ordinarily prompt a national response and would usually be dealt with locally (nationally defined); 'L' – hazards which have been added to national outcome descriptions as a result of local considerations (locally defined). All outcome description codes are followed by a sequential numerical suffix (either nationally defined for 'H' and 'HL' codes or locally defined for 'L' codes.)*

DATE OF REVISION: November 2005								NEXT REVIEW DATE: November 2006				
RISK REF. NO.	HAZARD OR THREAT CATEGORY	HAZARD OR THREAT SUB-CATEGORY	OUTCOME DESCRIPTION	LIKELI-HOOD	IMPACT	RISK RATING	CAPABIL-ITY REQUIRED	CONTROLS CURRENTLY IN PLACE	ADDITIONAL RISK TREATMENT REQUIRED (WITH TIME SCALE)	RISK PRIORITY	LEAD RESPONSIB-ILITY	REVIEW DATE
Industrial accidents and environmental pollution												
IA/1	**Industrial accidents and environmen-tal pollution**	Fire or explosion at a gas terminal as well as LPG, LNG and other gas onshore feedstock pipeline and flammable gas storage sites.	H1 – Up to 3km around site causing up to 500 fatalities and up to 1,500 casualties. Gas terminal event likely to be of short duration once feed lines are isolated; event at a storage site could last for days if the explosion damaged control equipment.	Negligible (1)	Significant (4)	MEDIUM		See individual risk assessment form	None identified	2	Avon Fire and Rescue Service	Nov 06
			L1 – Incident spread off-site with more than five fatalities and/or 20 hospitalisations, evacuation beyond the cordon and significant effects on gas distribution systems (top-tier sites).	Unlikely (3)	Moderate (3)	HIGH		See individual risk assessment form	None identified	3	Avon Fire and Rescue Service	Nov 06
			L2 – Incident spread off-site with more than five fatalities and/or 20 hospitalisations, evacuation beyond the cordon and significant effects on gas distribution systems (lower-tier sites).	Possible (4)	Moderate (3)	HIGH		See individual risk assessment form	None identified	3	Avon Fire and Rescue Service	Nov 06
			L3 – Incident contained on-site, up to five fatalities and/or 20 hospitalisations, advice to shelter but no evacuation beyond the cordon and no significant effect on gas distribution systems (top-tier sites).	Possible (4)	Minor (2)	MEDIUM		See individual risk assessment form	None identified	2	Avon Fire and Rescue Service	Nov 06

Figur 6.7 Eksempel fra Avon and Somerset

Som skjemaet viser er det laget fare- og trusselkategorier som brytes ned i underkategorier. For hver av disse underkategoriene er det gitt en kort beskrivelse av mulige utfall dersom en bestemt hendelse inntreffer. For hvert utfall er det så gitt en beskrivelse av hvilken sannsynlighet dette har og hvilken konsekvens det har. Ved hjelp av Figur 6.7 har hvert utfall av en hendelse blitt tilegnet en risikorate og en indikasjon av hvilken prioritet risikoen har. I tillegg er det tatt med administrative detaljer som dato for revisjon, samt hvem som er ansvarlig for å følge opp tiltak.

Til grunn for dette oppsummeringsskjemaet ligger det separate skjemaer som viser farene og truslene i ytterligere detalj. Disse er ikke offentlige tilgjengelige, og vi kan dermed ikke si hvor mye arbeid som ligger til grunn. Likevel vitner metoden og den skjematiske fremstillingen fra Avon and Somerset om at dette har blitt gjennomført på en strukturert måte, og at man dermed har fått med alle tenkelige trusselkategorier. Oppsummeringsskjemaet viser også at det allerede ved oppstilling av scenariene i 2005 er planlagt en revisjon av risikoregisteret i 2006, og en slik systematisk oppstilling vil sannsynligvis være lett å vedlikeholde og ikke like tidkrevende som en første gjennomgang vil være.

På samme måte som for den danske metoden tilbyr den engelske metoden en strukturert måte å vurdere risiko på for ulike scenarier. Sluttproduktet gir en oversiktlig tabell med klare sammenligningsdata. I tillegg benytter metoden svært mange scenarier, noe som gir en mulighet for å konkretisere utfallet av ulike scenarier på en strukturert måte.

Metoden er i utgangspunktet utviklet som en del av beredskapsplanleggingen i England, og den er

ment til å anvendes innenfor de ulike politidistriktene. Metoden gir ingen direkte rangerte lister over hva som er kritisk infrastruktur, men basert på risikotall for de ulike scenariene har metoden potensial til å peke ut de mest kritiske infrastrukturene. Den engelske metodikken har dermed gitt BAS5-prosjektet innspill til scenarieutvelgelse, samt hva slags kriterier som ligger til grunn for fastsettelse av sannsynlighets- og konsekvensnivå for utfall av ulike trusler.

6.4 Sverige: Kriteriemodell för identifiering av samhällsviktiga verksamheter och system

I april 2005 utga FOI rapporten *Kriteriemodell för identifiering av samhällsviktiga verksamheter och system*. Rapporten er utarbeidet på oppdrag fra den såkalte *Informationssäkerhetsutredningen*, med mål om å utarbeide kriterier slik at hver enkelt aktør selv kan vurdere om egen virksomhet er samfunnsviktig eller ikke. Den ferdige metoden er tenkt å kunne anvendes på flere nivåer, helt fra den enkelte virksomhet, til bransjeorganisasjoner og myndigheter, og kan videre anvendes på både private og offentlige aktører med nasjonalt, regionalt og lokalt perspektiv. Metoden er primært utformet med tanke på virksomheter og systemer som er relatert til informasjonssystemer, men er ment å være så generell at den også kan brukes i andre sammenhenger når grad av samfunnsviktighet skal bedømmes.

Arbeidet er på mange områder parallelt med deler av BAS5, og er derfor et sentralt underlagsmateriale. Rapporten inneholder i grove trekk en redegjørelse for hensikten med å etablere en metode, den har en omtale av arbeid i andre land og presenterer en metode for å identifisere samfunnskritske virksomheter og systemer. Det er også en gjennomgang av hvordan metoden skal eller burde forvaltes av offentlige myndigheter. Hele rapporten er relevant for BAS5, men det vil i det følgende bli fokusert på selve metoden.

Modellen skiller seg noe fra målsettingen i BAS5 ved at den har fokus på å identifisere, ikke rangere. Legg også merke til at den ikke er en ferdig metode. Det er lagt opp til at erfaringer fra praktisk bruk vil justere metoden underveis. Metoden er kun testet i et relativ enkelt case, nemlig vannforsyning i en kommune. I studien er det benyttet litteraturstudier, intervjuer og analyse som metode.

Før vi redegjør for selve metoden, la oss først se på noen relevante problemstillinger, forutsetninger og observasjoner som fremkommer i rapporten, og som er relevante for BAS5:

- Det er behov for en ensartet metode
- Ved vurderinger av samfunnskritikalitet mangler et helhetlig og omforent sett med kriterier
- Man mangler kunnskap om hvilke kriterier som er lagt til grunn ved tidligere anledninger
- Metoden skal komme med adekvate kriterier for samfunnsviktighet
- Metoden skal være uavhengig av virksomhet eller system
- Metoden skal være uavhengig av nivå
- Metoden skal gi tydelighet og sporbarhet i resonnement og vurderinger
- Skal være et verktøy for å prioritere og å velge relevante tiltak for dagens samfunn til

fredstidskriser og forhøyet beredskap.
- Hvem skal være ansvarlig for forvaltningen av metoden?

Det blir vist til en rekke fordeler og ulemper med en metode for å identifisere. Fordelene er:

- Det er et behov for å peke ut samfunnsviktige virksomheter.
- Flere sentrale myndigheter mangler oversikt over samfunnsviktige virksomheter.
- Er beskrevet som problematisk at systemeiere og systemforvaltere bruker sine egne modeller.
- En omforent modell vil samkjøre synet på hva som er en samfunnsviktig virksomhet, og bidra til at aktører "snakker samme språk".
- En kriteriemodell kan utgjøre et underlag for å analysere endrede eller nye trusler (f. eks ved store infeksjonsepidemier vil en kriteriemodell gjøre det enklere å iverksette relevante tiltak).
- Ha en ensartet tilnærming for å komme med kontrolltiltak mot de riktige virksomhetene.

Ulempene er:

- Hva skjer med de virksomheter som utpekes? Vil det skapes et statlig forvaltningssystem som virker konkurransevridene, og at krav blir satt uten å ta hensyn til næringslivets vilkår?
- Hvis det innebærer en fordel (f. eks. økonomisk kompensasjon) å bli inkludert på en liste, vil det føre til at for mange blir inkludert, og at verdien av listen blir mindre?
- Det er en fallgruve å snakke om allmenn viktighet. Hvis ikke samfunnsviktigheten blir relatert til "hvorfor" og ikke bedømmes ut fra f. eks. tidsaspekter, blir det vanskeligere å prioritere mellom ulike virksomheter. Modellen kan på en slik måte skape usikkerhet.
- Verktøyet kan fungere på sentralt nivå, men kan bli opplevd som for firkantet på lokalt nivå.
- En kriteriemodell blir for styrende og dermed hemmende. Det kan være vanskelig å forene kriterier med fleksibilitet, og tanken kan bli låst.
- Ansvarsprinsippet kan få mindre å si; hvis man ikke er på "listen", så reduseres ansvarsforholdet.
- Gir en feil fordeling av ressurser, ved at ressurser avsettes til arbeid på sentralt hold med vurderinger som ikke har vist sin nytte, i stedet for å prioritere mer praktisk arbeid.
- Risiko for at tiltak som kobles til samfunnsviktighet relativt raskt kan bli foreldet.
- Risiko for at kriterier og lister blir permanente uten å bli gjenstand for regelbundet revurdering.

6.4.1 Vurdering av andre lands arbeid

Samfunnsviktige virksomheter er i økende grad avhengig av forhold utenfor landet. Det blir i rapporten oppgitt å være en fordel hvis de svenske kriteriene er i samklang med det øvrige Europa. Med det som bakgrunn blir det i korte trekk vist til studier i utlandet som er relevante for FOIs studie. I hovedsak omhandlet det:

- Europakommisjonens *Critical Infrastructure in the fight against terrorism*[69] fra 2004:
  Er et sett med kriterier for å identifisere samfunnsviktig infrastruktur uten at det er satt inn i noen spesiell metode. Kriteriene er organisert ut fra tre hovedkategorier, nemlig rekkevidde, størrelse/alvorlighet og effekter av tid. For en nærmere redegjørelse, se senere i bakgrunnsstudien.
- Finlands strategi for sikring av samfunnets livsviktige funksjoner fra 2003.[70]
  Den finske strategien har, i følge FOIs rapport, kommet til at kriseberedskapsarbeidet skal struktureres ut fra syv livsviktige funksjoner. FOI har ikke funnet noen utførlig redegjørelse for hvordan strategien har blitt utarbeidet, men tilkjennegir hva som blir ansett som mest viktig. De syv livsviktige funksjonene er:
  - Ledelse av staten
  - Ekstern handlingsevne
  - Rikets militære forsvar
  - Intern sikkerhet
  - Økonomiens og samfunnets funksjonsevne
  - Beskyttelse av befolkningens utkomme/livsopphold og evne til å ha virksomheter(verksamhetsförmåga)
  - Mental evne til å takle kriser (mental kristålighet)
- Den canadiske studien *Y2K Experience*.
  Dette er en canadisk studie som kom i forbindelse med årtusenskiftet, hvor det ble formulert fire mål for å sikre seg ved overgangen. Omtalen er meget kort, og den canadiske studien er svært lite relevant sett opp mot annet arbeid som pågår i Canada.
- Den nederlandske studien *Quick Scan*.
  Quick Scans målsetting var å identifisere kritisk infrastruktur og beskrive gjensidige avhengigheter. I Quick Scan ble en sektor sett på som kritisk hvis sammenbrudd eller alvorlig forstyrrelse kan lede til skade på et nasjonalt nivå. Det vises til tekst om Quick Scan senere i denne studien.
- Det norske BAS-prosjektet
  Rapporten konstaterer at BAS5 har store likheter med FOIs studie, og at fortsatt kontakt innenfor informasjonssikkerhetsarbeidet mellom BAS5 og FOI bedømmes som fruktbart.

6.4.2 Annet relevant arbeid i Sverige

Rapporten viser til flere relevante arbeider i Sverige sett opp mot å identifisere hva som er kritisk for et samfunn i ulike situasjoner. Det er studier om hvilke samfunnsfunksjoner som er viktige for å gjennomføre mobilisering, minimumsnivå for individers overlevelse og samfunnets funksjon i krig, energiproblemer i krig, strategier for sikker elforsyning, innledende analyse av gjensidige avhengigheter i samfunnet, samfunnskritiske transportert og så videre. Felles for disse er at det blir presentert en rekke lister, men uten av det ligger noen kriterier bak utvalget. Vurderingene er ofte produsert som resultat av diskusjoner.

[69] Communication from the Commission to the Council and the European Parliament. COM (2004) 702 final. *Critical Infrastructure Protection in the fight against terrorism*. Brussels. 20.10.2004.
[70] Försvarsministeriet, Finland 2003. *Strategi för tryggande av samhällets livsviktiga funktioner*. Statsrådets principbeslut 27.11.2003.

Et arbeid som er av interesse ut fra en teoretisering av kriterier, er en FOI-rapport fra 1996 om store belastninger (*Svåra påfrestningar*). Som en del av arbeidet ble det presentert en teoretisk diskusjon om de kriterier som ble ansett å karakterisere begrepet "store belastninger". Kriteriene ble delt i tre grupper:

1. De som utgår fra årsakene til en hendelse – *årsakskriterier*
2. De som utgår fra hendelsens konsekvens – *konsekvenskriterier*
3. Metoder for å håndtere situasjonen etter hendelsen – *metodekriterier*.

De konsekvenskriteriene som ble beskrevet bestod av to typer, nemlig *karakteristika* eller basisfaktorer som ligger til grunn for at en hendelse får omfattende konsekvenser (plutselighet, varighet, gjentakelse, kompleksitet), samt *konsekvenser av situasjonen* (ressurstilgang, sentrale eller perifere virkninger, sosiale virkninger).

6.4.3 Grunnleggende verdier i samfunnet og samfunnets vitale interesser

Metoden legger opp til en diskusjon om de grunnleggende verdiene i samfunnet. Eksempler på slike verdier er befolkningens liv og helse, miljø, økonomi, demokrati, menneskerettigheter, trygghet, frihet, toleranse, pluralisme og rettsikkerhet. Det blir også vist til at man kan ta et individperspektiv i stedet for et samfunnsperspektiv som utgangspunkt. For eksempel den enkeltes rett til liv, frihet, god levestandard, rent miljø, helse, arbeid osv. Disse verdiene konkretiseres og presiseres til det som blir omtalt som samfunnets vitale interesser. De vitale interessene utgjør grunnlaget for å vurdere hvor viktig en virksomhet er for samfunnet. Med andre ord: Virksomheten blir å betrakte som viktig for samfunnet hvis en forstyrrelse eller et bortfall medfører alvorlige konsekvenser for samfunnets vitale interesser. Studien går så på bakgrunn av dette gjennom flere definisjoner og konkretiseringer av kritisk infrastruktur, før den faller ned på fem grunnleggende vitale interesser. Disse danner et utgangspunkt for metoden.

Samfunnets vitale interesser anses å være:

- *Beskytte liv og helse*
  Dette handler om å tilfredsstille viktige behov for befolkningens overlevelse og velstand. Eksempler som blir trukket frem er mat, vann, varme, sanitet og et sted å bo. Å ha et helsevesen, ha evne til verne menneskeliv og beskytte mennesker fra ulykker, terrorangrep, sykdommer og katastrofer, å kunne forhindre spredning av alvorlige smittestoffer, giftige kjemikalier og radioaktive stoffer og ha evne til akuttberedskap for beskyttelse, redning og omsorg.
- *Beskytte miljøet*
  Det trekkes frem at dette må gjøres på både kort og lang sikt. På kort sikt å redusere risikoer for og beskytte seg mot naturkatastrofer, store ulykker, utslipp av miljøskadelige stoffer, forstyrrelser i tekniske systemer, forstyrrelser i økosystemer osv. På lang sikt blir det trukket frem et ikke-påvirket klima, biologisk mangfold og et balansert økosystem. Ren luft, rent vann, levende hav og skog og andre naturmiljø opprettholdes ved å begrense utslipp og lekkasje av forsurende, klimaendrende og forgiftende stoffer samt minimering av utslipp av gjødselsprodukter i naturen.

- *Opprettholde en god samfunnsøkonomi og beskytte økonomiske verdier*
  Dette innebærer å sikre økonomisk vekst og fremme en langsiktig og bærekraftig utvikling, utvikle velferd o.l. Det skal være et fungerende marked med lav arbeidsledighet, og man skal ha fungerende tjenester i økonomien, så som finansvesenet, ha økonomisk sikkerhet, produksjon av viktige varer og tjenester, transport, kommunikasjoner, energiforsyning og ulike typer av teknisk infrastruktur for å opprettholde disse virksomhetene. I et lengre perspektiv spiller utdannelse og forskning en avgjørende rolle.
- *Opprettholde en demokratisk rettsstat*
  Dette handler for en stor del om hvordan grunnleggende verdiene kommer til praktisk uttrykk i samfunnets ulike offentlige funksjoner. Ytringsfrihet, allmenn og lik stemmerett, en representativt og parlamentarisk statsskikk, at offentlig makt skal utøves ved lov, opprettholdelse av rettsikkerhet, likhet for loven, at man har en politisk ledelse og viktige offentlige organer og tjenester som politi, tollvesen og så videre.
- *Bevare fred og nasjonal selvstendighet*
  Inn under dette faller en fungerende utenrikstjeneste, forsvar, politi, redningstjeneste, grensekontroll med mulighet til å virke innenlands og utenlands innenfor rammen av internasjonalt samarbeid.

6.4.4 Kriteriemodell for vurdering av virksomheter betydning for samfunnet – et prosessverktøy

Med listen over samfunnets vitale interesser i bunn, blir det nedfelt et sett med kriterier for å vurdere virksomheters betydning for samfunnet. Valget av kriteriene er produsert blant annet gjennom intervjuer. Kriteriene som er valgt er ulike aspekter av *konsekvenser, tid og årsaker*. Også kriteriene *unicitet* og *avhengighet* er med. *Konsekvenskriterier* kan uttrykkes gjennom utbredelse i tid og rom som virkninger av ulike aspekter for egen eller annen virksomhet for mennesker, miljø og samfunn. De kan også ses på som karakteristika som ligger til grunn for at en situasjon får konsekvenser som plutselighet, gjentagelse og kompleksitet. Ulike tidsaspekter kan med andre ord ses som en del av konsekvenskriteriet. *Tidsaspektet* kan også betraktes som et frittstående tidskriterium som angir hvordan hendelsesmåten på en hendelse – respektive hendelsestidspunktet, påvirker en virksomhet og de konsekvenser som oppstår. *Årsaken* til en hendelse kan ha stor betydning for konsekvensen, for eksempel for hvordan den vurderes og for akseptnivået for en konsekvens. Hvis en virksomhet er *unik* (unicitet) øker vekten i modellen. Her gjelder unicitet både innen egen virksomhet og unicitet opp mot annen virksomhet.

Avhengighetskriteritet angir virksomhetens avhengighet av andre virksomheter, eller annen virksomhets avhengighet av egen. En virksomhet som viktig i seg selv, vil få en betydning hvis annen viktig virksomhet er avhengig av den. Kriteriemodellen kan derfor bistå med å identifisere gjensidige avhengigheter i samfunnet.

Grunnleggende aspekter som beskriver en virksomhet blir bedømt å være *kapasitet, kvalitet* og *hemmelighold*. Dette er aspekter som for enkelte kan variere med situasjonen, men som for andre er uavhengig av situasjon.

