Metode for identifisering og rangering av kritiske samfunnsfunksjoner

Stein Henriksen, Kjetil Sørli og Lene Bogen

Forsvarets forskningsinstitutt/Norwegian Defence Research Establishment (FFI)

23. mars 2007

FFI-rapport 2007/00874

1014

ISBN 978-82-464-1192-7

Emneord

Kritisk infrastruktur

Samfunnsfunksjoner

Risikoanalyse

Beslutningsstøtte

IKT

Godkjent av

Håvard Fridheim	Prosjektleder
Jan Erik Torp	Avdelingssjef

Sammendrag

Prioritering av samfunnskritiske funksjoner og virksomheter er en politisk og ikke en teknokratisk prosess. Blind anvendelse av en metodikk til dette formålet er derfor lite hensiktsmessig – det må være klart hva prioriteringen skal anvendes til og hvilke ulike hensyn som skal tas i ulike prioriteringssituasjoner. Eksempler på beredskapsproblemstillinger med behov for prioritering er utpeking av nøkkelobjekter som beskyttes av militære styrker i en krisesituasjon, klassifisering kritiske infrastrukturer for å avklare hvilke som skal underlegges de hardeste sikkerhetskravene, og utpeking av sektorer som skal prioriteres med vaksiner i tilfelle en pandemi. Muligheten for prioritering er også et vesentlig aspekt av en nasjonal tverrsektoriell ROS-vurdering, hvor ulike sektorer, virksomheter eller til og med personer og stillinger kan ses mot hverandre.

Prioriteringsproblematikken knyttet til IKT kan ikke bare inkludere IKT-systemene i seg selv, men må også inkludere brukerne som er avhengige av systemene. BAS5 har derfor utviklet en metode for identifisering og rangering av alle kritiske samfunnsfunksjoner, herunder alle kritiske infrastrukturer, og ikke bare kritiske IKT-systemer. Prosjektet har videre beskrevet et system for beslutningsstøtte, og ikke et system for automatisk prioritering. Dette betyr at relevante beslutningsmiljøer må involveres i bruken av metoden.

I BAS5-prosjektet er ulike samfunnsfunksjoners kritikalitet knyttet til sårbarheten overfor ulike hendelser som kan ramme dem, i tillegg til betraktninger om deres vesentlighet eller viktighet for samfunnet. Det er derfor knapt mulig å prioritere kritiske samfunnsfunksjoner uten samtidig å gjøre seg opp en grunnleggende mening om hvilke risiko de er utsatt for eller utsetter andre for. Det vil si at det må forutsettes at det foretas risiko- og sårbarhetsvurdering (ROS-vurdering) på sektor- og virksomhetsnivå.

Metoden som er utviklet beskriver hovedtrekkene for beslutningstøtte i situasjoner hvor det kan være nødvendig å prioritere mellom forskjellige kritiske samfunnsfunksjoner. Metoden er risikobasert, og inneholder to hovedaspekter. Det utvikles og forankres en permanent løpende prosess som involverer ansvarlige departementer og alle andre som har ansvar og kunnskap innen egen sektorer. Til støtte for denne prosessen brukes en teknikk som er ROS-basert, da antagelser om kritikalitet bør forutgås av nærmere analyse og vurdering

Prosessen krever at ”noen” pekes ut til å samordne den på nasjonalt nivå, på tvers av ansvarsgrenser, at det ordinære ansvarsprinsippet utnyttes for å strukturere arbeidet, at det etableres tverrsektorielle felles prosedyrer, inklusive permanente fora med tett møtefrekvens og at det etableres tverrsektorielle standarder. Konkret valg av metodikk for ROS-analyse er overlatt til den enkelte sektor eller virksomhet, tilpasset dennes forutsetninger. Innrapportering av resultater fra ROS-analyse skal derimot foretas i et rigid standardisert format. Det forutsettes at det utvikles en enkel standard database for å håndtere informasjon på tvers av virksomheter og samfunnssektorer.

English summary

Making priorities about societal critical functions and entities is a political and not a technocratic process. The blind usage of a methodology does not meet the purpose – there must also be clear ideas about the purpose of priority and what other concerns that may have to be considered in different situations. The following are some examples of emergency planning problems that highlight the need for priorities: determining key assets to be protected by military forces in a crisis situation, classifying critical infrastructures to determine levels of security, and determining priority for vaccines during a pandemic. Making priorities possible is also a significant aspect of a national cross sector risk assessment, juxtapositioning sectors, entities, or even persons and positions.