Modellen som er utviklet skal danne et grunnlag for vurderinger av den vekt en virksomhet har for samfunnets vitale interesser, og utgår fra følgende kriterier og aspekter hos en virksomhet:

- Den konsekvens som bedømmes oppstår ved et *totalt bortfall* av en virksomhet, respektive *redusert kapasitet*
- Den konsekvens som bedømmes oppstår ved *sviktende kvalitet* – redusert/lav/manipulert
- Den konsekvens som bedømmes oppstår ved *sviktende hemmelighold*
- Virksomhetens *unicitet*
- Virksomhetens *avhengighetsforhold*

Konsekvensen skal ved vurderingen ses på ut fra *intensitet, hvor omfattende og utbredelse*. Intensitet beskriver konsekvensens karakter hva gjelder alvorlighetsgrad.

Konsekvensvurderingen skal også gjøres med hensyn til årsaken og ulike tidsaspekter, da disse kan påvirke den konsekvens som oppstår. De valgte tidskriteriene er som følger:

- Tidspunktet for en forstyrrelse eller bortfall
- Egenskapen til forstyrrelsen eller bortfallet
- Varighet

6.4.5 Arbeidsprosessen – åtte ulike arbeidstrinn

For å sikre at samtlige viktige aspekter blir ivaretatt, og for å få en enhetlig vurdering, tydelighet og sporbarhet, er det lagt opp til en arbeidsprosess i åtte trinn. De åtte arbeidstrinnene er som følger:

Arbeidstrinn 1. Diskusjon rundt grunnleggende verdier og samfunnets vitale interesser
De fem vitale interessene er som tidligere nevnt:

- Beskytte liv og helse
- Beskytte miljøet
- Opprettholde en god samfunnsøkonomi og beskytte økonomiske verdier
- Opprettholde en demokratisk rettsstat
- Bevare fred og nasjonal selvstendighet

Første trinn er å diskutere hvilken eller hvilke av de vitale interessene som virksomheten har betydning for.

Arbeidstrinn 2. Vurdering av konsekvenser ved totalt bortfall av virksomheten med hensyn til tids- og årsakskriterier
Andre trinn skal svare på: Hvilke konsekvenser oppstår ved *bortfall av virksomheten* sett opp mot de fem vitale interessene for samfunnet? Hvordan er disse avhengige av konsekvenser på tids- og årsakskriteriene?

Konsekvensene beskrives i Tabell 6.8 under med kriteriene intensitet, hvor omfattende hendelsen er og utbredelse sett opp mot de fem vitale samfunnsinteressene. Intensitet beskriver

konsekvensene ”alvorlighet som sykdom (ohälsa)”, ”katastrofal” og ”krenkelse”. Hvert av kriteriene konkretiseres med de faktorer som vurderes som viktige for dette. I Tabell 6.9 beskrives de ulike tids- og årsakskriteriene med sine respektive faktorer som varm/kald årstid, plutselig, langsomt. For hvert konsekvenskriterium man går igjennom skal man ta hensyn til den eventuelle betydningen som tid og årsak har for konsekvensen av bortfallet.

Liv og helse			**Miljø**		**Samfunnsøkonomi og økonomiske verdier**		
Intensitet	**Ant. Berørte**	**Geo. Utbre-delse**	**Intensitet**	**Geo. Utbre-delse**	**Kostnad**	**Berørt/ berørte**	**Utbre-delse**
Ingen	Ingen	Ingen	Ingen	Ingen	Ingen	Ingen	Ingen
Sykdom	Få	Lokal	Mindre alvorlig	Lokal	Lav kost-nad	Individ	Lokal
Psyk. skade	Nøkkel-personer	Regional	Alvorlig	Regional	Høy kostnad	Virksomhet	Regional
Fys. skade	Mange	Nasjonal	Katastrofal	Nasjonal	Uover-stigelig	Det offentlige	Nasjonal
Døde		Inter-nasjonal		Inter-nasjonal		Samfunnet	Inter-nasjonal

Demokratisk rettsstat			**Fred og nasjonal selvstendighet**		
Tiltro	**Evne**	**Utbredelse**	**Fred og selvstendighet**	**Handlingsfrihet**	**Utbredelse**
Ingen	Fungerende	Ingen	Upåvirket	Upåvirket	Ingen
Bristende tiltro	Enkelt brister	Lokal	Krenket	Mindre påvirket	Lokal
Mistro	Større brister	Regional	Ikke opprettholdt	Større påvirkng	Regional
	Ikke-funge-rende	Nasjonal		Ikke opp-rettholdt	Nasjonal
		Inter-nasjonal			Inter-nasjonal

Tabell 6.8 FOI - bortfall av virksomhet - konsekvenser

Tidspunktet for en forstyrrelse eller bortfall	**Egenskapen til forstyrrelsen eller bortfallet**	**Varighet på forstyrrelsen eller bortfallet**	**Årsak**
Varm årstid	Plutselig	Ikke-eksisterende	Antagonistisk
Kald årstid	Langsom	Sekunder	Aktør uten hensikt
Dag	Gjentagende	Minutter	Ikke aktør
Natt		Timer	Uavhengig
Hverdag		Dag/dager	
Helligdag		Uke/uker	
Økonomisk viktig tidspunkt		For alltid	
Uberørt av tidspunkt			
Aldri			

Tabell 6.9 FOI - bortfall av virksomhet – tids- og årsakskriterier

Arbeidstrinn 3. Vurdering av konsekvenser ved redusert kapasitet ved virksomheten med hensyn til tids- og årsakskriterier
Det tredje trinnet skal svare på følgende spørsmål: Hvilke konsekvenser oppstår ved *redusert kapasitet* hos virksomheten sett opp mot de fem vitale interessene? Hvordan er disse konsekvensene avhengige av tids- og årsakskriteriene? (Tabellene er identiske med de foregående).

Konsekvensene beskrives – som i arbeidstrinn to, med kriteriene intensitet, hvor omfattende hendelsen er og utbredelse sett opp mot de fem vitale samfunnsinteressene.

Arbeidssteg 4. Vurdering av konsekvenser ved sviktende kvalitet ved virksomheten med hensyn til tids- og årsakskriterier
Det fjerde arbeidstrinnet skal svare på følgende spørsmål: Hvilke konsekvenser oppstår ved *sviktende kvalitet* hos virksomheten sett opp mot de fem vitale interessene? Hvordan er disse konsekvensene avhengige av tids- og årsakskriteriene? (Tabellene er identiske med de foregående).

Arbeidstrinn 5. Vurdering av konsekvenser ved sviktende hemmelighold hos virksomheten
Det femte arbeidstrinnet skal svare på følgende spørsmål: Hvilke konsekvenser oppstår ved s*viktende hemmelighold* hos virksomheten sett opp mot de fem vitale interessene? (Tabellene er identiske med de foregående).

Arbeidstrinn 6. Vurdering av virksomheten med hensyn til unicitet
Det sjette arbeidstrinnet skal svare på følgende spørsmål: Er virksomheten unik? Ved vurderingen skal det ses opp mot de fem vitale samfunnsinteressene.

Utbyttbar med annen virksomhet	**Utbyttbar innen samme virksomhet**
Ikke utbyttbar	Nei
Delvis utbyttbar	Til en viss grad
Utbyttbar	Ja

Tabell 6.10 FOI – unicitet

Arbeidstrinn 7. Vurdering av virksomheten med hensyn til avhengighet
Det syvende arbeidstrinnet skal svare på følgende spørsmål: I hvilket omfang er virksomheten avhengig? Ved vurderingen skal det ses opp mot de fem vitale samfunnsinteressene.

Avhengighet (indirekte påvirkning)
Ingen
Andre virksomheter avhengighet av egen virksomhet
Virksomhetens avhengighet av andre
Gjensidig avhengighet

Tabell 6.11 FOI - hensyn til avhengighet

Arbeidstrinn 8. Sluttvurdering av virksomhetens betydning for de fem vitale samfunnsinteressene

Det åttende arbeidstrinnet skal svare på spørsmålet: Hvilken betydning har virksomheten for samfunnets vitale interesser?

I det siste arbeidstrinnet i modellen skal man sluttføre og samle opp den betydning virksomheten har for samtlige fem vitale interesser for samfunnet. Det siste trinnet bygger på den samlede vurderingen for respektive vitale interesser fra samtlige syv arbeidstrinn. Ved vurderingen arbeider man således med en kolonne om gangen fra de andre arbeidstrinnene. Det er viktig å markere i kolonnene, og gjøre verbale beskrivelser. Vurderingsskalaen er angitt i en skala på fem fra ingen til stor betydning, som vist i Tabell 6.12

Betydning for å beskytte liv og helse	**Betydning for å beskytte miljøet**	**Betydning for å opprettholde god samfunnsøkonomi og beskytte økonomiske verdier**	**Betydning for å opprettholde en demokratisk rettsstat**	**Betydning for å bevare fred og nasjonal selvstendighet**
Ingen betydning	Ingen betydning	Ingen betydning	Ingen betydning	Ingen betydning
Veldig liten betydning	Veldig liten betydning	Veldig liten betydning	Veldig liten betydning	Veldig liten betydning
Liten betydning	Liten betydning	Liten betydning	Liten betydning	Liten betydning
Middels betydning	Middels betydning	Middels betydning	Middels betydning	Middels betydning
Stor betydning	Stor betydning	Stor betydning	Stor betydning	Stor betydning

Tabell 6.12 Sverige – sluttvurdering

6.4.6 Kort vurdering av den svenske metoden

Metoden er ment å identifisere hva som er kritisk infrastruktur. Den er ikke eksplisitt tenkt brukt til å rangere, selv om den muligens kan utvikles til dette formålet også. Det er videre en svakhet at metoden ikke er testet, med unntak av et lite testcase. Metoden har også et omfattende bruksområde ved at den skal gjelde for alt fra samfunnsnivå til enkeltvirksomheter. I hvilken grad dette er en ulempe er ikke kjent, men det er et forhold man må være bevisst på.

Generelt kan det anføres at det må vises forsiktighet med å legge samfunnets grunnleggende verdier til grunn for en operasjonalisering av kritisk infrastruktur. For eksempel kan det være

problematisk å konkretisere hvilken kritisk infrastruktur som understøtter verdiene frihet og demokrati. Det kan hevdes at trusselen mot disse verdiene er av politisk art, og således må møtes med politiske virkemidler, ikke tekniske/organisatoriske virkemidler. Likeledes er verdien en fri og uavhengig presse en grunnleggende samfunnsverdi, men å operasjonalisere verdien til konkrete tekniske og organisatoriske systemer kan by på problemer. Det kan også anføres at trusselen mot enkelte av disse verdiene fremstår som usannsynlige per i dag.

Slike motforestillinger betyr ikke nødvendigvis at det ikke er fruktbart å legge samfunnets grunnleggende verdier i bunn for en analyse. Det kan tvert i mot hevdes at samfunnets grunnleggende verdier er fundamentet for alle vurderinger av hva som er kritisk for samfunnet. Men det må utvises varsomhet, og man må være bevisst begrensningene med fremgangsmåten. I den svenske metoden er dette forsøkt imøtegått ved å konkretisere og presisere verdiene ned til det de kaller samfunnets vitale interesser.

KBM arbeider med oppfølging av FOIs forslag til metode innenfor rammen av deres prosjekt om gjensidige avhengigheter.

6.5 Canada

6.5.1 Utvalgskriterier for å identifisere og rangere kritisk infrastruktur

Canada har utgitt ett sett med kriterier, med forventning om at eiere av infrastruktur, operatører og interessenter skal bidra til en videreutvikling av disse kriteriene for identifisering og rangering av kritisk infrastruktur.[71] Kriteriene tar utgangspunkt i det canadiske sikkerhetsdepartementets (PSEPC) ti identifiserte sektorer med kritisk infrastruktur.[72] Kriteriene må ikke anses som ferdig utviklet. Det vil i det følgende bli redegjort for utvalgskriteriene.

I den canadiske tilnærmingen deles kritisk infrastruktur opp i *systems*, *assets* og *network elements* som vil få innvirkning på nasjonalt nivå hvis de blir utilgjengelig i en krise. På norsk kan dette oversettes til systemer, realøkonomisk ressurs og nettverkselementer. Det blir også referert til *service. Service* viser til en kritisk tjenesteleveranse. Bruken av begrepet *Assets*, eller en ressurs, er sentral i forhold til identifisering og rangering av kritisk infrastruktur. Ressursene kan bestå av en enkelt del i et teknisk system, for eksempel en enkel turbin, eller et enkelt element i en sektor, for eksempel en dam eller en kraftstasjon. Begrepet beveger seg dermed mellom forskjellige nivåer.

Kriteriene går inn som det første ledd av fire i en risikostyringsprosess. Denne prosessen består av

1. Identifisering og rangering av (realøkonomiske) ressurser (Identification of Assets)
2. Risikoanalyse (Risk Analysis)
3. Risikokontroll (Risk Control)
4. Vedlikehold og utholdenhet (Sustainability)

[71] Public Safety and Emergency Preparedness Canada. 2004, *National Critical Infrastructure Assurance Program. Selection Criteria to Identify and Rank Critical Infrastructure Assets*. 20 January 2004
[72] Omtalt tidligere i dette dokumentet.

Det vil i det følgende blir redegjort for det første leddet av denne prosessen.

Det er identifisert fem skritt for å identifisere og rangere kritiske ressurser:

1. Karakterisere eller standardisere ressurser
2. Etablere kritikalitet
3. Vurdere hvilken innvirkning tap av en ressurs får, sett opp mot
    a. Konsentrasjon av mennesker og elementer
    b. Økonomi
    c. Kritisk infrastruktur sektor
    d. Gjensidig avhengighet
    e. Tjenesteleveranser
    f. Publikums tillit
4. Vurdering av hvilken konsekvens tap av en ressurs får sett opp mot
    a. Konsentrasjon av mennesker og elementer
    b. Økonomi
    c. Kritisk infrastruktur sektor
    d. Gjensidig avhengighet
    e. Tjenesteleveranser
    f. Publikums tillit
5. Benytte et regelsett for å rangere ressursene

Punktene 3. a-f og 4. a-f fremstår i den canadiske tilnærmingen som kriterier for identifisering og rangering. De fem skrittene med tilhørende kriterier vil i det følgende blir gjengitt:

Karakterisere eller standardisere ressurser

For å utvikle en oversikt over kritiske (realøkonomiske) ressurser, er en standardisering av ulike ressurser vurdert som vesentlig. Et team burde benyttes for å identifisere og klassifisere ressurser på ulike nivåer. Eksempelvis er en enkeltstående turbin på ett nivå, en kraftstasjon på et annet mens kraftsektoren kan sies å utgjøre et tredje nivå. Graden av detalj vil variere fra sektor til sektor, og er avhengig av om ressursen påvirker operatøren og befolkningen på lokalt, regionalt eller nasjonalt nivå. Ved utvikling av oversikter over realøkonomiske ressurser, må de stadfestes av de eiere og operatører som drifter infrastrukturen.

Etablere kritikalitet

Metoden viser til erfaring som tilsier at det er relativt ukomplisert å identifisere kritiske ressurser. Utfordringene er knyttet til å etablere hvor kritisk en ressurs er i forhold til andre, og å tallfeste i presise termer den potensielle innvirkningen tap eller delvis ødeleggelse har, eksempelvis i kroner og øre. Unntaket er presisering i enkle skalaer som lav, medium og høy. Det blir hevdet at enkle skalaer gir en nøyaktighet som er god nok for å identifisere og prioritere de mest kritiske av de realøkonomiske ressursene.

Vellykkede modeller må finne en balanse mellom enkelthet og relevans (validitet) og de må være

konstruert for å vurdere kritikaliteten til de forskjellige ressursene. De første resultatene må heller ikke vurderes som endelige, men må justeres underveis i prosessen eller ved en evaluering i etterkant.

Vurdering av hvilken innvirkning tap av et element får – påvirkningsfaktorer

Påvirkningsfaktorer er kriterier for å prioritere kritiske ressurser. Tapet av kritiske ressurser eller tjenester blir i den canadiske tilnærmingen foreslått til å bli vurdert opp mot seks *påvirkningsfaktorer*. En samlet vurdering av påvirkningsfaktorene og konsekvenser kan bli brukt for å fastslå kritisk infrastruktur og deres relative rangering seg i mellom. Påvirkningsfaktorene blir analysert ut fra omfanget, størrelsen, tid på året og effekter av tid. Faktorene er også skalerbare ved at de kan bli anvendt og bygget opp på grunnlag av en virksomhet (v), en enkelt sektor (s), sektorovergripende (so) og på myndighetsnivå (m). De er:

1. Konsentrasjon av mennesker og ressurser:
   Fokus er på hva tap av en ressurs eller en tjeneste kan medføre av dødsfall, hardt skadde eller antall evakuerte. Jo høyere konsentrasjon av personer, jo større potensial for katastrofale følger (v).
2. Økonomi:
   Har fokus på økonomiske konsekvenser ved tap av en ressurs eller tjeneste (v).
3. Kritisk infrastruktur sektor:
   Ser på hvordan tap av en ressurs eller tjeneste har av innvirkning på en kritisk infrastruktur sektor. Kritisk infrastruktur sektor kan bli definert ut fra det kanadiske sikkerhetsdepartementets (PSEPC) ti identifiserte sektorer med kritisk infrastruktur (s).[73]
4. Gjensidig avhengighet:
   Hensikten er å se på kaskadeeffekter ved tap av en realøkonomisk ressurs eller tjeneste opp mot andre kritiske sektorer eller tjenester. Gjensidige avhengigheter inkluderer forhold som fysiske, geografiske og logiske (so).
5. Tjenesteleveranser:
   Ser på konsekvenser av tap av en ressurs eller tjeneste for samfunnets generelle økonomi (so).
6. Publikums tillit:
   Kriteriet måler hvordan tap av en ressurs eller tjeneste påvirker publikums tillit, alt fra jobbsikkerhet og tillit til kunderelasjoner i en virksomhet til myndighetenes evne til å sikre helsetjenester, økonomisk sikkerhet og andre basale tjenester (m).

Vurdering av hvilken konsekvens tap av et element får – konsekvenskriterier

Den andre hovedbolken av kriterier i den canadiske tilnærmingen – *konsekvenskriterier* – er laget for å bli fremlagt for sektorspesifikke eksperter og grupper med eksperter, slik at disse kan utvikle og komme med tilleggsinformasjon om konsekvensene knyttet til hvert av konsekvenskriteriene.

[73] (1) Energy and Utilities, (2) Communications and Information Technology, (3) Finance, (4) Health Care, (5) Food, (6) Water, (7) Transportation, (8) Safety, (9) Government, (10) Manufacturing. Disse sektorene er delt i undersektorer. For eksempel består sektoren (1) Communications and Information Technology av (a) Telekommunikasjon [telefon, faks, kabel og satellitt], (b) kringkastningssystemer, (c) programvare, (d) maskinvare og (e) nettverk [internett].

Brukere skal ved denne tilnærmingen bruke følgende spørsmål, og forbedre dem til eget behov.

1. Konsentrasjon av mennesker og ressurser:
   a. Kan bortfall av denne ressursen resultere i dødsfall, hardt skadde eller evakuering av personer?
   b. Hvor mange personer vil bli berørt (dødsfall, skade, evakuering) ved bortfall eller degradering av tjenester knyttet til bortfallet av ressursen?
   c. Hva er konsentrasjonen av andre elementer som er samlokalisert med den kritiske ressursen?
2. Økonomi:
   a. Hvilken potensiell økonomisk innvirkning får det for virksomheten ved tap eller degradering av tjenester som det er sannsynlig vil oppstå ved tap av ressursen?
   b. Hva koster den direkte skaden på elementet/hva koster det å gjenopprette ressursen?
   c. I hvilken grad er kritisk informasjon og kritiske systemer kompromittert?
   d. Er grad av økonomisk innvirkning avhengig av sesong?
3. Kritisk infrastruktur sektor:
   a. Er ressursen en del av den kritiske infrastrukturen slik den er definert av canadiske myndigheter i NCIAP?[74]
   b. Er innvirkningen av tapet eller degraderingen av tjenesten/ ressursen av lokal, provinsiell, regional, nasjonal eller internasjonal karakter?
4. Gjensidig avhengighet:
   a. Er ressurser innenfor sektoren avhengig av denne ressursen?
   b. Er ressurser utenfor sektoren avhengig av denne ressursen?
   c. List kjente ressurser eller tjenester som er innenfor eller utenfor ressursens egen sektor som er avhengig av denne ressursen.
   d. Hvordan er andre infrastruktursektorer avhengig av ressursen eller tjenesten?
   e. Hvordan er denne ressursen avhengig av tjenester eller ressurser i andre sektorer?
   f. Eiere av infrastrukturressurser som har erfaring med naturkatastrofer har vanligvis bedre forståelse for gjensidige avhengigheter, og har større sannsynlighet for å ha utarbeidet kriseplaner. Hvilken informasjon og planer eksisterer med hensyn til denne ressursen.
5. Tjenesteleveranser:
   a. Er innvirkningen på samfunnsøkonomien en umiddelbar, rask eller forsinket?
   b. Hvor stor vil innvirkningen av tapet av denne ressursen være, når man tar hensyn til tap eller degradering av tjenester som er knyttet til å miste denne ressursen?
   c. Hvor lang tid vil det ta å tilbakeføre tjenesten eller erstatte ressursen?
   d. Hvilke erstatninger eller alternativer er tilgjengelige?
   e. Er innvirkning på tjenesteleveransen variabel med hensyn til årstid?
   f. Sett på bakgrunn av de andre spørsmålene, så som tilgjengelighet til erstatninger, er den potensielle innvirkningen av lokal, provinsiell, regional, nasjonal eller internasjonal art?

[74] NCIAP står for *National Critical Infrastructure Assurance Program*. Det blir henvist til ti sektorer med undersektorer som dette organet har definert som kritisk infrastruktur i Canada.

6. Publikums tillit:
    a. Kan tap av denne ressursen resultere i dødsfall, hardt skadde eller forflytning av personer?
    b. Kan tap av denne ressursen resultere i lav moral, tap av nasjonal prestisje, panikk, opptøyer eller uro?
    c. Vil tapet av ressursen ha en økologisk innvirkning ved at den endrer miljøet?
    d. Hvilken innvirkning på publikums tiltro (eksempelvis evne til å forsvare nasjonal suverenitet/territoriell integritet) kan tap av denne ressursen ha, enten direkte eller gjennom relatert degradering av tjenesten?
    e. Har ressursen eller tjenesten en symbolsk betydning?
    f. Vil tap av ressursen i betraktelig grad redusere myndighetenes evne og sentrale tjenesteleverandørers evne til å levere basale tjenester rettet mot å fremme offentlig velferd?

Benytte et regelsett for å rangere elementene

En innledende skala for å kategorisere innvirkning vil være kvalitativ. Den vil ta i bruk termer som lav, middel og høy, eller bruk av tall eksempelvis mellom 0 og 15. Estimatene kan videre bli foredlet ved å la eksperter undersøke spesifikke innvirkningsfaktorer, for eksempel potensiell innvirkning på personer, miljø, tiltro til myndighetene og så videre, enten gjennom modeller eller en metode som på engelsk blir omtalt som *Business Impact Assessment studies.*

Å tilegne numeriske verdier på individuelle påvirkningsfaktorer og eller konsekvenskriterier burde unngås. Det kan gi inntrykk av en matematisk validitet som ikke er tilstede. En bedre tilnærming er å utvikle et regelsett hvor vurderingen er basert på at spesifikke forutsetninger blir innfridd.

En vurdering av prioritering av kritisk infrastruktur kan brukes som foreslått i modellen i Tabell 6.13. Det er et regelsett, basert på konsekvenskriteriene med en skala fra lav, medium, høy og ekstra høy. Hvis det ikke blir vurdert noen kritikalitet blir den satt til 0.

Prioritering av kritisk infrastruktur skjema - konsekvenskriterier				
Påvirkningsfaktorer	**Meget høy**	**Høy**	**Medium**	**Lav**
Poengsum	15	5	3	1
Konsentrasjon av mennesker og ressurser (potensialet for katastrofale effekter)	Mer enn 10,000 personer	Mellom 1,000 og 10,000 personer	Mellom 100 og 1000 personer	Mindre enn 100 personer
Økonomisk innvirkning / Direkte kostnad med rekonstruksjon inkludert kostnadene knyttet til rekonstruksjon av kritisk informasjon og informasjonsteknologi (tjenesten er avhengig av eller innholder kritisk informasjon og IT.)	Direkte ødeleggelse og restaurering > $1 mrd	Direkte ødeleggelse og restaurering mellom $100 mill til $1 mrd	Direkte ødeleggelse og restaurering mellom $10 mill til $100 mill	Direkte ødeleggelse og restaurering under $10 mill
Kritisk infrastruktur sektor innvirkning (Tjenesten eller ressursen er relatert til en kritisk infrastruktur sektor)	Hele sektoren kan bryte sammen – internasjonale konsekvenser	Nasjonal	Provinsiell/ regional	Lokal
Gjensidig avhengighet innvirkning	Sterkt svekkende innvirkning på andre sektorer	Betydelig innvirkning eller sammenbrudd av andre sektorer	Moderat innvirkning på viktige oppgaver til andre sektorer	Liten innvirkning på viktige oppgaver til andre sektorer
Innvirkning på tjenesteleveranser – potensialet for umiddelbar og betydningsfull innvirkning	Høy tverrsektoriell kostnad, gjenoppbyggingstid er lenger enn ett år	Høy kostnad, lang gjenoppbyggingstid (måneder – år)	Medium kostnad, betydelig gjenoppbyggingstid (dager – uker)	Lave kostnader, kort gjenoppbyggingstid (timer – dager)
Innvirkning på publikums tillit	Høy nasjonal risiko og tvil om myndighetenes evne til å kontrollere	Publikum oppfatter høy nasjonal risiko og lav evne til å håndtere risikoen	Publikum oppfatter moderat risiko og moderat evne til å kontrollere risiko	Publikum oppfatter lav risiko og høy evne til å kontrollere risiko
Totalt poeng: **Noter:** **En fortegnelse over ressurser og/eller tjenester er helt nødvendig for å danne et komplett bilde og fullverdig dokumentasjon** **Hvis en ressurs ikke er kritisk ved at den har ubetydelige konsekvenser, skal poenget bli satt til 0.** **Denne vurderingen kan bli foredlet ved å benytte kvantitative poeng (eksempelvis 0 til 15)** **Estimatene kan bli videre foredlet ved å la eksperter undersøke andre variable så som potensiell innvirkning på personer, miljø, tillit til regjeringen eller gjennom andre modeller eller gjennom det som på engelsk er omtalt som Business Impact Assessment studies.**				

Tabell 6.13 Canada - prioritering av kritisk infrastruktur skjema – konsekvenskriterier

For å finne en rangering kan skjemaet i Tabell 6.14 benyttes:

Ressursliste	**Påvirkingsfaktorer**						**Poengsum**
	Konsentrasjon av mennesker og ressurser	Økonomi	Kritisk infrastruktur sektor	Gjensidig avhengighet	Tjeneste-leveranser	Publikums tillit	

Tabell 6.14 Canada – rangering

6.5.2 En annen tilnærming – innvirkningskategorier og innvirkningsfaktorer

I en tidligere utgave av den canadiske tilnærmingen fra desember 2002, er kriteriene etablert ut fra to forhold. For det første ut fra innvirknings*kategorier*, og for det andre ut fra innvirknings*faktorer*. Innvirkningskategoriene består av ett sett med kriterier, mens innvirkningsfaktorene består av elementer som påvirker kriteriene. For eksempel kan en innvirkningskategori være økonomi, mens en innvirkningsfaktor kan være hvilke konsekvenser tap av en ressurs får for økonomien i forhold til geografisk omfang, hvilken størrelse hendelsen har, varighet etc. Det er meningen at metoden skal danne et grunnlag for nasjonale og regionale myndigheter i Canada for å identifisere kritisk infrastruktur. Videre skal den være et referansedokument for andre eiere av kritisk infrastruktur i utviklingen av egne utvelgelseskriterier for egen kritiske infrastruktur. Det er også meningen at metoden skal danne grunnlag for partnerne i det såkalte NCIAP[75] Partnership i utviklingen av utvelgelseskriterier for nasjonal kritisk infrastruktur.

Ved bruk av metoden er det viktig å være seg bevisst på hvilket nivå metoden skal anvendes, og at man er konsekvent på dette. For eksempel ved vurdering av et lands vannkraftinfrastruktur vil en vannkraftstasjon og dam ligge på et annet nivå enn en turbin.

Innvirkningskategorier (kriterier)

Disse brukes til å gi en vurdering av innvirkningen av tapet av en potensielt kritisk ressurs i forhold til følgende innvirkningskategorier.

- Innvirkning på tjenesteleveransen
  Dette kriteriet er en kvalitativ måling av hvilken innvirkning ødeleggelse eller et midlertidig bortfall av en ressurs eller element i en sektor har i forhold til tap eller forringelse av tjenesteleveransen.
- Innvirkning på publikum
  Kriteriet tilrettelegger for å måle innvirkningen av forringet tjenesteleveranser sett opp mot den fysiske velværen til befolkningen. Det er en vurdering av mulige dødsfall, hardt skadde eller antall evakuerte personer som resultat av bortfallet. Inkluderer ikke personer som får mindre ubehag som resultatet av bortfall

[75] NCIAP står for *National Critical Infrastructure Assurance Program* i Canada

- Økonomisk innvirkning
  Kriteriet måler den potensielle økonomiske påvirkningen som kommer av dårligere tjeneste på grunn av tap av en kritisk infrastrukturressurs. Det er en vurdering av mulig økonomisk påvirkning på befolkningen, selskaper eller myndighetene i kvalitative termer.
- Politisk innvirkning
  Kriteriet måler den potensielle innvirkningen på myndighetenes evne til å fortsette å fungere og publikums tiltro til myndighetenes evne til å håndtere tap som følge av bortfall av en tjeneste eller ressurs. Det er en vurdering av mulig innvirkning på publikums tiltro til myndighetenes evne til å vedlikeholde helsetjenester, økonomisk sikkerhet eller til å skaffe til veie vesentlige tjenester.
- Innvirkning på miljøet
  Gir et mål på potensiell innvirkning på miljøet ved tap av en kritisk ressurs.
- Innvirkning på gjensidig avhengighet
  Et mål på innvirkningen av tap eller degradering av en tjenesteleveranse på en sektor og dens påvirkning på andre sektorer. Kriteriet gir en vurdering av mulige gjensidige avhengigheter som andre tjenester eller funksjoner har på egen sektor.

Innvirkningsfaktorer

Elementene som er gjenstad for analyse blir vurdert ut fra innvirkningskategoriene (kriterier) ovenfor, ut fra følgende faktorer: rekkevidde, størrelse og effekter av tid.

- Rekkevidde
  - Lokal
    Lokal innvirkning er definert til å påvirke det lokale nivået. Det gjelder for forhold som innvirker de lokale styringsorganer og/eller det lokale/kommunale geografiske området. Hendelser som får innvirkning på flere lokale områder/kommuner faller også inn i denne kategorien så fremt det ikke går over de regionale grensene.
  - Regional
    Gjelder hendelser som får regionale innvirkninger. Innvirkningsområde kan gå over flere regionale områder, men får ikke nasjonale konsekvenser.
  - Nasjonal
    Har innvirkning på nasjonalt nivå. Tap av en ressurs som får internasjonale effekter defineres også inn i denne kategorien.
- Størrelse
  Denne faktoren er avhengig av at man er i stand til å benytte sektorspesifikke mål fordi et felles mål (eksempelvis økonomi) ikke lar seg benytte på tvers av alle sektorer på en konsistent måte.
  - Ingen (Business as usual)
  - Minimal
  - Moderat
  - Stor
- Effekter av tid
  Tid kan påvirke tapet av en ressurs sett opp mot både omfang og rekkevidde

Effekter av tid kan måles ut fra hvilket punkt tapet av en ressurs kan få en nasjonal betydning.

- Ikke relevant
- Umiddelbar (Definert som innenfor noen få timer fra hendelsen)
- 24-48 timer
- En uke
- Annet
  Kan brukes som en kategori for å spesifisere en tidslinje som ikke korresponderer med den gitt tidslinjen.

Bruk av metoden i praksis – spørreskjema

Kriteriene er ment brukt til å identifisere kritiske infrastrukturelementer. Det er utarbeidet en liste over de ulike ressursene og elementene som undersøkes. Med utgangspunkt i den første av disse ressursene, innvirkning på tjenestesektoren, vises hvordan hvert av elementene blir analysert ut fra følgende tre faktorer: størrelse, rekkevidde og effekter av tid.

Ved bruk av et slikt spørreskjema, må respondenten svare innenfor rammen av et scenario, for eksempel et *worst case*-scenario.

1. Innvirkning på tjenesteleveranse

A. Hva er innvirkningen av tapet av denne ressursen/elementet på leveransen eller nivået på akkurat denne tjenesten/produkt innenfor sektoren?

Størrelse: *Ingen* *Minimal* *Moderat* *Stor*
Rekkevidde: *Lokal* *Regional* *Nasjonal*

B. På hvilket tidspunkt vil tapet av denne ressursen få innvirkning på tjenesteleveranser av nasjonal betydning?

Effekt av tid: *Umiddelbar* *24-48t* *En uke* *Ikke gyldig* *Annet*

2. Innvirkning på publikum

A. Kan tapet av denne ressursen resultere i dødsfall, alvorlig skade eller evakuering av personer?
B. Kan tapet av denne ressursen resultere i lav moral, panikk, opprør, politisk uro?
C. På hvilket tidspunkt vil tapet av ressursen få en innvirkning på publikum nasjonalt?

3. Økonomisk innvirkning

A. Hva vil den økonomiske innvirkningen være som resultat av tap eller degradering?
B. På hvilket tidspunkt vil tapet av denne ressursen få en økonomisk innvirkning nasjonalt?

4. Politisk innvirkning

A. Hvilken innvirkning på publikums tiltro til myndighetene får tapet av ressursen, enten direkte eller indirekte gjennom relaterte tjenesters bortfall eller tap?
B. Vil tapet av ressursen signifikant redusere myndighetenes evne til å levere basale myndighetstjenester rettet mot å bevare publikums helse og sikkerhet, økonomisk sikkerhet eller til å gi vesentlige tjenester?
C. På hvilket tidspunkt vil tapet av denne ressursen få en politisk betydning nasjonalt?

5. Innvirkning på miljøet

A. Hvilken innvirkning på miljøet kan tapet eller degraderingen av tjenesten få?
B. Hva vil bli berørt ved tap eller degradering av tjenesten eller ressursen?
C. På hvilket tidspunkt kan tapet av ressursen få en miljømessig nasjonal betydning?

6. Innvirkning på gjensidig avhengighet

A. Er ressurser/elementer innenfor sektoren avhengig av denne ressursen?
B. Er ressurser/elementer utenfor sektoren avhengig av denne ressursen?
C. På hvilket tidspunkt vil tapet av ressursen ha en innvirkning på gjensidig avhengighet på et nasjonalt nivå?
Viktig: Inkluder en liste over kjente ressurser/elementer innenfor og eksterne til elementets sektor som er avhengig av denne ressursen.

Basert på dette kan det settes opp følgende oversikt, se Tabell 6.15:

RESSURSNAVN:	**Innvirkningsvurdering**		
SEKTOR:			
Innvirkningskategorier	**Størrelse**	**Rekkevidde**	**Effekt av tid**
1) Innvirkning på tjenesteleveranse			
a) Hva er innvirkningen av tapet av denne ressursen/elementet på leveransen eller nivået på akkurat denne tjenesten/produkt innenfor sektoren?			
2) Innvirkning på publikum			
a) Kan tapet av denne ressursen resultere i dødsfall, alvorlig skade eller evakuering av personer?			
b) Kan tapet av denne ressursen resultere i lav moral, panikk, opprør, politisk uro?			
3) Økonomisk innvirkning			
c) Hva vil den økonomiske innvirkningen være som resultat av tap eller degradering?			
4) Politisk innvirkning			
a) Hvilken innvirkning på publikums tiltro til myndighetene får tapet av ressursen, enten direkte eller indirekte gjennom relaterte tjenesters bortfall eller tap?			
b) Vil tapet av ressursen signifikant redusere myndighetenes evne til å levere basale myndighetstjenester rettet mot å bevare publikums helse og sikkerhet, økonomisk sikkerhet eller til å gi vesentlige tjenester?			
5) Innvirkning på miljøet			
a) Hvilken innvirkning på miljøet kan tapet eller degraderingen av tjenesten få?			
b) Hva vil bli berørt ved tap eller degradering av tjenesten eller ressursen?			
6) Innvirkning på gjensidig avhengighet			
a) Er ressurser/elementer innenfor sektoren avhengig av denne ressursen?			
b) Er ressurser/elementer utenfor sektoren avhengig av denne ressursen?			

Tabell 6.15 Canada – innvirkningsanalyse

6.5.3 Kort vurdering av de to canadiske tilnærmingene

En generell betrakting er at det til tider er vanskelig å følge resonnementene. Begrepsbruken er heller ikke alltid konsekvent. Det er også et tankekors at den første versjonen av den canadiske tilnærmingen fra desember 2002 fremstår som mer gjennomarbeidet enn den andre fra januar 2004. Årsaken til dette er ikke kjent. Likevel fremstår de som viktige bidrag til utarbeidelsen av en norsk metode, særlig med tanke på kriteriene som er valgt.

Det foreligger ikke noen eksempler på bruk av metoden i tilgjengelig litteratur. Det kan skyldes flere forhold, men en hovedårsak kan være at en kartlegging slik det er lagt opp til her, vil avdekke sårbarheter som man ønsker å holde for seg selv. Samtidig gjør dette det vanskelig å se hvor fruktbar metoden er for norske forhold.

6.6 CIP i Nederland

Nederlandske myndigheter la i 2002 opp til en plan i fire faser for å sikre landets kritiske infrastruktur.

Fase én var å få oversikt over kritisk infrastruktur, gjensidige avhengigheter og en foreløpig vurdering av potensielt skadeomfang ved sammenbrudd. Infrastruktur ble i fase én definert som kritisk hvis sammenbrudd eller alvorlige avbrudd fører til skade på et nasjonalt nivå. Det ble også lagt opp til en underdeling av definisjonen, for eksempel skade som resultat av avbrudd i en sektor av økonomisk art, tap av menneskeliv og miljøskade. Fase én gikk under navnet *Quick Scan* og ble presentert på engelsk i april 2003.

Fase to ble bestemt å ha fokus på eksisterende planverk og beskyttelsestiltak allerede på plass. Spesiell oppmerksomhet skulle rettes mot terrorisme, men også naturkatastrofer, utilsiktede skadelige menneskelige handlinger og teknisk svikt skulle omtales. Rammen rundt er store hendelser.

Fase tre ble bestemt å involvere en diskusjon om hvorvidt funksjonsdyktigheten til kritisk infrastruktur er god nok og om den kan bedres. Det ble vist til at eventuelle tiltak i denne sammenheng er justering av lovgivning, økt tilsyn, målrettede investeringer i kritisk infrastruktur, bedret objektsikkerhet, bedret sikkerhet ved endringer i organisasjon og informasjonssikkerhet, tiltak for å oppnå bedre personlig beskyttelse og opprettelse av alternative ordninger.

Den *fjerde* og siste fasen ble bestemt å være innføring av tiltak. Det er ikke kjent i hvilken grad de forskjellige fasene er gjennomført. Unntaket er fase én som blir presentert her. Det er også den som er av særlig interesse for å utvikle en norsk metode for å identifisere og rangere kritiske samfunnsfunksjoner og infrastruktur.

6.6.1 Quick Scan

I april 2003 utga det nederlandske *Ministry of Interior and Kingdom Relations* ut et dokument med resultater fra det såkalte *Quick Scan*-prosjektet.[76] Hensikten med *Quick Scan* var å identifisere kritisk infrastruktur i Nederland og kartlegge gjensidige avhengigheter. *Quick Scan* var et samarbeid mellom myndigheter og privat næringsliv. Ved å bruke eksperter fra myndigheter og det private næringsliv kom nederlandske myndigheter frem til et bilde over hvilke sektorer, produkter og tjenester som inngår i Nederlands kritiske infrastruktur.

[76] Ministry of the Interior and Kingdom Relations 2003. *Critical Infrastructure Protection in the Netherlands.* April 2003.

Hovedkonklusjonene fra *Quick Scan* var:

- Nederlands kritiske infrastruktur består av 11 sektorer og 31 produkter og tjenester
- *Quick Scan* har gitt myndighetene og industrien en klar forståelse av gjensidige avhengigheter. Kritiske forretningsprosesser har vist seg langt mer avhengig av hverandre enn det tidligere var forståelse for i sektorene
- Avbrudd, svikt eller sammenbrudd i et vitalt produkt eller tjeneste kan generere kaskadeeffekter som har vesentlig påvirkning på det nederlandske samfunnet og på naboland, dersom beskyttelsestiltak ikke iverksettes
- De ansvarlige for kritiske forretningsprosesser har en begrenset forståelse av gjensidige avhengigheter og omfanget av avhengighetene. Å beskytte tilgjengelighet og integritet kan bare bli gjort ved å ta hensyn til hele verdikjeden. Dette er så langt ikke sikret på en tilfredsstillende måte.
- For å forhindre og forberede seg på eventuelle katastrofer, er det essensielt å se forskjeller i karakteristika i sammenbrudd og gjenoppretting av produkter og tjenester som er del av en større kjede. *Quick Scan* har laget en oversikt over dem.

For å komme frem til en oversikt over kritisk infrastruktur, ble det først utviklet et spørreskjema som ble sendt til forskjellige myndigheter og virksomheter. Hensikten var å få en første oversikt. Etter en analyse utført av *Netherlands Organisation for Applied Scientific Research* (TNO), ble resultatene presentert i et bredt anlagt arbeidsseminar. Dette dannet grunnlag for videre arbeid i 17 nye arbeidsgrupper hvor det ble utarbeidet en ytterligere spesifisering. I tillegg ble det arrangert et møte med nasjonale eksperter på risiko- og skadevurderinger. Her ble et estimat av potensiell skade gitt ut fra kriteriene antall døde mennesker og dyr, økonomiske konsekvenser, miljømessige konsekvenser og sosiologiske/psykologiske effekter.

6.6.2 Kritiske sektorer, produkter og tjenester

11 sektorer og 31 produkter og tjenester ble utpekt. De ble ansett som kritiske fordi:

- de utgjør essensielle, uunnværlige fasiliteter for samfunnet. Avbrudd vil raskt resultere i en nasjonal krise.
- sammenbrudd eller avbrudd kan ha skadelige sosiale effekter på lang sikt
- de utgjør uunnværlige redskaper for å garantere opprettholdelsen av en normal situasjon eller for å kontrollere en krise, eksempelvis politi, brann og forsvar.

Tabell 6.16 ble sluttproduktet:

No.	Sector	Product or service
1	**Energy**	Electricity
2		Natural gas
3		Oil
4	**Telecommunications**	Fixed telecommunication networks services
5		Mobile telecommunication services
6		Radio communication and navigation
7		Satellite communication
8		Broadcast services
9		Internet access
10		Postal and courier services
11	**Drinking water**	Drinking water supply
12	**Food**	Food supply and food safety
13	**Health**	Health care
14	**Financial**	Financial services and financial infrastructure (private)
15		Financial transfer services (government)
16	**Retaining and managing surface water**	Management of water quality
17		Retaining and managing water quantity
18	**Public Order and Safety**	Maintaining public order
19		Maintaining public safety
20	**Legal order**	Administration of justice and detention
21		Law enforcement
22	**Public administration**	Diplomacy
23		Information provision by the government
24		Armed Forces / Defence
25		Public administration
26	**Transport**	Road transport
27		Rail transport
28		Air transport
29		Inland navigation
30		Ocean shipping
31		Pipelines

Tabell 6.16 Nederland Quick Scan I

Det ble også gjort en rangering, i form av en tabell hvor kritiske produkter og tjenester ble samlet og arrangert med hensyn til hvor stor skade et avbrudd eller sammenbrudd vil få, se Tabell 6.17. Det er ikke kjent hvordan rangeringen foregikk utover at det ble brukt en egen ekspertgruppe.

	Product or service
1	Electricity
2	Water quantity
3	Drinking water supply
4	Maintaining public safety Food supply Health care
5	Fixed telecommunication networks services Mobile communication services Maintaining public order Road traffic Satellite communication Radio communication & navigation Oil Administration of justice and detention Law enforcement Rail traffic
6	Natural gas
7	*Other products and services*

Tabell 6.17 Nederland Quick Scan II

Av interesse er at elektrisitet og vann blir rangert på topp. Legg også merke til at enkelte produkter og tjenester er rangert lavt, fordi det er blitt vurdert at de i utgangspunktet egentlig bare er kritiske i en krisesituasjon. Dette gjelder i følge dokumentet særlig politi og forsvar.

Dokumentet som omhandler resultatene av *Quick Scan* presenterer videre omfattende matriser og figurer for å illustrere gjensidige avhengigheter. Disse er kun omtalt i korte trekk i dokumentet. Av spesiell interesse i denne sammenheng er at figurene illustrerer at de mest kritiske sektorene er særlig avhengig av elektrisitet, telekommunikasjonstjenester og veitransport. Videre at elektrisitet og veitransport bare i begrenset grad er avhengige av andre kritiske sektorer. De viser også at luftkontroll og administrering av justissektoren er meget avhengige av andre kritiske sektorer. Det kommer også frem at svært mange sektorer undervurderer avhengigheten av GPS. I dokumentet blir GPS beskrevet som sårbart.

6.6.3 Vurdering av Quick Scan

Som med mye annen litteratur er fokus satt på hva som er kritiske sektorer, ikke metoden for å fremskaffe en slik oversikt. Listen i seg selv er interessant, og forteller hvilke prioriteringer som blir gjort i Nederland. For formålet med BAS5-prosjektet er det imidlertid ikke tilstrekkelig. I utarbeidelsen av *Quick Scan* har det vært omfattende bruk av arbeids- og ekspertgrupper. Arbeids- og ekspertgrupper er en nødvendig del av å identifisere og rangere kritisk infrastruktur, men så lenge det ikke er dokumentert hva disse gruppene har gjort, er det vanskelig å vurdere godheten av resultatene. I den grad det finnes en slik dokumentasjon, har det ikke lykkes å få tak i denne ved internettsøk. Det er også naturlig å anta at bakgrunnsdokumentasjonen er skrevet på nederlandsk, og at det kun er sluttproduktet som er produsert på engelsk.

Av interessante kriterier som fremkommer i teksten, er kriteriene som er lagt til grunn for å vurdere potensiell skade. De er følgende:

- Antall døde mennesker og dyr
- Økonomiske konsekvenser
- Miljømessige konsekvenser
- Sosiologiske/psykologiske effekter

Annet av interesse som kan bidra til et kriterieutvalg er at:

- ekstra oppmerksomhet må rettes mot de som i stor grad bidrar til andre kritiske sektorer
- bortfall av enkelte produkter og tjenester vil raskt skape nasjonal krise, mens andre får store konsekvenser på litt lengre sikt
- enkelte tjenester og produkter er kritiske for å opprettholde en normalsituasjon og/eller for å kontrollere kriser; eksempelvis, politi, brann, forsvar.

CIP i Nederland har arbeidet videre med relevante spørsmål. Dette arbeidet er ikke tatt med fordi det ikke er like relevant med hensyn til å utvikle en metode for å identifisere og rangere kritisk infrastruktur. For mer informasjon, se *Critical Infrastructure Protection in the Netherlands. The Dutch approach on CIP*.[77]

6.7 Italia

Per i dag er det ingen overordnet italiensk metode for identifisering og rangering av kritisk infrastruktur.

Derimot foreligger en gjennomarbeidet metode for beredskap på nasjonalt, regionalt og lokalt plan. Innenriksdepartementet og Avdelingen for sivil beskyttelse har utviklet "Augustusmetoden"[78] som tar sitt navn og konsept fra keiser Octavius Augustus: *"Verdien av planlegging minsker med tingenes kompleksitet"*. Nøkkelordene er enkelthet og fleksibilitet, og metoden skal være en motsats til planer som kun eksisterer på byråkratisk nivå og ikke i praksis. På bakgrunn av Augustusmetoden ble det opprettet flere regionale og kommunale operative enheter med ansvar for ulike støttefunksjoner. Enhetene skal sikre kontinuerlig oversikt over kritiske forhold i nærmiljøet, og informasjonen går til Avdeling for sivil beskyttelse som har et nasjonalt overblikk. Med denne metoden oppnår man å ha ressurser tilgjengelig for enhver støttefunksjon, og enhetene er også ansvarlige for støttefunksjonen i en operativ fase samt for all oppdatering. Beredskapsplaner utarbeides således på kommunalt, regionalt og nasjonalt nivå, med bakgrunn i informasjon fra denne desentraliserte organiseringen. I beredskapsplanene forelegges lister over kritiske områder, bedrifter og personer på nasjonalt, regionalt og lokalt nivå. Det foreligger dessverre lite informasjon om selve utarbeidelsen av innholdet i beredskapsplanene, men Avdeling for sivil beskyttelse opplyser at de tar utgangspunkt i beredskapsplaner oppført

[77] Ministry of the Interior and Kingdom Relations. 2004. *Critical Infrastructure Protection in the Netherlands. The Dutch approach on CIP*. March 2004.
[78] Mer om Augustusmetoden, se Protezione Civile Internettside 2006.

etter Augustusmetoden når de skal vurdere prioritet i en krise. Som eksempel nevnes at da man utarbeidet denne typen beredskapsplan for et område, ble det avdekket at enkelte personer ville være vanskelige å evakuere ved for eksempel skred, på grunn av deres handikap eller uførhet. Det vil da være naturlig å assistere disse personene først ved en evakuering.

Augustusmetoden sier lite om hvordan man velger ut de ulike kritiske infrastrukturene og hvordan man går frem for å prioritere mellom dem. Den er også i hovedsak innrettet mot naturkriser, og ikke mot for eksempel terrorisme og cyberkriminalitet.

På spørsmål til Avdelingen for sivil beskyttelse[79] om hvordan beredskapsplanene og listene utformes henvises det til risikofaktoren:

Risiko = utsatthet x sårbarhet x verdi

Utsatthet evalueres ut fra sannsynligheten for at en hendelse av en viss karakter inntreffer i løpet av en gitt periode. Utsatthet er dermed en funksjon av hendelsens hyppighet (sannsynlighet). *Sårbarhet* regnes som evnen til å motstå effektene av en hendelse, og uttrykkes på en skala fra 0 (ingen skade) til 1 (total ødeleggelse). *Verdi* er betydningen av elementet som utsettes for hendelsen, enten det er av human karakter (tap av liv) eller verdien av materielle skader som har konsekvenser for befolkningen. Kritisk infrastruktur identifiseres ut fra nasjonale sikkerhetshensyn på områdene *institusjoner, transport, finans, kommunikasjon og energi*. De to sistnevnte oppfattes som sektorovergripende, og er også kjernen i det som regnes som grunnleggende tjenester.

Risikoanalysene danner altså grunnlaget for utarbeidelsen av beredskapsplaner, og for identifiseringen av hvilke samfunnsfunksjoner som regnes som kritiske. En slik identifisering skal ikke skje på bakgrunn av rigide forhåndsbestemte kriterier, men de lokale risikofaktorer skal evalueres ut fra situasjonen. Her kommer også de desentraliserte støttefunksjonen til sin rett, og tilføyer lokalkunnskap om kritisk infrastruktur og beredskap.

Ansvaret for beskyttelse av kritisk infrastruktur er lagt til Innenriksdepartementet[80], ved Politiets post og kommunikasjonsbyrå, herunder CNAIPIC-senteret for motarbeidelse av informasjonskriminalitet og beskyttelse av kritisk infrastruktur. ”*Vi mottar lister fra departementene over kritisk infrastruktur og har ingen del i en eventuell prioritering*”, uttaler en sentral aktør i CNAIPIC.[81] Senteret på sin side kontakter de identifiserte kritiske enhetene og inngår en avtale med disse om assistanse.

I en rapport utarbeidet for eiere av kritisk infrastruktur henvises det til behovet for en fleksibel

[79] Epostkorrespondanse med Andrea Duro, Presidenza del Consiglio dei Ministri, Dip. della Protezione Civile, 6.12.2005.
[80] Ansvaret er lagt til CNAIPIC gjennom Antiterrorloven. *Decr.legge* 144 / 24 juli 2005, *art. 7 bis*. Italia.
[81] Opplyst av Dr. Claudio Caroselli i Servizio Polizia Postale e delle Communicazioni (Politiets post og kommunikasjonsvesen), telefonintervju, 24.11.2005

metode for håndtering av risiko som kan benyttes på alle systemer.[82] En slik metode må ta hensyn til gjensidige avhengigheter som kan være operative, logiske og/eller geografiske. Metoden bør i følge ISCOM-gruppen følge disse stegene:

1. Identifisering og modellering av hva som skal beskyttes (kontekst som innbefatter kritisk element, gjensidige avhengigheter og risikonivå: en form for virkelighetsrepresentasjon).
2. Trussel- og konsekvensanalyse (identifisere trusler mot kritiske element i infrastrukturen, konsekvens, vurdering av beskyttelseseffekt). Fordrer kvantitativ eller kvalitativ konsekvensberegning samt sårbarhetsberegning.
3. Risikoevaluering basert på alvorlighetsgraden av et angrep i forhold til sannsynligheten for at et angrep inntreffer (funksjon av parametere fra steg 2; konsekvens og sårbarhet).
4. Definisjon av strategi for risikohåndtering.
5. Evaluering av effektivitet for eventuelt å lansere nye, mer effektive tiltak. Tilfører også læring (incident learning) og ny informasjon kan lagres i en database over hendelser.
6. Simulering (matematisk modellering) og testing av operasjonsprosedyren.

ISCOM avslutter med å anbefale en kriseenhet hvor eiere av kritisk infrastruktur er representert. Det ser ut til at CNAIPIC til en stor grad vil ta denne rollen, supplert av en nyopprettet nasjonal CERT, spesifikt for informasjons- og kommunikasjonsteknologi.

Det arbeides også på andre nivå med metoder for identifisering av kritisk infrastruktur. Ved Statsministerens kontor arbeider Roberto Setola[83] og Paolo Donzelli med muligheten for å lage en målstyrt metode (*top-down*) ut fra to tilnærminger. Den første går ut på å identifisere hva slags grunnleggende behov hver organisasjon baserer seg på for å kunne levere sine tjenester (avhengighet), mens den andre tilnærmingen ser på hva slags innvirkning et brudd i et slik grunnleggende behov har (konsekvens). Rammeverket som presenteres er en målstyrt avhengighetsbasert analyse som tar utgangspunkt i organisasjoners kjernevirksomhet, og ser på hva slags grunnleggende ressurser, fra egen og andre sektorer, som en organisasjon er avhengig av for sin egen tjenesteleveranse. Sannsynlighet for og innvirkning av (konsekvens) et brudd i en slik avhengighet blir evaluert for å bidra til å identifisere, analysere og redusere risikoer i bedrifters avhengighetsforhold. Rammeverket som det arbeides ut fra er organisasjonsmodelleringsteknikk i kombinasjon med en *infrastruktursimulator*.[84]

---

[82] Amici, Stefano et.al. 2005. *Network Security in Critical Infrastructures*. Istituto Superiore delle Comunicazionie delle Tecnologie dell'Informazione (ISCOM) 2005. www.iscom.gov.it/documenti/files/news/pub_003_eng.pdf

[83] Roberto Setola er teknisk ansvarlig for regjeringens arbeidsgruppe for beskyttelse av kritisk infrastruktur, og medlem av G8s seniorekspertgruppe for CIIP. Se forøvrig Donzelli, Paolo. Setola, Roberto og Tucci, Salvatore. 2004. *Identifying and Evaluating Critical Infrastructures- A Goal Driven Dependability Analysis Framework - Communications in Computing* 2004; Donzelli, Paolo. Setola, Roberto .2005. *Identifying and Evaluating Risks related to External Dipendencies: A Practical Goal Driven Risk Analysis Framework.*

[84] Eksempel på simuleringsverktøy er *Fuzzy Logic* (FL) og *Critical Infrastructure Simulation by Interdependent Agents* (CISIA).

6.8 Tyskland – ”Protection of Critical Infrastructures – Baseline Protection Concept”

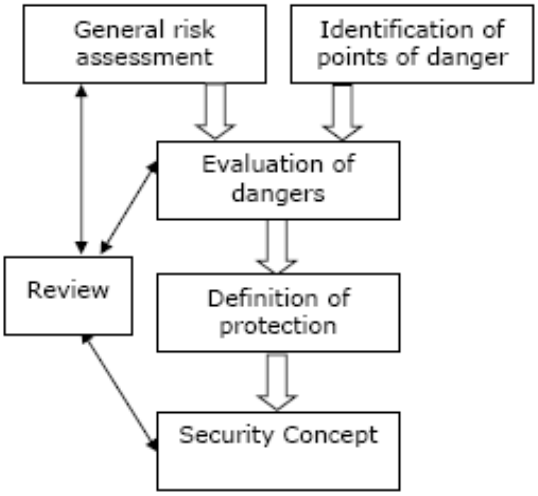
Som et ledd i å beskytte kritisk infrastruktur mot terror og naturkatastrofer har tyske myndigheter utarbeidet et *Baseline protection concept* som gir et sett med sikkerhetsanbefalinger til virksomheter.[85] Beskyttelseskonseptet er utviklet av det tyske Forbundskontoret for samfunnssikkerhet og katastrofehåndtering (BKK) og det Føderale kriminalpolitiet. Myndighetene har hatt et tett samarbeid med næringslivet under denne prosessen.

Den overordnede målsettingen for beskyttelseskonseptet er gjennom et tett samarbeid med infrastruktureiere å kunne sette prioriteringer og operasjonalisere tiltak for å beskytte kritisk infrastruktur. Beskyttelseskonseptet innebærer en analyse- og planleggingsprosess i åtte trinn:

1) Etablere farekategorier (gruppert etter områdene naturkatastrofer, ulykker og terrorisme/kriminalitet): lister opp fareområder og mulige scenarier innenfor disse. Inkluderer også konsekvenser for de ulike scenariene.
2) Basert på punkt 1; definere de respektive beskyttelsesnivåene
3) Utvikle skade- og trusselscenarier
4) Analysere svake punkter (sårbarheter)
5) Formulere beskyttelsesmål som grunnlag for å definere beskyttelsestiltak og mottiltak
6) Definere nødvendig handlingsrom (koordinering av tiltak mellom offentlig og privat sektor)
7) Implementere handlingsrom
8) Jevnlig revidere analyse- og planleggingprosessen med henblikk på kvalitetssikring

Figur 6.8 viser hvilke overordnede steg som skal dekkes før et endelig beskyttelseskonsept/*security concept* er klart:

[85] Federal Ministry of the Interior. 2005. *Protection of Critical Infrastructures – Baseline Protection Concept. Recommendation for Companies.* Germany 2005.



Figur 6.8 Tysklands beskyttelseskonsept

For å operasjonalisere sikkerhetskonsepter for virksomheter, er det utarbeidet et spørreskjema og en sjekkliste. Spørreskjemaet er laget som et hjelpemiddel for virksomhetene, og vil kunne styre diskusjonen inn på hvordan sikkerhet kan forbedres på en målrettet måte. Spørreskjemaet har fire hovedkategorier med underliggende spørsmål:

1. **Strukturer og samarbeidsprosjekter**
   Kartlegge hvordan sikkerhet (fysisk-, informasjons- og personellsikkerhet) blir håndtert internt: avdekke samarbeidsmønstre internt og eksternt i bl.a. krisesituasjoner.
2. **Undersøkelser, konsepter (analyse av beskyttelseskrav)**
   Avdekke om det er gjennomført risikoanalyser og mer detaljerte systemanalyser for å avdekke gjensidige avhengigheter.
3. **Forebyggende tiltak**
   Kartlegge hva som er gjennomført av undersøkelser i etterkant av alvorlige hendelser: hvilke virkemidler som er benyttet til teknisk overvåkning, etterforskning og bevisinnsamling, samt hvilke tekniske og organisatoriske tiltak som er gjort for å beskytte produkter og produksjons/prosessutstyr.
4. **Kriseledelse for store hendelser (avbruddsplaner, redundans, beredskapsplaner)**
   Avdekke hvordan kriser håndteres og hvilke planer som finnes for krisehåndtering.

Sjekklisten vil være et hjelpemiddel for kontroll under implementeringsprosessen, og er inndelt etter følgende kategorier:

a) Beskyttelse av objekter (fasiliteter/anlegg, installasjoner)
b) Personell
c) Organisasjon
d) Risikostyring
e) Kriseberedskap og katastrofeplaner

For hver kategori er det definert en rekke underpunkter med spørsmål. Eksempler på spørsmål

innenfor den siste kategorien (kriseberedskap og katastrofeplaner) kan se ut som i Tabell 6.18:

	Ja	Nei	Planlagt/ påtenkt	Nødvendige tiltak
Finnes det beredskapsplaner for krisesituasjoner?				
Er ansvarsområder definert i tilfelle en krise?				
Blir det regelmessig gjennomført beredskapsøvelser?				

Tabell 6.18 Eksempel på spørsmål fra sjekklisten

Både spørreskjemaet og den seks siders lange sjekklisten er vedlagt beskyttelseskonseptet.[86]

Vi har ennå ikke sett denne metoden anvendt. Forbundskontoret for samfunnssikkerhet og katastrofehåndtering og det føderale kriminalpolitiet skal ivareta oppfølging av konseptet. Virksomheter med kritisk infrastruktur blir oppfordret til å samarbeide med hverandre, og til å benytte fagmyndigheter innen for eksempel helse, brannsikring og krisestyring i prosessen.

Gjennomføring av metoden vil kreve store ressurser, og det foreligger ingen planer på hvordan man skal få virksomheter til å implementere prosessen. I tillegg er det ikke sagt noe om hvordan resultatene av de ulike prosessene skal benyttes på nasjonalt plan. Slik den tyske metoden er i dag, er den kun et verktøy for egenbeskyttelse av den enkelte virksomhet.

Metoden gir ingen innspill til hvordan man kan gjennomføre en fullstendig nasjonal gjennomgang for å identifisere kritiske infrastrukturer. Metodikken inkluderer heller ikke rangering, annet enn at det innledningsvis nevnes at resultatene kan bidra til prioritering. Likevel inneholder spørreskjemaet og sjekklisten en rekke punkter som kan være interessante for en norsk metode.

6.9 Portugal – Ranking Critical Infrastructures for the Definitions of Protection Policies

Den 22. november 2004 ble det holdt en presentasjon for SCEPC (Senior Emergency Planning Committee) i NATO fra det portugisiske *National Council for Civil Emergency Planning* (NCCEP)[87] om en måte å rangere kritisk infrastruktur på. Følgende informasjon er hentet fra denne presentasjonen:

Portugiserne definerer kritisk infrastruktur som et område, en fasilitet eller et sett av fasiliteter, eller et element som kjennetegnes av at en forstyrrelse eller misbruk, ødeleggelse (total eller delvis), permanent eller for en lang tidsperiode, vil redusere befolkningens velvære ved å påvirke funksjonaliteten til egen sektor eller andre sektorer, kontinuiteten i myndighetsutøvelse, rikets sikkerhet eller kollektive verdier og symboler.

Kritisk infrastruktur kan med dette utgangspunktet deles inn i fire sektorer, som vist i Tabell 6.19:

[86] Federal Ministry of the Interior 2005. *Protection of Critical Infrastructures – Baseline Protection Concept. Recommendation for Companies.* Germany 2005.
[87] NCCEP (på portugisisk): http://www.cnpce.gov.pt/

Security	Myndighetsutøvelse	Økonomiske sektorer	Verdier og symboler
• Forsvar • Lovgivende, dømmende makt og intern sikkerhet • Safety • Etterretning	• Regjering • Utenrikspolitikk • Offentlig administrasjon • Justis	• Elektrisitetsforsyning • Drivstoff • Naturgass • Vann og avløp • Kommunikasjon • Posttjenester • Mat og jordbruk • Helse • Transport • Media • Finans • Industri • Handel	• Miljø • Arv (kultur, religion) • Symboler

Tabell 6.19 Oversikt over kritiske infrastrukturer, Portugal ("Ranking Critical Infrastructures for the Definition of Protection Policies", presentasjon av NCCEP for SCEPC, 2004)

Alle disse sektorene er dermed med å understøtte det overordnede målet for nasjonen, som er å sikre befolkningens ve og vel.

Som arbeidsprosess for å identifisere og rangere kritisk infrastruktur, har NCCEP satt sammen en ekspertgruppe, *CIP Working Group*, bestående av 50 representanter fra ulike sektorer. Dette er gjort fordi NCCEP mener Portugal har mange eksperter, og at deres kompetanse og synspunkter må utnyttes. Ekspertene er plukket ut med bakgrunn i tre kriterier:

- Mangfold i synspunkter - ekspertene må tilhøre både privat og offentlig sektor, fra brede og representative kunnskapsfelt.
- Uavhengighet - ekspertenes meninger skal ikke være påvirket av andres innflytelse og restriksjoner.
- Desentralisering - flesteparten av ekspertene må tilhøre og jobbe i uavhengige tematiske

sektorer (helse, energi, sikkerhet, transport etc.)

For å rangere har NCCEP utviklet en metode som baserer seg på flermålsanalyse.[88] To rammeverk er brukt for å rangere:

- MCDA – Multi Criteria Decision Aid for selve rangeringen
- Operasjonsanalyse; nettverksanalyse (graf-teori) for å modellere gjensidige avhengigheter

Følgende kriterier er brukt i forbindelse med analyse av gjensidige avhengigheter:

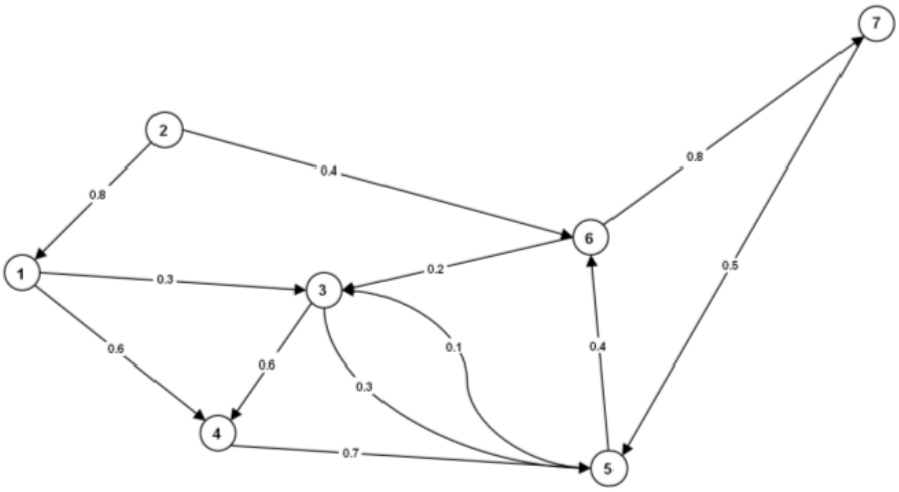
- Forventet skadeverdi for hele systemet – her er det snakk om direkte konsekvenser
- Avhengighet – gjennomsnittlig eller maksimal sannsynlighet for å bli indirekte påvirket
- Kritikalitet – vektet forventet skadeverdi i forhold til utsatthet

NCCEP legger følgende definisjon til grunn for å måle kritikalitet av en infrastruktur:

> *An infrastructure, or asset, should be considered more critical than another if there is greater evidence that the exploitment of vulnerability could seriously affect one of the major objectives present in the definition of critical infrastructure*.[89]

Med andre ord ligger fokus på sårbarheten i infrastrukturen, det vil si hvor utsatt en infrastruktur er. For å måle kritikalitet er det lagt vekt på sannsynligheter. I stedet for å bruke kvalitative mål på sannsynlighet (for eksempel høy, middels, lav) blir det tilegnet tallverdier på sannsynlighetene. Ved hjelp av grafteori kan man dermed få frem en matematisk representasjon av en graf, som vist i Figur 6.9:

[88] National Council for Civil Emergency Planning (NCCEP. Planeamenta Civil de Emergência) 2005. *Critical Infrastructure Protection in Portugal – Ranking Critical Infrastructures – the Portuguese Methodology*.
[89] National Council for Civil Emergency Planning (NCCEP. Planeamenta Civil de Emergência) 2005. *Critical Infrastructure Protection in Portugal – Ranking Critical Infrastructures – the Portuguese Methodology*.



Figur 6.9 Eksempel på hvordan modellere avhengigheter og sannsynligheter ved hjelp av grafteori. Nodene kan representere f.eks. en sektor, infrastruktur eller et element. Pilene mellom nodene representerer avhengigheter og deres sannsynligheter (NCCEP, 2005, "Critical Infrastructure Protection in Portugal – Ranking Critical Infrastructures – the Portuguese Methodology", s. 20).

Videre er det illustrert med en rekke eksempler hvordan man kan bruke matematiske algoritmer for å kalkulere sannsynligheten for at hver node skal bli berørt dersom det er oppstått forstyrrelse i en annen node.

NCCEP understreker at MCDA ikke egner seg som metode i en første fase for å komme frem til overordnede lister over hva som er mulige kritiske infrastrukturer. Dette skyldes blant annet at modellen må være forståelig for alle som skal delta i arbeidet, i tillegg til de som skal ta beslutninger. For å komme frem til tall som kan brukes for å tallfeste konsekvenser, kreves det modellering som både er tidkrevende og kostbart. MCDA vil derimot være et bra verktøy når man har kommet til en mer detaljert fase i hele prosessen og skal foreta rangeringer. Fordelene med å bruke verktøy innen MCDA er blant annet at det tilbyr en konsistent måte å aggregere score på og for å oppnå en endelig rangering for hvert alternativ.

Til grunn for å identifisere og rangere kritiske infrastruktur ligger det en 4-årig arbeidsplan som ledes og følges opp av NCCEP.[90] Planen er nokså detaljert og lister opp aktiviteter som skal foregå over de fire årene, slik at man til slutt ender opp med en total gjennomgang av kritiske infrastruktur i Portugal. Et foreløpig resultat er vist i avhengighetsmatrisen i Figur 6.10:

[90] National Council for Civil Emergency Planning (NCCEP. Planeamenta Civil de Emergência) 2005. *Critical Infrastructure Protection in Portugal – Workplan 2003-2007.*

Dependencies			1	2	3	4	5	6	7	10	18	20	21	23	24	25	26	28	29	30	31	32	33	34
							Security				Values			Economy										
			Well-Being	Security	Governance	Values	Navy	Air Force	Army	Civil Prottection	Water	Food	Public Health	Electric Power	Combustibles	Natural Gas	Road Transportation	Railroads	Ocean Shipping	Civil Aviation	Pipelines	Fixed Communications	Mibile Communications	Satelite Communications
1	Well-Being		1	1	1	1																		
2		Security		1			1	1	1	1														
3		Governance			1																			
4		Values				1					1	1	1											
5	Security	Navy					1.00	0.70	0.70	0.30	0.83	0.45	0.30	0.60	0.80	0.05	0.15	0.15	0.30	0.20	0.05	0.50	0.50	0.05
6		Air Force					1.00	1.00	1.00	0.63	1.00	0.88	0.75	0.88	0.88	0.38	0.75	0.75	0.75	0.75	0.75	0.88	0.88	0.88
7		Army					1.00	1.00	1.00	0.79	1.00	0.99	0.96	0.95	0.96	0.03	0.79	0.84	0.65	0.75	0.08	0.88	0.86	0.70
10		Civil Prottection					0.50	0.50	0.50	1.00	0.95	0.75	0.50	0.97	0.75	0.25	0.10	0.10	0.03	0.03	0.10	0.97	0.97	0.75
18	Values	Water									1.00													
20		Food					0.24	0.24	0.24	0.44	1.00	1.00	0.47	0.88	0.87	0.31	0.89	0.38	0.64	0.45	0.16	0.58	0.49	0.32
21		Public Health					0.65	0.65	0.65	0.50	1.00	0.96	1.00	1.00		0.53	0.72	0.23	0.32	0.29	0.32	0.87	0.79	0.06
23	Economy	Electric Power					0.42	0.42	0.42	0.70	1.00	0.05	0.10	1.00	0.99	0.95	0.95	0.30	0.97	0.20	0.80	1.00	0.99	0.15
24		Combustibles					0.15	0.15	0.15	0.64	1.00	0.10	0.35	0.93	1.00	0.15	1.00	0.10	1.00	0.05	1.00	0.85	0.86	0.65
25		Natural Gas					0.05	0.05	0.05	0.53	0.20	0.07	0.07	1.00	1.00	1.00	0.72	0.10	1.00	0.25	1.00	0.65	0.83	
26		Road Transportation					0.29	0.29	0.29	0.71	0.92	0.57	0.57	0.95	0.95	0.29	1.00	1.00	0.43	0.29		0.71	0.71	0.57
28		Railroads					0.29	0.29	0.29	0.71	0.92	0.57	0.57	0.95	0.95	0.29	1.00	1.00	0.43	0.29		0.71	0.71	0.57
29		Ocean Shipping					0.22	0.22	0.22	0.35	0.32	0.10	0.09	0.83	0.85	0.07	0.76	0.58	1.00	0.08	0.48	0.65	0.67	0.54
30		Civil Aviation					0.10	0.10	0.10	0.07	0.23		0.20	0.96	0.76	0.20	0.43	0.26		1.00	0.26	0.86	0.56	0.26
31		Pipelines																			1.00			
32		Fixed Communications								0.10	0.92	0.50	0.50	1.00	0.80		0.80	0.20		0.20		1.00	1.00	1.00
33		Mibile Communications								0.10	0.92	0.50	0.50	1.00	0.80		0.80	0.20		0.20		1.00	1.00	1.00
34		Satelite Communications								0.10	0.92	0.50	0.50	1.00	0.80		0.80	0.20		0.20		1.00	1.00	1.00

Figur 6.10 Eksempel på resultater fra portugisisk metode, som viser avhengigheter mellom strategiske sektorer (NCCEP, 2005, "Critical Infrastructure Protection in Portugal – Ranking Critical Infrastructures – the Portuguese Methodology", s. 25).

Det understrekes i metoden at denne figuren ikke er et helt ferdig produkt, men den gir en indikasjon på noe av det som vil komme ut av det portugisiske arbeidet. Dersom man ønsker å gå i dybden med enkelte sektoranalyser, er dette ett eksempel på hvordan det kan gjøres i praksis. Det vil imidlertid stille store krav til kompetanse hos de som skal utarbeide det, i tillegg til at det vil være en tidkrevende prosess å få modellert alle forholdene.

6.10 EU – Critical Infrastructure Protection in the fight against terrorism

EU har styrket innsatsen på området CIP ved at Ministerrådet støtter opprettelsen av et EU-program for beskyttelse av kritisk infrastruktur (EPCIP) etter forslag fra Kommisjonen.[91] Kommisjonen følger opp Rådets tilslutning i en grønnbok om beskyttelse av kritisk infrastruktur.[92] Her fremlegges diskusjonsforslag til hva et slikt program skal inneholde. Formålet

[91] Ministerrådets konklusjoner: *Prevention, Preparedness and Response to Terrorist Attacks* og *EU solidarity Programme on the Consequences of Terrorist Threats and Attacks* av desember 2004 samt Kommisjonens meddelelse: Communication from the Commission to the Council and the European Parliament. COM (2004) 702 final. *Critical Infrastructure Protection in the fight against terrorism.* Brussels. 20.10.2004.

[92] Commision of the European Comunities 2005. *Green Paper on a European Programme for Critical Infrastructure Protection.* Brussels, 17.11.2005. COM (2005) 576 final.

er å sikre et hensiktsmessig og ensartet beskyttelsesnivå for kritisk infrastruktur, å minimere de svake punkter og å teste beredskapsordninger i EU. Kommisjonen foreslår et sett med kriterier for å fastslå hva kritisk infrastruktur er.

6.10.1 EUs forslag til kriterier i følge kommisjonen

I Kommisjonens meddelelse blir det fastslått at Europas infrastrukturer i høy grad er sammenkoblet og gjensidig avhengige. Sammenslåing av selskaper, rasjonalisering av industri, effektivisering av forretningspraksis slik som *just-in-time* prinsippet og befolkningskonsentrasjon til urbane områder har alle bidratt til det. Videre henvises det til at Europas kritiske infrastrukturer er blitt mer avhengig av vanlig informasjonsteknologi, inkludert internett og verdensrombasert radionavigasjon og kommunikasjon. Problemer kan spres gjennom gjensidig avhengige infrastrukturer, og skape uventede og alvorlig svikt i essensielle tjenester. Sammenkobling og gjensidige avhengigheter gjør disse infrastrukturene mer sårbare for avbrudd og ødeleggelse.

Kommisjonen foreslår en definisjon av europeisk kritisk infrastruktur (EKI) i grønnbokens første anneks. EKI bestemmes i hovedsak ut fra dens grenseoverskridende effekt, det vil si om en hendelse har effekt på to eller flere medlemsstater. En vurdering av alvorlighetsgrad baseres på tre faktorer.[93]

1. *Geografisk rekkevidde* – Tap av et kritisk infrastrukturelement er rangert ut fra omfanget av det geografiske området som kan bli berørt av tapet eller av manglende tilgjengelighet – ut over to eller tre medlemsstaters territorium.[94] Graden av innvirkning eller tap kan vurderes til Ingen, Minimal, Moderat eller Stor. For å vurdere potensiell størrelse kan man se på:
    a) Innvirkning på publikum (antall mennesker berørt, tap av liv, sykdom, alvorlig skade, evakuering).
    b) Økonomisk innvirkning (effekt på BNP, betydning av økonomisk tap og/eller degradering av produkter og tjenester).
    c) Innvirkning på miljøet (innvirkning på befolkningen og de omliggende områder).
    d) Innvirkning på gjensidig avhengighet (mellom andre kritiske infrastrukturelementer).
    e) Politisk innvirkning (tillit til myndighetenes evne til å utøve myndighet).
    f) Psykologiske effekter kan ved mange tilfeller føre til en eskalering av mindre hendelser.
2. *Effekter av tid* – for eksempel kan en sky med radioaktivt innhold krysse statsgrenser over tid.
3. *Grad av gjensidig avhengighet* – for eksempel hvilken effekt en elektrisk nettverksfeil i

[93] I den tidligere Kommisjonens meddelelse var disse faktorene nært identiske med de som Canada foreslår i sin metode fra desember 2002, ref.: *Draft. Tool to Assist Owners and Operators to Identify Critical Infrastructure Assets*. Office of Critical Infrastructure Protection and Emergency Preparedness. 19 December 2002. www.ocipep.gc.ca/critical/nciap_criteria_e.asp

[94] Om det skal være to eller tre medlemsstater er en del av debatten i anledning grønnboken. Med tre stater som minstekrav ekskluderes allerede eksisterende bilateralt samarbeid om kritisk infrastruktur.

én medlemsstat har på en annen.

Kommisjonen foreslår en prosess i syv steg.

1) Kommisjonen og medlemsstatene setter kriteriene for å identifisere EKI på sektorspesifikk basis.
2) Identifisering og verifisering av sektorspesifikk EKI. Hvorvidt en kritisk infrastruktur er europeisk bestemmes på EU-nivå ut fra dens grenseoverskridende natur (to eller tre medlemsstater), med unntak av forsvarsrelatert infrastruktur.
3) Medlemslandene og Kommisjonen analyserer eventuelle mangler og tomrom innen EKI ut fra enkeltsektorer.
4) Kommisjonen og statene enes om hvilke sektorer og EKI som bør ha prioritet, også tatt i betraktning gjensidige avhengigheter.
5) Kommisjonen og landene setter minstekrav for beskyttelsestiltak, der det er relevant.
6) Etter Rådets godkjenning implementeres disse tiltakene.
7) Kommisjonen, sammen med egne organ i medlemslandene overvåker og oppdaterer EPCIP-implementeringen.[95]

Det foreslåes at operatørene selv utarbeider sikkerhetsplaner (*Operator Security Plans*, OSP), som identifiserer kritisk infrastruktur hos operatøren selv, og etablerer relevante beskyttelsesløsninger. OSP vil kunne være en *bottom-up* tilnærming som gir større spillerom (og ansvar) i privat sektor.

I Kommisjonens grønnbok legges ved en indikativ liste over sektorer som kan inneholde kritiske infrastrukturer, med tilhørende produkter og tjenester, se Tabell 6.20. Denne listen er kun ment som diskusjonsgrunnlag, og er ikke utarbeidet med bakgrunn i en spesifikk metode.[96]

[95] Kommisjonen foreslår egne *National CIP Coordination Bodies* (NCCB)
[96] Samtale med Piotr Rydzkowski, CIP Desk officer, DG JLS.D.1, 27.01.2006

INDICATIVE LIST OF CRITICAL INFRASTRUCTURE SECTORS

Sector		Product or service	
I	Energy	1	Oil and gas production, refining, treatment and storage, including pipelines
		2	Electricity generation
		3	Transmission of electricity, gas and oil
		4	Distribution of electricity, gas and oil
II	Information, Communication Technologies, ICT	5	Information system and network protection
		6	Instrumentation automation and control systems (SCADA etc.)
		7	Internet
		8	Provision of fixed telecommunications
		9	Provision of mobile telecommunications
		10	Radio communication and navigation
		11	Satellite communication
		12	Broadcasting
III	Water	13	Provision of drinking water
		14	Control of water quality
		15	Stemming and control of water quantity
IV	Food	16	Provision of food and safeguarding food safety and security
V	Health	17	Medical and hospital care
		18	Medicines, serums, vaccines and pharmaceuticals
		19	Bio-laboratories and bio-agents
VI	Financial	20	Payment services/payment structures (private)
		21	Government financial assignment
VII	Public & Legal Order and Safety	22	Maintaining public & legal order, safety and security
		23	Administration of justice and detention
VIII	Civil administration	24	Government functions
		25	Armed forces
		26	Civil administration services
		27	Emergency services
		28	Postal and courier services
IX	Transport	29	Road transport
		30	Rail transport
		31	Air traffic
		32	Inland waterways transport
		33	Ocean and short-sea shipping
X	Chemical and nuclear industry	34	Production and storage/processing of chemical and nuclear substances
		35	Pipelines of dangerous goods (chemical substances)
XI	Space and Research	36	Space
		37	Research

Tabell 6.20 Kritisk infrastruktur i EU

6.10.2 Utfordringer og videre utvikling

EPCIP er fremdeles i startgropen når det gjelder identifisering av europeisk kritisk infrastruktur. For eksempel er det usikkert hvordan nasjonale kritiske infrastrukturer skal behandles i forhold til europeisk infrastruktur, men det er klart at medlemsstatene har mulighet til å være mer restriktive angående for eksempel minstekrav til sikkerhet, enn hva EPCIP kan legge opp til.

Kommisjonen har utlyst flere pilotprosjekter innen EPCIP, blant annet på området sårbarhetsmetode og utholdenhet i kritisk infrastruktur, herunder metodeutvikling.[97] Disse prosjektene skal delfinansieres av EU, og kan føre arbeidet flere skritt videre mot en europeisk

[97] EU EPCIPs Pilotprogram: http://ec.europa.eu/justice_home/funding/epcip/funding_epcip_en.htm

strategi for beskyttelse av kritisk infrastruktur. Et forslag til fullstendig program for beskyttelse av kritisk infrastruktur skal forelegges.

Deler av EPCIP, og spesielt det sektorspesifikke arbeidet videreføres, til tross for at man ennå ikke er enige om et felles rammeverk for EPCIP. For eksempel er det utarbeidet spørreskjema til europeiske regjeringer samt bedrifter om risikoberedskap på områder som informasjonssikkerhet,[98] energi og transport. Man har også bedt alle medlemsland, inklusive Norge, om å utnevne nasjonale kontaktpersoner for beskyttelse av kritisk infrastruktur. I Norge er kontaktpersonen i Justis- og politidepartementet.

Norsk nytte av EPCIP kan begrenses av at tilgang til deler av informasjonen i EPCIP i følge forslaget i grønnboken vil bli gradert og kun utveksles på *need-to-know*-basis. I tillegg er det mindre sannsynlig at man kommer frem til en omforent metode blant alle medlemslandene som er tilstrekkelig spesifikk til at den kan gi nyttige innspill til BAS5.

6.11 BAS1-prosjektet

I det første BAS-prosjektet ble det gjennomført en prioritering av ulike samfunnsfunksjoner.[99] Metodikken som ble benyttet gikk kort ut på at en for hver enkelt samfunnsfunksjon foretar en beskrivelse av funksjonen, egenskaper ved funksjonen og hvilke definisjoner som er benyttet. Videre argumenteres det for en del kvalitative vurderinger som gjøres mht. mulighet for alvorlig funksjonssvikt og konsekvens av alvorlig funksjonssvikt. Forutsetninger som gjøres og usikkerhet i de metoder og modeller som benyttes blir også diskutert. Denne informasjonen sammenstilles til slutt.

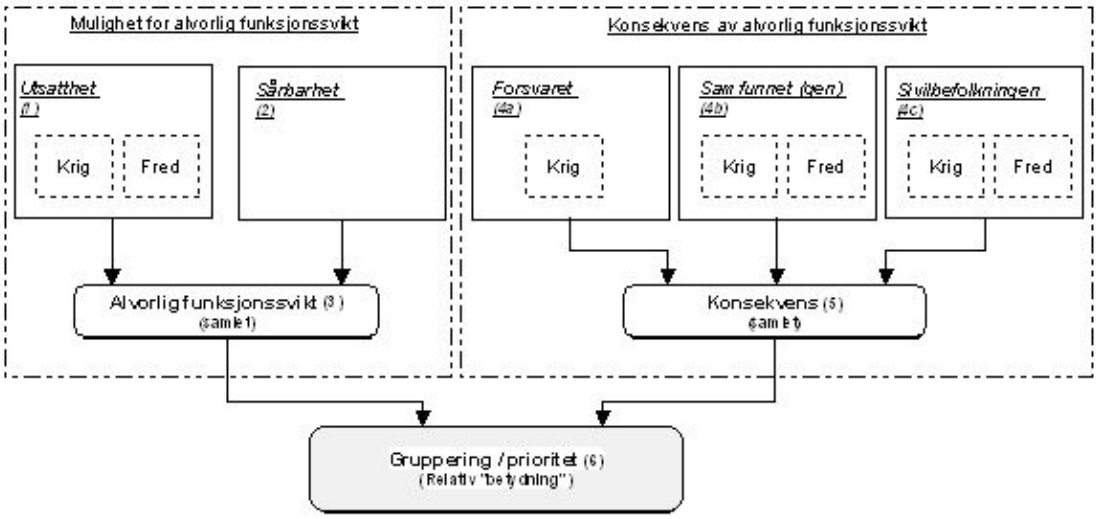
Metoden bygger på:

- Scenariobasert risikovurdering av samfunnsfunksjoner. Metoden for scenariobasert risikovurdering tar utgangspunkt i et krigsscenario og et fredsscenario. Krigsscenariet er basert på at et angrep kommer relativt overraskende og er begrenset i tid og rom. I fredsscenariet tas det utgangspunkt i en større naturkatastrofe hvor flom eller kraftig uvær fører til omfattende skade i en region av landet.
- Vurdering av den gjensidig avhengigheten mellom samfunnsfunksjoner. De gjensidige avhengigheten presenteres i en matrise.
- Oppbyggingsevne for beredskap innenfor en forberedelsestid på 1 måned og på 6 måneder.

Figur 6.11 viser en skjematisk fremstilling av modellen som er benyttet ved scenariobasert risikovurdering.

[98] Unisys Belgium 2005. *Survey to Assess Risk Preparedness in European businesses*. Done for the European Commission and The European Network and Information Security Agency. www.unisys.be/eprise/main/admin/country/doc/be/Risk_Preparedness_Survey_2005_FINALENG.pdf

[99] Fridheim, Håvard. Hæsken Ole Morten. Olsen Thor Gunnar. Balke, T, Ensrud May-Kristin 1997. *Viktige samfunnsfunksjoner*. FFI/RAPPORT-97/01458 (Begrenset)



Figur 6.11. Modellbeskrivelse BAS1

6.11.1 Begreper fra BAS1-arbeidet

Funksjonssvikt er et relativt begrep som kan omfatte alle grader av svikt fra de svært begrensede, som mer alminnelige operasjonsavbrudd på få timer, til langvarige brudd på dager og uker. I denne sammenheng fokuseres det på alvorlig svikt. Det ligger i det sivile beredskaps mål og organisering at det først og fremst planlegges for situasjoner der de dagligdagse rutiner (selv vanlige beredskapsrutiner) ikke kan anvendes eller viser seg utilstrekkelige.

Mulighet for alvorlig funksjonssvikt, søkes beskrevet gjennom en kvalitativ vurdering av funksjonens utsatthet og sårbarhet, definert som:

- Utsatthet = sannsynligheten for at en funksjon blir utsatt for en påkjenning som kan medføre svikt.
- Sårbarhet = sannsynligheten for at en svikt oppstår gitt at en påkjenning har funnet sted.

Utsatthet

En vurdering av en funksjons utsatthet medfører å kartlegge årsakene til at funksjonssvikten oppstår. Årsaken kan være knyttet til utenforliggende freds- eller krigstidsforhold som dårlig vær, terror, luftangrep osv. Slike årsaker er i modellen kalt *påkjenninger.* Påkjenningene vil ha stor innvirkning på funksjonenes evne til å fungere, og det er derfor nødvendig å se på sannsynligheten for svikt i lys av disse. Da det ikke er ønskelig å dele opp analysen for mye, og et hovedskille anses å gå mellom utfordringer i fred og i krig, opereres det med to grove kategorier av utsatthet: Utsatthet i krig og utsatthet i fred, der disse innbyrdes veies nøytralt.

Sårbarhet

Svikt som følge av en hendelse vil også kunne oppstå på grunn av mer interne tekniske og organisasjonsmessige forhold ved samfunnsfunksjonen. I modellen innbefatter dette også avhengighetsforhold til andre samfunnsfunksjoner. Årsak til svikt kan ligge i for eksempel kompleksitet i organisasjonsstruktur og rutiner, teknologiavhengighet, kritiske punkter og

avhengighet av kritiske komponenter og så videre. Disse årsakene er å finne innenfor den enkelte funksjon eller i et større system utenfor funksjonen, for eksempel ”samfunnet”, og representerer mer permanente egenskaper ved systemene, til forskjell fra de plutselige påkjenninger. Begrepet sårbarhet knyttes først og fremst til diskusjonen av disse egenskapene. Begrepet *store ytre påkjenninger* benyttes for å kunne klassifisere sårbarhet mellom funksjonene. Dette er en samlebetegnelse for påkjenninger som er typiske for scenariene, eksempelvis målrettet ødeleggelse under krigsscenariet og regionale naturkatastrofer under fredsscenariet.

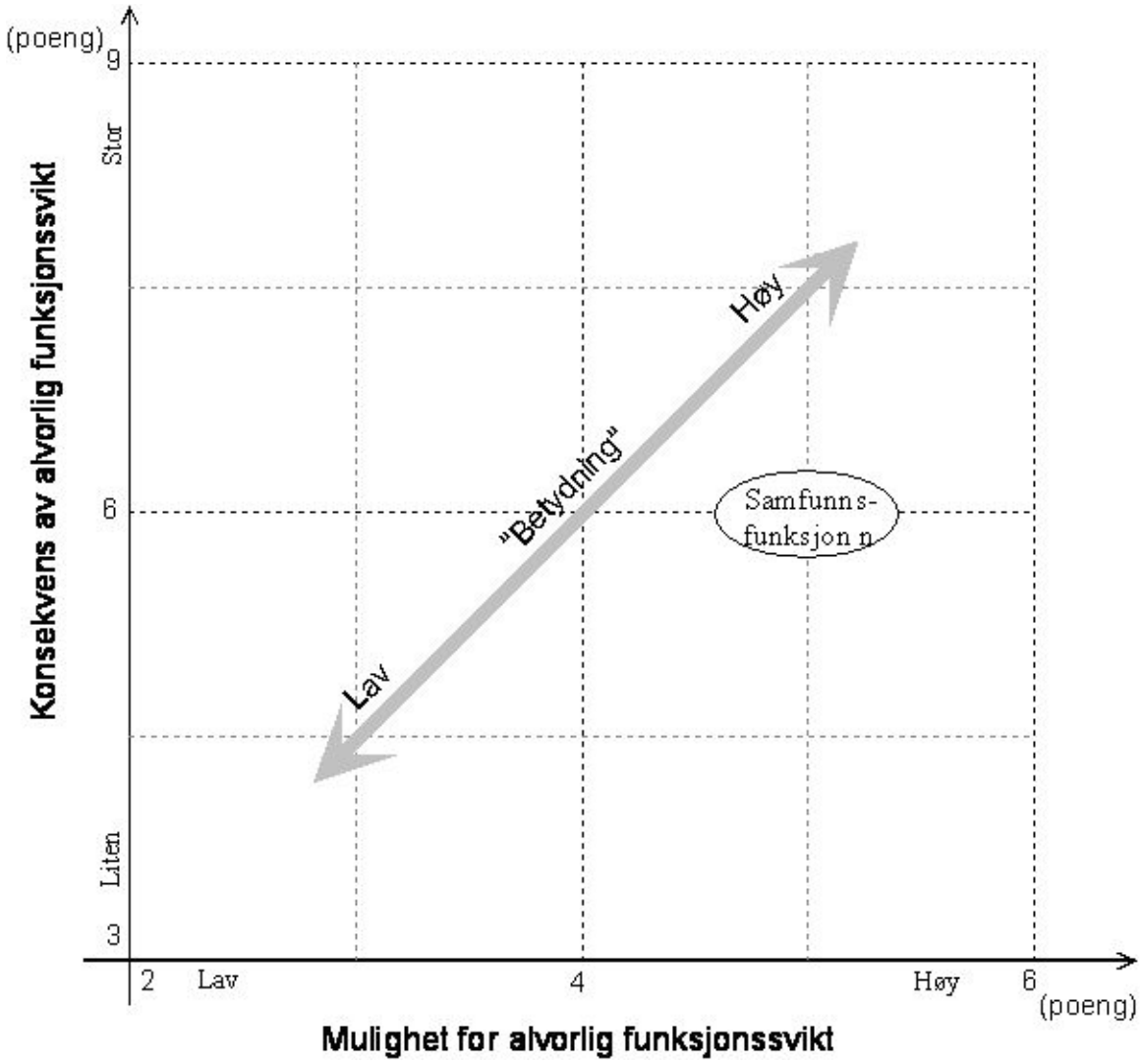
Konsekvenser

Konsekvensene av funksjonssvikt beskrives ved en gjennomgang av effekten av en alvorlig funksjonssvikt for Forsvaret (forsvarsevnen), andre samfunnsfunksjoner og sivilbefolkningen. De tre målgruppene er avledet av hovedmålene for det sivile beredskap. I BAS diskuteres kun de direkte effektene knyttet til hver av målgruppene som følge av en alvorlig funksjonssvikt. Indirekte effekter for Forsvaret, andre samfunnsfunksjoner eller sivilbefolkningen som følge av alvorlig svikt i en samfunnsfunksjon behandles ikke på grunn av manglende oversikt over ringvirkningene til sin ytterste konsekvens.

6.11.2 Presentasjon av resultater

Målet med analysemetoden er å komme frem til et grovt mål for de enkelte samfunnsfunksjonenes innbyrdes betydning for samfunnet. Begrepet *betydning* vil i denne sammenheng ha en utvidet definisjon, og betydning for samfunnet innbefatter elementene utsatthet, sårbarhet og konsekvens.

Ved beregning av mål for *konsekvens av alvorlig funksjonssvikt* og *mulighet for alvorlig funksjonssvikt* er det allerede foretatt forenklinger som medfører klare usikkerheter. For å unngå å innføre enda større usikkerheter ved bruk av beregningsmetoder er det valgt å presentere målet for *betydning for samfunnet* grafisk i et todimensjonalt plan som utspenner konsekvens av alvorlig funksjonssvikt og mulighet for alvorlig funksjonssvikt. I Figur 6.12 vises et eksempel på en slik presentasjonsform.



Figur 6.12 Samfunnsfunksjonenes betydning for samfunnet

Ut fra denne grafiske fremstillingen kan samfunnsfunksjonene avslutningsvis grupperes og prioriteres etter innbyrdes betydning for samfunnet.

Metoden må imidlertid betraktes som en svært forenklet vurdering av funksjonenes innbyrdes viktighet. Strengt tatt er ikke dette en risiko- og sårbarhetsanalyse, men en kvalitativ vurdering av funksjoner der en benytter de samme begrepene som en finner i slike analyser.

6.12 Infrastrukturutvalgets skjønnsmessige retningslinjer

Utvalget utarbeidet et sett med skjønnsmessige retningslinjer for å identifisere kritisk infrastruktur og kritiske samfunnsfunksjoner.[100] Retningslinjene kan omtales som en enkel metodikk med lave krav til metodiske forkunnskaper. Retningslinjene kan derfor tenkes å være nyttig som en ramme for diskusjoner knyttet til kritikalitet hvor kravene til detaljering er lave. For eksempel kan retningslinjene være med på legge til rette for å avgjøre hvilke objekter som er kritiske i olje- og

[100] NOU 2006:6. *Når sikkerheten er viktigst.*

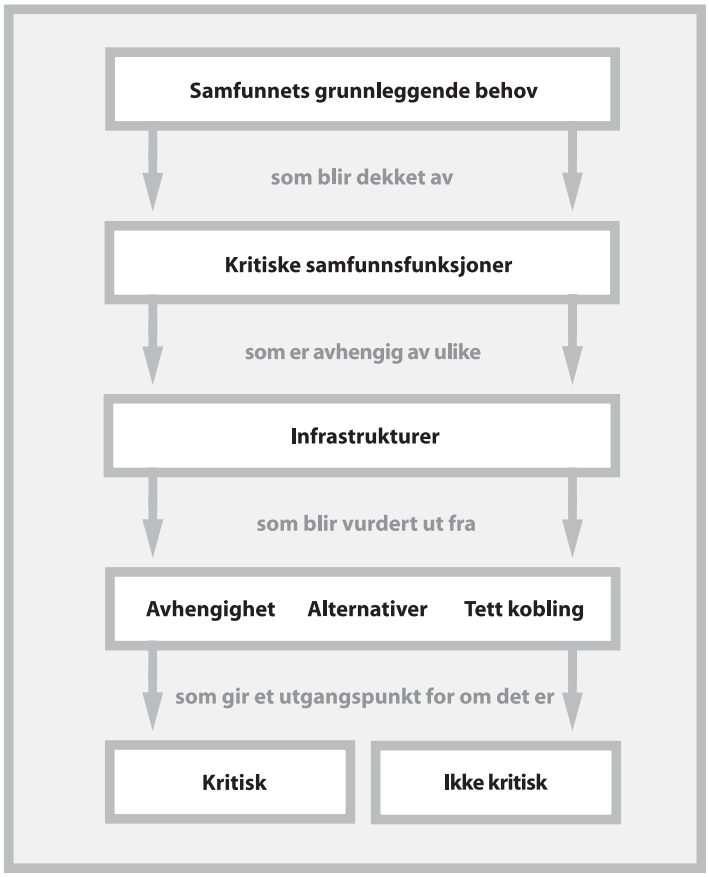
gassektoren. Samtidig er det usikkert om hvor nyttig retningslinjene er for å avdekke kritiske komponenter i mindre systemer og delsystemer. Retningslinjene gir heller ikke presise svar når det gjelder å rangere kritikalitet.

Retningslinjene tar utgangspunkt i samfunnets grunnleggende behov. Ut fra de grunnleggende behovene utledes hvilke samfunnsfunksjoner som må til for å dekke disse. Når forståelsen for hvilke funksjoner som er mest kritiske er etablert, har man et utgangspunkt for å se hvilken infrastruktur som understøtter samfunnsfunksjonene. Utvalget gir følgende eksempel for å illustrere sammenhengen.

> Eksempelvis kan ett av de mest grunnleggende behovene være å få hjelp ved sykdom og skade. Problemstillingene blir da som følger: Befolkningen har behov for hjelp ved sykdom og skade; samfunnsfunksjonen som dekker behovet er et helsevesen. Hvilke infrastrukturer er nødvendige for å opprettholde funksjonen helsevesen? Det kan eksempelvis være vann- og strøminfrastruktur, farmasøytisk industri osv.[101]

For å finne om infrastrukturen er kritisk eller ikke, benytter utvalget seg av tre kriterier. Det første kriteriet er *avhengighet*. Hvis mange er avhengig av infrastrukturen, vil et bortfall få store konsekvenser. Kriteriet er det som veier tyngst når kritisk infrastruktur skal identifiseres. Det andre kriteriet er *alternativer*. Manglende alternativer tilsier kritikalitet. Det tredje kriteriet innebærer å vurdere i hvilken grad infrastrukturen er tett koblet. Et tett koblet system innebærer at forstyrrelser et sted i et system få umiddelbare konsekvenser for systemet som helhet. Skjematisk kan retningslinjene fremstilles som i Figur 6.13.

[101] NOU 2006:6 *Når sikkerheten er viktigst*



Figur 6.13 Infrastrukturutvalgets retningslinjer for å identifisere kritisk infrastruktur og kritiske samfunnsfunksjoner.

6.13 Østfoldundersøkelsen[102]

Foranledningen for Østfoldundersøkelsen var den forventede kraftkrisen i 2002/2003 og NVEs pålegg om å forberede for kraftrasjonering med utgangspunkt i rasjoneringsforskriften.[103] Carl Georg Abel gjennomførte derfor en omfattende kartlegging av mulighetene for rasjonering i Østfold Energi sitt konsesjonsområde.[104] Utgangspunktet var å få til rasjonering på en mest skånsom og effektiv måte for samfunnet. I henhold til rasjoneringsforskriften var prioriteringskriteriene (1) liv og helse, (2) samfunnsviktig infrastruktur og (3) viktig industri, i den rekkefølgen.

Strømrasjonering er utført tidligere. Blant annet ble det gjennomført rasjonering i Bergen i 1982–83. Da ble bykjernen prioritert, med sonevise utkoblinger i utkantene. Dessuten ble varehus prioritert. Ellers var utkoblinger vanlige under krigen. Det var også vanlig å koble ut om nettene utover på 1950-tallet.

[102] Delkapittelet om Østfoldundersøkelsen baserer seg på intervju av Carl Georg Abel, NVE, 29. august 2006.
[103] Undersøkelsen ble gjennomført i perioden slutten av 2002 – sommeren 2003, av Carl Georg Abel, da i Østfold Energi, nå i NVEs Beredskapsseksjon.
[104] Carl Georg Abel var på det tidspunktet ansatt i Østfold energi.

I 2002 krevde NVE planer for sonevise utkoblinger for 75 % av normal last. Kun 25 % lasten kunne være fast innkoplet for forsyning av de viktigste forbrukerne i henhold til rasjoneringsforskriften. Det ble umiddelbart klart at nettet ikke er bygget for å fremme rasjonering og at gjennomføringen ville bli krevende. For eksempel er det ikke mulig å gi spesifikke kundegrupper prioritet uten at det følger med en stor mengde gratispassasjerer. Det ble også tidlig klart at det forelå lite informasjon som kunne understøtte arbeidet med å identifisere prioriterte brukere. NVE hadde en veileder som var til begrenset hjelp. Heller ikke det daværende Direktoratet for sivilt beredskap hadde tilstrekkelig detaljert informasjon for Abels formål.

Med BAS3 som utgangspunkt gjennomførte Abel en omfattende kartlegging av viktige brukere av kraft i sin egen hjemby Sarpsborg, hvor han er godt kjent. Metoden besto i å identifisere viktige brukere ved hjelp av kontakter. Kartleggingsprosessen ble gjennomført ved å identifisere på detaljnivå, før hovedstrukturene kunne identifisere. Kartleggingsprosessen viste at en rasjonering med utkoblinger på et så detaljert nivå som rasjoneringsforskriften og BAS3 tilsa, i praksis ikke var gjennomførbar. En detaljert utkoblingsrasjonering etter forskriftskriteriene ville medføre at man fysisk måtte ut og koble manuelt i hundrevis av trafokiosker flere ganger i døgnet.

Den foreløpige konklusjonen var at en tilsvarende undersøkelse måtte gjennomføres for hele konsesjonsområdet, men da kun basert på at utkoblinger skulle gjøres på avganger med fjernstyrte brytere på ”sekundærstasjonsnivå”, dvs. på nest laveste nettnivå; distribusjonsnettet. Disse dekker et mye større geografisk område, hvilket gir en rekke gratispassasjerer. Den videre kartlegging ble foretatt med søk i telefonkatalogen, dybdeintervju med personell på driftsentralen, møte med kommuner i Østfold, telefonhenvendelser til bedrifter, teleselskap, politi, NSB, sykehus og så videre.

Interessante observasjoner i prosessen, var at samarbeidet med Fylkesmannen var nyttig. De forstod problemstillingen. I kommunene ble problemstillingen dels ikke forstått, dels ikke tatt alvorlig. Videre var det vanskelig å få virksomheter til å foreta reelle prioriteringer i egen virksomhet. Prioriteringene kom først etter at de ble ”presset” til det. Dette gjaldt særlig i forhold til offentlige virksomheter. Eksempelvis viste det seg at Sarpsborg kommune måtte ”presses” til erkjennelsen om at driften av kommunens seks sykehjem kunne reduseres til ett sykehjem i en rasjoneringssituasjon. Det ble videre erfart at konklusjoner knyttet til prioriteringer ofte er avhengig av personlige kontakter med folk under ledernivå. Disse ønsket som regel ikke å bli sitert. En annen interessant observasjon var at det var vesentlig enklere å få klare svar fra industrien.

Datamengden gjorde at et databaseverktøy måtte tas i bruk, og metodikken var tilpasset dette. Alle ønsker om rasjoneringsfritak som kom inn (om lag 700) gjorde at kategorisering ble nødvendig for å kunne foreta en ensartet vurdering (gjengitt nedenfor). Datagrunnlaget måtte være strukturert og grundig, ellers ville resultatet av databasen bli verdiløs. Alle kundene ble derfor kategorisert med utgangspunkt i deres samfunnsmessige funksjon og registrert i databasen. Denne prosessen var tidkrevende. En vesentlig erfaring fra denne prosessen var også her at Abel

måtte forbi ledernivå i de enkelte virksomhetene og ned til operatørnivå for å få relevante og anvendelige svar. Kartleggingen omfattet muligheter til å bruke om lag 400 fjernstyrte brytere på de enkelte trafostasjoner til å regulere lasten.

Nedenfor er en oversikt over virksomheter, med virksomhetskoder, som ble vurdert og kategorisert i prosessen, i Tabell 6.21. De virksomhetstypene som er uthevet fikk prioritet med hensyn til fast innkobling, men det måtte likevel foretas prioritering innenfor disse.

Virk-kode	Virksomhetsbeskrivelse
SY	Sykehus i lovens forstand. Permanent innkoplet (Døgndrift)
VA	Vannverk med tilhørende renseanlegg for drikkevannsforsyning.
VK	Trykkøkningstasjon drikkevann, trykkbortfall. Kritisk, i den forstand at ved trykkbortfall kan det komme forurenset vann inn i vannledningene med påfølgende fare for epidemier. Svært "sløsende" ved knapp energitilgang, forutsettes at kommunen søker å løse dette ved egne mobile nødstrømsaggregat.
EV	Energiverk-internt Avganger brukt energiverk-internt, stasjonstrafo, avganger som forsyner andre stasjoner etc
KK	Kritisk Kloakkpumpe (eller annet kloakk-anlegg) hvor stans vil medføre snarlig overløp til drikkevannskilde, og kritisk forurensning av denne. Svært "sløsende" ved knapp energitilgang, forutsettes at kommunen søker å løse dette ved egne mobile nødstrømsaggregat.
DK	Døgnkritisk administrasjon (og tilhørende virksomhet i kategori 2). Politi, brannstasjon, alarmsentraler 110, 112, 113. Evt. kritisk kommunal adm. Energiverkets driftsentral. (Viking/Falken alarmsentral og tilsvarende store vaktselskaper: Her må innplassering av disse i hht rasjoneringsforskriften avgjøres av myndighetene)
TK	Viktige telekom Svært viktige (store) sentraler og hovedknutepunkt for telekommunikasjon, Radio- og TV-sendere for NRK. Med svært viktig menes at uten disse blir det fullstendig sammenbrudd i telenettet som helhet. Sentraler med dieselaggregat skal ikke med her - de klarer seg selv, så den strømmen kan brukes andre steder.
FK	Matforsyning av vesentlig betydning for befolkningen eller sykehus, hvor avbrudd vil få store konsekvenser. Dette gjelder store meierier, slakterier, evt. enkelte store bakerier, og kanskje fryselager.
LK	Legevakt / Tannlegevakt. Kritisk virksomhet i rasjoneringskategori 1 i hht forskriften. Dersom vakta f.eks bare driver på kveld, helg, natt, må det lages en egen utkoblingsplan for dette.
SH	Sykehjem, vil imidlertid medføre at store områder vil få permanent elektrisitetsforsyning. Kan vise seg at det ikke lar seg gjøre å opprettholde forsyningen til alle sykehjem. Det kan derfor bli nødvendig å koble ut enkelte mindre enheter, og pasienter/beboere må da flyttes i hht kommunenes evakueringsplaner.
VU	Trykkøkningstasjon drikkevann, trykkreduksjon. Ukritisk. Dette omfatter anlegg hvor stans medfører lavere trykk, men dog så høyt vanntrykk at det ikke er fare for at forurenset vann kommer inn i drikkevansnettet.
KU	Kloakk. Ukritisk Øvrig kloakk-anlegg for avløp. Både renseanlegg og pumpestasjoner. Alle slike pumper hvor stans ikke medfører kritisk samfunnskonsekvens plasseres i denne gruppe. Kategorisering av kloakrenseanlegg må eventuelt foretas av myndighetene (NVE).
RE	Renseanlegg vann/avløp
VS	Vaskerier - til sykehus sykehjem
AV	Kommunal administrasjon av sentral/viktig betydning for sentrale deler av kommunens drift for håndtering av rasjoneringssituasjonen og dennes konsekvenser. I denne kategori legges kun virksomheter som må ha strøm til bestemte tider på døgnet, og hvor det ikke finnes andre løsninger

Virk-kode	Virksomhetsbeskrivelse
	eller akseptable reserveløsninger.
OK	NSB kjøre- og signalstrøm, havneanlegg med fergeanløp som krever strøm for å være i drift..
AU	Off.Adm, Ukrit Kommunal administrasjon, post, eldresenter, som kan drive sin virksomhet med tilpassede utkoblingstider, f.eks roterende dagtid og kveldstid, eller hver annen uke. Det meste av den kommunale virksomhet.
FU	Forsyninger ukritisk. Bakerier, bryggeri, lager, terminaler, havneanlegg, bensinstasjoner. Virksomheter som kan tilpasse sin drift De fleste prioriterte virksomheter forutsettes plassert i denne kategori.
LD	Vanlig Lege/tannlege kontor. I den grad det er praktisk mulig alltid strøm på dagtid.
AP	Apotek, (Kun apotekvakt kan evt. prioriteres)
BU	Barnehage og tilsvarende.
HO	Hoteller
AL	All forsyning som ikke er prioritert i hht rasjoneringsforskriften. Sonevis roterende utkobling.
NM	Mekanisk industri, verksteder osv.
NP	Næringsliv som krever forsyning på spesielle vilkår, f.eks på ukebasis. Prosessindustri og næringsmiddelindustri.
OU	Omsorgsboliger og aldershjem er et sted hvor folk bor, og betraktes i denne sammenheng som en vanlig bolig. I denne gruppen hører bl.a omsorgsbolig for demente, aldershjem og tilsvarende.
MQ	Gårdsbruk med melkekyr. Permanent forsyning til ventilasjon ved oppdrett av fjørfe og svin skal ikkeprioriteres.
UN	Skole, undervisning, ukritisk. All undervisning kommer i denne kategori.
TU	Vanlige telefonsentraler, kabel-TV osv
UP	Uprioriterte Enheter som kobles ut permanent. Flomlys, Varmekabler i gågate, Elektrokjel med oljereserve, gatelys og tilsvarende.
ØH	Øvrige Helseinstitusjoner
NN	Næringsliv ukjent
UU	Ukjent- under arbeid
NU	Næringsliv ukritisk. Økonomisk, administrativt, handelsvirksomhet og butikker. Det meste av næringslivet tilhører denne kategorien. Avisredaksjoner, bank

Tabell 6.21. Virksomheter med virksomhetskoder i Østfoldundersøkelsen.

Gitt sparekravet er det svært mye på denne listen som ikke kan prioriteres, for eksempel radiobasert samband, mobiltelefoni, kloakkrensing, trykket presse, skoler, trafikkstyring, mm.

Hvem som var beslutningstager med hensyn til denne type prioritering varierte. I de fleste tilfeller kan og bør Fylkesmannen foreta prinsipielle prioriteringer i en krisesituasjon. Dette gjelder imidlertid ikke beslutning om frakobling av kraftkrevende industri, som må tas på høyere politisk nivå. Abel opplevde imidlertid at han selv i praksis måtte foreta prinsipielle og politiske vurderinger, i mangel på tilstrekkelige retningslinjer for dette.

Praktiske prioriteringer i en rasjoneringssituasjon kunne og kan bare foretas på driftssentral, med ut- og innkoblinger av fjernstyrte brytere på såkalte avganger fra trafostasjoner (i praksis gjelder dette sekundærstasjoner som er laveste nivå med fjernstyring). Med praktiske prioriteringer

menes hvilke konkrete kunder (i praksis: avganger) som får strøm, og når. Til støtte for dette formålet utarbeidet Abel en rekke rasjoneringsprofiler tilpasset strømkundene i området (f.eks. vil næringsområder primært få strøm i arbeidstiden) for de som kunne prioriteres av kategoriene ovenfor, det vil si tidsskjemaer for inn- og utkobling, med hensyn til det som er fysisk mulig innenfor den lokale nettarkitekturen i det aktuelle området. Boligmassen er et element som ikke er nevnt i listen, men som ble gitt egne rasjoneringsprofiler, og hensynet til boligmassen kunne gjerne bli ivaretatt ved at de ble gratispassasjerer sammen med samfunnsviktige funksjoner. Dessuten ble det foretatt vurderinger i forhold til om rasjonering på enkelte punkter kostet mer enn det smakte. Virksomheter med nødstrøm ble prioritert noe ned. En flaskehals for praktisk gjennomføring var tilstrekkelig driftspersonale på driftssentralene. Sluttproduktet for prioriteringen ble skriftlige koblingsordrer for de enkelte trafostasjonene som konkret anga når strømmen skulle kobles inn, ut og når.

I tillegg til rasjonering fant Abel ut at det må gjennomføres diverse tilpasningstiltak i hele samfunnet. Eksempelvis må det innføres graveforbud for å hindre skader på ledningsnett, fartøyer må holdes igjen når fyr er slukket og visuell navigasjon ikke er mulig, desentralisert virksomhet må konsentreres og så videre. Dessuten må forbrukere få beskjed om å slå av elektriske apparater ved strømbrudd, slik at ikke alt slås på igjen samtidig ved innkobling. Det vil medføre at trafoavgangen overbelastes med nytt strømbrudd som følge.

Abel regner med at det under gunstige forhold, og med utgangspunkt i Østfoldundersøkelsens resultater, vil ta fra to til tre uker å utvikle en praktisk prioritering med rasjoneringsprofiler etter at en grunnleggende kartlegging av samfunnsviktige funksjoner er foretatt. Videre regner han med at de fleste fylker vil falle ut likt som Østfold. Etter at man har vært gjennom kartleggingsprosessen, vil det dessuten være mulig å sette opp ”tommelfingerregler” for praktisk gjennomføring. Et eksempel på en slik regel er at ett sykehjem i drift dekker en befolkning på om lag 50 000 personer.

Et alternativ til sonevis roterende utkobling som beskrevet ovenfor, er kvoterasjonering. Det vil si at forbrukerne tildeles kvoter basert på tidligere forbruksmønster og at noen grunnleggende regler følges, for eksempel med hensyn til minimums og maksimums tildelt kvote. Videre at det betales en avskrekkende straffeavgift ved overforbruk. Dette vil kreve hyppige måleravlesninger, for eksempel hver uke, men datasystemene for strømregningen slik de er i dag vil ikke kunne håndtere dette.

En hovederfaring fra prosessen, var at den var iterativ. Man måtte lære underveis.

6.14 Kartlegging av sårbarheter i samferdselssektoren – SAMROS[105]

Samferdelsesdepartementet ønsket med SAMROS-prosjektet å kartlegge sårbarheter og gjensidige avhengigheter i samferdselssektoren. SINTEF ble gitt i oppdrag å produsere et

[105] Delkapittelet om SAMROS baserer seg på intervju med Anders Hovdum, Samferdselsdepartementet, 24. oktober 2006.

teorigrunnlag for kartleggingen.[106]

SINTEFs la til grunn standarden IEC60300-3-9 for risikoanalyse.[107] Metoden ble modifisert ved at det ble lagt større vekt på konsekvens enn på sannsynlighet.[108] Vektleggingen ble gjort for å sikre at diskusjonene i størst mulig grad skulle handle om sårbarhet i sektorens infrastruktur, og ikke trusler mot sektorens infrastruktur. SINTEFs deltagelse i prosjektet ble sluttført høsten 2005, og DNV overtok den praktiske tilretteleggelsen av den videre prosessen. Sluttrapport vil foreligge tidlig 2007.

SAMROS har vært og er en iterativ prosess. Datagrunnlaget og vurderingene rundt disse er i hovedsak fremarbeidet av departementets underlagte etater og virksomheter. På den måten har departementet, etatene og virksomhetene fått nærhet til informasjon om sektorens infrastruktur. Arbeidsgruppens medlemmer er i hovedsak personell med infrastrukturkompetanse. Nasjonal sikkerhetsmyndighet har i tillegg deltatt i sluttføringen av prosjektet som faglig rådgiver på objektsikkerhet.

Prosjektet har fokus på sårbare objekter, fremføringsveier og hjelpesystemer. Det er i noen grad er tatt hensyn til avhengighetsforhold til infrastrukturer utenfor sektoren.

Departementets underlagte etater og virksomheter kartla i prosjektets innledende fase sårbare objekter, fremføringsveier og hjelpesystemer innen sitt ansvarsområde. Som en del av denne kartleggingen, ble etatene og virksomhetene bedt om å prioritere de ti mest kritiske *objektene, fremføringsveiene* og *hjelpesystemene*. I prosjektet er disse områdene omtalt som noder, eksempelvis Oslo-området som node, med vekt på sentraler og terminaler. Videre er *fremføringsveiene* mellom nodene vurdert. Det var ikke et krav at bortfall av noden skulle ha ringvirkninger på nasjonalt nivå.

Det ble høsten 2005 gjennomført et eget seminar for å gjennomgå og vurdere etatene og virksomhetenes prioriteringer. Rangeringsskalaen for "kritikalitet" (en kombinert rangering av risiko[109] og sårbarhet[110]) ble satt fra 1 til 6. Med dette som grunnlag ble kritikaliteten til objektene, hjelpesystemene og fremføringsveiene diskutert på tvers av samferdselsgrenene. På seminaret ble samtlige objekter rangert fra 1-6, og det ble utarbeidet en liste over de 10-15 mest kritiske objektene i hele samferdselssektoren, på tvers av veg, bane, luft og tele. Metoden var altså diskurs- og prosessbasert, med vekt på konsensusprosesser og forankring. Objektene ble deretter lagt inn i sine respektive geografiske noder for videre analyse av avhengighet.

Det ble lagt hovedvekt på uønskede hendelser av næringsmessig viktighet, og mindre vekt på rene trusselscenarier. Enkelte dilemmaer ble avdekket, for eksempel det at stor intern risiko for NSBs

[106] http://www.odin.no/filarkiv/265656/ROS.pdf
[107] IEC 60300-3-9. Dependability management - Part 3: Application guide - Section 9: Risk analysis of technological systems. 1995.
[108] Hokstad, Per. 2005. *Overordnet risiko- og sårbarhetsanalyse for samferdselssektoren*. SINTEF.
[109] Dvs et mål for sannsynlighet og konsekvens for en uønsket hendelse
[110] Dvs et mål for robust heten til et system

togdrift ikke nødvendigvis er en stor samfunnsrisiko, men at uønskede hendelser knyttet til dette kan gi risiko for permanente endringer i transportbruk av en type som ikke er politisk ønskelig.

Våren 2006 gjennomførte Veritas en rekke heldagsmøter med etatene og virksomhetene for å komplimentere oversikten over objektene med nødvendige data om sikkerhetsnivå, beredskapsløsninger og så videre. Det ble også vurdert ulike scenarier som kunne føre til at objektene eller fremføringslinjene ble satt ut av spill over lengre tid – for eksempel over 5 dager. I løpet av desember 2006 blir det avholdt et nytt seminar. Formålet er å avdekke gjensidig avhengighet mellom kartlagte samferdselsobjekter og fremføringslinjer, for produksjonen i den enkelte geografiske node eller for rikets sikkerhet. Objekter og fremføringslinjer som i den første prioriteringslisten ble rangert lavt kan være kritisk fordi enkelte allerede definerte kritiske objekt er avhengig av dem, enten som hjelpesystem eller som avlastingssystem ved beredskap. Det vil også søkes gjort ytterligere prioriteringer i den enkelte node, mellom de geografiske nodene, og mellom samferdselsgrenene.

I så fall vil SAMROS gå et skritt videre fra HelseROS, hvor slik prioritering ikke er foretatt. På bakgrunn av seminaret og tidligere innhentet informasjon, vil DNV produsere en sluttrapport i prosjektet. Rapporten vil bli oversendt til departementet tidlig i 2007. Den vil så danne grunnlag for et eget strategidokument. Strategidokumentet vil gi føringer for de tiltak som blir foreslått i neste St.prp nr. 1.

Et hovedinntrykk av prosessen er at den i begrenset grad er en faktisk ROS-analyse ”etter boka”, men i stor grad vil bli en kartlegging av antatte fremtidige sikkerhetsmessige utfordringer, og kanskje heller er en *Horizon Scanning*. Som i HelseROS og tilsvarende andre prosesser er sannsynlighetsbegrepet relativt lite vektlagt. Det er i SAMROS dikotomisert, det vil si slik at hendelser med antatt lav sannsynlighet eller plausibilitet er silt fra før den egentlige prosessen begynner. Bemerk at det i HelseROS eksplisitt påstås at vanlig metodikk for ROS-analyse ikke er egnet for ROS-vurdering på samfunnsnivå (politisk ROS-vurdering). Preliminært synes dette argumentet å ha noe for seg, og synes å underbygges av empiri.

6.15 Prioritering i Kredittilsynet[111]

Grunnlaget for prioritering av Kredittilsynets virksomhet, inklusive tilsyn på IKT-området, er, som normalt i staten, prosessen i forbindelse med tildelingsbrevet og utarbeidelse av en virksomhetsplan. I forbindelse med virksomhetsplanleggingen foretas det en analyseprosess med innheting av data og prioritering av tiltak. Til grunn for tilsynsvirksomheten ligger prinsippet om risikobasert tilsyn. Basert på tilgjengelige erfaringsdata foretas det en såkalt SRV, Samlet Risiko Vurdering, i forhold til potensielle tilsynsobjekter. Erfaringer fra gjennomførte tilsyn, reelle hendelser, kunnskaper om endringer i bransjen og annen tilgjengelig informasjon vurderes under et og munner ut i et utvalg av virksomheter som det planlegges tilsyn overfor. I tillegg plukkes en del virksomheter ut etter et random-prinsipp for å sikre muligheten for å oppdage uventet risiko.

[111] Delkapittelet baserer seg på intervju med Frank Robert Berg, Stig Ulstein og Åshild Johnsen, Kredittilsynet, 23. juni 2006.

Et vesentlig kriterium for utvalg av tilsynsobjekt er ellers en forventning om at det utfører en tidskritisk tjeneste. Dette fører til at de store og viktige aktørene er garantert årlige tilsynsbesøk, mens mindre viktige eller random-utplukkede virksomheter besøkes sjeldnere. Et performance-kriterium for Kredittilsynets IKT-tilsyn er at det gjennomføres om lag 30 tilsyn pr år.

Grunnlaget for tilsynsvirksomheten på dette området kan føres tilbake til den såkalte Baselkomiteen (Basel 2), som er en sammenslutning av forskjellige nasjoners tilsynsmyndigheter på området. Innenfor Basel 2 utvikles og vedlikeholdes den såkalte CobIT-standarden. Tilsvarende standard er inkorporert i EUs Acquis[112] og er på normal måte introdusert i norsk lovgivning gjennom EØS-avtalen. Relevant norsk lovgivning er i hovedsak Kredittilsynsloven med tilhørende forskrifter. Det stilles her krav til ROS-analyse/-vurdering/-prosess i den enkelte relevante virksomheten. Det legges vekt på såkalt operasjonell risiko, definert som: "risiko for tap som følge av utilstrekkelige eller sviktende interne prosesser eller systemer, menneskelige feil eller eksterne hendelser". Videre legges det vekt på økonomisk konsekvens. Forventninger til operasjonell risikostyring legger særlig vekt på:

- Identifisering og vurdering av faktorer som påvirker operasjonell risiko
- Evne og vilje til å etablere kontrolltiltak for forsvarlig håndtering av risikoen
- Evne til forsvarlig å gjennomføre disse
- Logg og evaluering av uønskede hendelser

Rammeverket for CobIT som den brukes av Kredittilsynet, er en liste på om lag 170 spørsmål som stilles til alle relevante virksomheter en gang årlig. Denne datainnsamlingen er en vesentlig del av det datatilsiget som er nevnt ovenfor, men brukes ikke direkte som en prioriteringsmekanisme eller screening for å prioritere tilsyn, tiltak eller tema for egen ROS-rapport. Spørsmålene er videre delt opp i enklere og mer saksspesifikke lister (om lag 10) etter horisontale og vertikale dimensjoner eller temaer.

CobIT egner seg for å etablere horisontal 360° oversikt. CobIT er prosessorientert og er til nå den viktigste metoden for Kredittilsynets IKT-tilsynsenhet. Bruken av CobIT videreutvikles i tematiske versjoner som nevnt. Dette kan være hvitvaskingsproblematikk, virus, brannmurberedskap med mer. CobIT er funnet å være den mest hensiktsmessige standarden for formålet, og egner seg betydelig bedre enn for eksempel ISO-standarder som (forhenværende) ISO17799. I tillegg er det gjort forsøk med såkalt transaksjonstesting, det vil si å følge livsløpet til bestemte transaksjoner. Andre standarder (f eks ITIL – IT Infrastructure Library) egner seg bedre til andre formål, for eksempel "dypdykk" innen en virksomhet.

7 Avslutning og Oppsummering

Samfunnets endringstakt, avhengighet og sårbarhet skaper i ulike sammenhenger behov for en

[112] Acquis (Communautaire), dsv EUs samlede (fr. acquis = eng. acquired, no. samlet) lovgivning til dags dato; for tiden delt i 35 kapitler, hvorav kapittel 32 inneholder direktiver vedrørende finansnæringen.

metode for å identifisere og rangere hva som er mest kritisk for samfunnet. Denne studien har vist til aktuelle metoder, kriterier, teori og begreper som er relevante i utarbeidelsen av en norsk metode.

Et hovedinntrykk er at det ikke er produsert en helhetlig metodikk for rangering av samfunnsfunksjoner og kritisk infrastruktur som er tatt i bruk av de lands myndigheter som studien har tatt for seg. Det er i alle tilfeller ikke funnet noen metodikk som faller helt sammen med målsettingen i BAS5-prosjektet. Det eksisterer likevel mye metodikk som kan relateres til denne problemstillingen, for eksempel for analyse av gjensidige avhengigheter og nasjonale ROS-vurderinger. I enkelte tilfeller er eksisterende metodikk nylig utgitt og ikke utprøvd, som for eksempel svenskenes metodikk for identifisering av samfunnsfunksjoner og danskenes metodikk for nasjonal ROS-analyse.

Samtidig har denne studien vist at det eksisterer mange kriterier med potensial for å bli benyttet i en metode. Det er også vist at enkelte teorier kan brukes som kriterier. Det fremstår derfor som en utfordring å omsette dette til en norsk metode som er enkel å bruke og forstå, og som i størst mulig grad gjenspeiler virkeligheten. I metoderapporten er dette forsøkt gjort.[113]

Utformingen av en metode må også ta hensyn til hvem som skal bruke den. Er det den enkelte virksomhet, de enkelte sektormyndigheter eller en myndighet med tverrsektorielle interesser som DSB og NSM eller forskningsinstitusjoner som FFI, UiS og SINTEF? Det kan tenkes at selv en enkel metode er for vanskelig å bruke for aktører som ikke er vant til å tenke tverrsektorielt. Det reiser også spørsmål om den skal vedlikeholdes og eventuelt av hvem?

Det må også tas hensyn til hva man ønsker at metoden skal gi svar på. Skal den produsere en ”autoritativ” rangert liste over hvilke funksjoner som er mest kritiske for samfunnet, skal den brukes av den enkelte virksomhet som en egenevaluering av hvor kritisk egen virksomhet er for samfunnet, eller skal den fungere som et utgangspunkt for konkrete oppdrag? Eksempelvis kan man tenke seg at en sektormyndighet henvender seg til ”metodeforvalteren” med et oppdrag om å identifisere samfunnets mest kritiske objekter, eller kanskje en liste over sektorens mest kritiske virksomheter?

Det kan også tenkes at metoden ikke gir endelige svar, men at resultater må justeres i samråd med sektoreksperter. Man kan lett forestille store forskjeller mellom eksempelvis en oversikt over prioriterte brukere av mobilnettet, og prioriterte mottagere av vaksine ved en pandemi. En metode må ha rom for å ta opp i seg slike forskjeller, for eksempel ved å inngå samtaler med sektoreksperter.

En metode må også legge opp til åpenhet om hvordan et resultat er produsert. Det vil gjøre det enklere å få et resultat som er tilpasset det spesifikke behovet. Det gjør det også enklere å få tilbakemeldinger på selve metoden, for justeringer etter hvert som man høster erfaring med den.

[113] Henriksen, Stein. Sørli, Kjetil. Bogen, Lene. 2007. Metode for identifisering og rangering av kritiske samfunnsfunksjoner. FFI/RAPPORT-2007/00874

Litteraturliste

Amici, Stefano et.al. 2005. *Network Security in Critical Infrastructures*. Istituto Superiore delle Comunicazionie delle Tecnologie dell'Informazione (ISCOM) 2005.

Antón, Phillip S. et al. 2003. *The The Vulnerability Assessement & Mitigation Methodology. Finding and Fixing Vulnerabilities in Informasjons Systems.*Rand National Defense Research Institute.

Audestad, J. 2005. *E-bomber og e-granater – om IKT og sårbarhet*. FFI/NOTAT-2005/00938.

Aven, Terje. 2003. *Foundations of Risk Analysis. A Knowledge and Decision-Oriented Perspective*. John Wiley & Sons, Ltd 2003.

Aven, Terje. Boyesen, Marit. Njå, Ove. Olsen, Kjell Harald. Sandve, Kjell. 2004. *Samfunnssikkerhet*. Universitetsforlaget.

Avon and Somerset Local Resilience Forum. 2006. *Community Risk Register*. Version 2.1 January 2006.

Beck, Ulrich. 1986. *Risikogesellschaft: Auf dem Weg in eine andere Moderne*. Suhrkamp Verlag, Frankfurt am Main. Engelsk utgave: Beck, Ulrich. 1992. *Risk Society: Towards a New Modernity*. Sage Publ. 1992.

Beredskapsstyrelsen. 2004. *National Sårbarhedsudredning*. Udvalget for National Sårbarhedsudredning.

Beredskapsstyrelsen. 2005. *ROS-modellen. Beredskabsstyrelsens model for risiko- og sårbarhedsanalyse af samfundets kritiske funktioner*.

Bjørgo, Tore. 2003. *Norske dammer – i hvilken grad er de sannsynlige terror- og sabotasjemål*. Revidert utgave april 2003. NUPI.

Commision of the European Comunities 2005. *Green Paper on a European Programme for Critical Infrastructure Protection*. Brussels, 17.11.2005. COM (2005) 576 final.

Communication from the Commission to the Council and the European Parliament. COM (2004) 702 final. *Critical Infrastructure Protection in the fight against terrorism*. Brussels. 20.10.2004.

Council of the European Union. 2004. *Prevention, Preparedness and Response to Terrorist Attacks* og *EU solidarity Programme on the Consequences of Terrorist Threats and Attacks.*

Departement of Homeland Security. 2003. Homeland Security Presidential Directive (HSPD)-7 2003. *Critical Infrastructure Identification, Prioritization, and Protection*.

Departement of Homeland Security. 2006. Draft NIPP v.2.0 2006.

Donzelli, Paolo. Setola, Roberto .2005. *Identifying and Evaluating Risks related to External Dipendencies: A Practical Goal Driven Risk Analysis Framework.*

Donzelli, Paolo. Setola, Roberto og Tucci, Salvatore. 2004. *Identifying and Evaluating Critical Infrastructures- A Goal Driven Dependability Analysis Framework - Communications in Computing.*

EAPC(CCPC)D(2003)0007-REV1. 26 april 2004. *Policy on the implementation of the international emergency preference scheme in the EAPC area*.

Federal Emergency Management Agency Strategic Plan, Fiscal Years 2003 – 2008. *A Nation Prepared.*

Federal Ministry of the Interior. 2005. *Protection of Critical Infrastructures – Baseline Protection Concept. Recommendation for Companies.* Germany 2005.

Føli, Anja Elisabeth 2006. Hovedoppgave: *Utvikling av verktøy for evaluering av risiko- og sårbarhetsanalyser*. Universitetet i Stavanger 22. juni 2006.

Försvarsministeriet, Finland. 2003. *Strategi för tryggande av samhällets livsviktiga funktioner*. Statsrådets principbeslut 27.11.2003.

Fridheim, Håvard. Betten, Stian. Hagen, Janne M. Henriksen, Stein. Rodal, Gry Hege. Rodal, Siv Kjersti. Rutledal Frode. 2001. *Sårbarhetsreduserende tiltak i kraftforsyningen – Sluttrapport*. FFI/RAPPORT – 2001/02383 (Begrenset).

Fridheim, Håvard. Hæsken Ole Morten. Olsen Thor Gunnar. Balke, T, Ensrud May-Kristin. 1997. *Viktige samfunnsfunksjoner*. FFI/RAPPORT-97/01458 (Begrenset).

Hæsken, Ole Morten. Olsen, Thor Gunnar. Fridheim, Håvard. 1997. *Beskyttelse av samfunnet (BAS) – Sluttrapport.* FFI/RAPPORT-97/01459.

Hagen, Janne M. Rodal, Gry Hege. Hoff, Erlend. Lia, Brynjar. Torp, Jan Erik. Gulichsen, Steinar. 2003. *Beskyttelse av samfunnet med fokus på transportsektoren.* FFI/RAPPORT-2003/00929.

Hellevik, Ottar. Forskningsmetode i sosiologi og statsvitenskap. 5. utgave, 2. opplag 1993. Universitetsforlaget.

Henriksen, Stein. 2004. Ikke utgitt manus *NSBR04*. Direktoratet for samfunnssikkerhet og beredskap.

Henriksen, Stein. Sørli, Kjetil. Bogen, Lene. 2007. Metode for identifisering og rangering av kritiske samfunnsfunksjoner. FFI/RAPPORT-2007/00874.

HM Government (Udatert). *Emergency Preparedness. Guidance on Part 1 of the Civil Contingencies Act 2004, its associated Regulations and non-statutory arrangements*.

Hokstad, Per. 2005. *Overordnet risiko- og sårbarhetsanalyse for samferdselssektoren*. SINTEF.

Hokstad, Per. Jersin, Erik. Rossnes, Ragnar. Steiro, Trygve. Tinmannsvik, Ranveig K. 2002. *Risiko på tvers (RPT). Gjennomgående og helhetlig strategi for risikovurdering på HMS-område*t. SINTEF Rapport STF38 A01435.

IEC 60300-3-9. Dependability management - Part 3: Application guide - Section 9: *Risk analysis of technological systems*. 1995.

International Telefommunication Union (ITU). E.106 (03/2000). *Description of an international emergency preference scheme IEPS*; ITU er FNs spesialistorgan for telekommunikasjon.

Klinke & Renn. 2002. *A New Approach to Risk Evaluation and Management: Risk-based, Precaution-based, and Discourse-based Strategies*.

Lewerentz, Birgitta. Frost, Christina. Marklund, Anna. Franzén, Göran. Wahlberg, Maria. Ånäs, Per. 2005. *Kriteriemodell för identifiering av samhällsviktiga verksamheter och system.* FOI Memo 1283. Totalförsvarets forskningsinstitut.

Mærli, Morten Bremer. 2004. *Crude Nukes on the Loose?* Unipub AS 2004.

Ministry of the Interior and Kingdom Relations. 2003. *Critical Infrastructure Protection in the Netherlands.*

Ministry of the Interior and Kingdom Relations. 2004. *Critical Infrastructure Protection in the Netherlands. The Dutch approach on CIP*.

Moteff, John and Parformak, Paul. 2004. *Critical Infrastructure and Key Assets: Definition and Identification.* CRS Report for Congress.

National Council for Civil Emergency Planning (NCCEP. Planeamenta Civil de Emergência). 2005. *Critical Infrastructure Protection in Portugal – Ranking Critical Infrastructures – the Portuguese Methodology*.

National Council for Civil Emergency Planning (NCCEP. Planeamenta Civil de Emergência) 2005. *Critical Infrastructure Protection in Portugal – Workplan 2003-2007*.

NOU 2000:24. *Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*.

NOU 2006:6. *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner.*
OECD. 2003. *Emerging risks in the 21st century*. An OECD international futures project.

Office of Critical Infrastructure Protection and Emergency Preparedness. 2002. *Draft. Tool to Assist Owners and Operators to Identify Critical Infrastructure Assets*.

Office of Homeland Security. 2002. *National Strategy for Homeland Security*.

Office of Public Sector Information.2004. *Civil Contingencies Act 2004*.

Perrow, Charles. 1999. *Normal Accidents. Living with High-Risk Technologies*. Princeton University Press.

Krisberedskapsmyndigheten.2003. Planeringsprocessen. 2003:7. *Samhällets krisberedskap 2005. Planeringsinriktning.* Krisberedskapsmyndigheten.

Post- og teletilsynet. 2003. *Risiko og sårbarhetsanalyse av mobilnettene i Norge*. Saksnummer: 200205841. (Unntatt off i.h.t. offentlighetsloven § 6.1. ledd nr. 1).

Public Safety and Emergency Preparedness Canada. 2003. National Critical Infrastructure Assurance Program. *An Assessment of Canada's National Critical Infrastructure Sectors*. July 2003.

Public Safety and Emergency Preparedness Canada. 2004. *National Critical Infrastructure Assurance Program. Selection Criteria to Identify and Rank Critical Infrastructure Assets*. 20 January 2004.

Schneier, Bruce. 2003. *Beyond Fear. Thinking Sensibly about Security in an Uncertain World*. Copernicus Books.

Sosial- og helsedirektoratet. 2005. *Nasjonal ROS- og beredskapsanalyse innen helse*. Hovedrapport. Dok. nr. ST-25459-RA-15-Rev03. Juni 2005.

St.meld. nr. 39 (2003–2004). *Samfunnssikkerhet og sivilt-militært samarbeid*.

St.meld. Nr. 47 (2000-2001). *Telesikkerhet og –beredskap i et telemarked med fri konkurranse*.

St.prp. nr. 42 (2003–2004). *Den videre moderniseringen av Forsvaret i perioden 2005–2008*.

UK Resilience internettside mai 2006. *Introduction to the Civil Contingencies Secretariat*. http://www.ukresilience.info/ccs/index.shtm .

Unisys Belgium. 2005. *Survey to Assess Risk Preparedness in European businesses*. Done for the European Commission and The European Network and Information Security Agency.

US Senate. 2001. *US Patriot Act of 2001*. H.R. 3162.

Vinje, Finn-Erik 2005. *Sikkerhet – Safety/Security. En begrepsutredning* – i NOU 2006:6. *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastruktur og kritiske samfunnsfunksjoner*.