The problem of prioritising relative to ICT must not only include the ICT systems themselves, but also users that depend upon them. BAS5 has developed a method for the identification and ranking of all critical functions of society, not only critical ICT systems. Furthermore, the project has described a system for decision support, and not a system for making automatic priorities. This means that relevant decision making environments have to be involved in the use of the method.

In the BAS5 project, the criticality of various sectors of society is related to vulnerabilities derived from various events that might befall them, in addition to thoughts about their significance or importance to society. It is therefore hardly possible to prioritise the critical functions of society without, at the same time, making up one's mind about the risks that they are subjected to or subject others to. That means that risk assessments must be assumed to be performed at sector and entity levels.

The developed method describes a system for decision support for situations that make prioritising between various critical societal functions necessary. The method is risk based, and contains two main aspects. Firstly, a permanent and ongoing process between ministries and others with responsibilities within their own sectors is established. Secondly and to support this process, a risk assessment based technique is applied, as assumptions about criticality should be preceded by some analysis and assessment.

The process requires that "somebody" is appointed as coordinator at national level and across sectors, that the normal principle of sector responsibility is exploited to structure the work, that cross-sectoral common procedures are implemented, including the establishment of permanent fora meeting frequently, and the establishment of cross-sectoral standards. The choice of risk assessment methodologies should be left to sectors and entities, adapted to their particular circumstances. The reporting of results from risk assessments should however be subjected to a rigidly standardised format. It will also be necessary to develop a simple standard database for the management of cross-sectoral information.

Innhold

1 Innledning

Denne rapporten beskriver hovedtrekkene i en metode for beslutningstøtte for situasjoner hvor det kan være nødvendig å prioritere mellom forskjellige kritiske samfunnsfunksjoner. Rapporten er skrevet i forbindelse med prosjektet "Beskyttelse av samfunnet 5".

Det er lagt vekt på at rapporten skal være relativt kortfattet. Rapporten inneholder derfor ikke drøfting av bakgrunnsmateriale eller forskjellige løsningsalternativer. Bakgrunnsmateriale er behandlet i en egen rapport.[1] Her er det lagt vekt på å fremstille én valgt løsning som etter forfatternes mening er den løsningen som vil føre frem. Det understrekes at metoden ikke er testet, men at den er sondert mot akademiske og administrative miljøer. Det vil bli vurdert å teste metoden senere som et ledd i eventuelt å få den administrativt forankret.

Metoden er risikobasert. Det kan i denne sammenhengen vises til politiske målsetninger slik de er fremlagt i Stortingsmelding 39 (2003-2004), Samfunnssikkerhet og sivilt-militært samarbeid:

> Sikkerhets- og beredskapsarbeidet skal organiseres slik at det oppnås en best mulig ressursbruk og et godt samvirke på tvers av sektorer. **Analyser av risiko- og sårbarhetsforhold og samordnede sikkerhetskrav er viktige virkemidler for å oppnå en slik helhet.** Ikke minst er det nødvendig å se til at sikkerhets- og beredskapstiltak ikke bare er planlagte, men at de også kan gjennomføres og at de som berøres kjenner til rutiner og tiltak. De enkelte tilsynsmyndigheter har ansvar for å føre tilsyn innenfor sine fagfelt og sektorer. **I tillegg er det behov for å se spesifikt på sikkerhets- og beredskapsarbeidet på tvers av sektorer, spesielt rettet mot samfunnskritiske infrastrukturer og funksjoner.** Uansett hvilket nivå krisen håndteres på skal ansvarlige myndigheter og aktører sørge for at befolkningen opplever størst mulig grad av trygghet.
>
> **Vurderinger om risiko legger grunnlag for prioriteringer i samfunnssikkerhetsarbeidet.** Risiko beregnes ut fra sannsynligheten for at en hendelse inntreffer i forhold til hvor alvorlige konsekvensene blir i tilfelle en slik hendelse inntreffer. Både hendelser med høy sannsynlighet og mindre konsekvenser, for eksempel trafikkulykker, og hendelser med lav sannsynlighet, men antatt alvorlige konsekvenser, eksempelvis alvorlige atomhendelser, kan sies å innebære en stor risiko.[2]

Det kan også vises til at de tilsyn som gjennomføres i henhold til Kgl. res. av 3. november 2000, Instruks om innføring av internkontroll og systemrettet tilsyn med det sivile beredskapsarbeidet i departementene, etterspør risiko- og sårbarhetsvurderinger.

[1] SØRLI Kjetil, HENRIKSEN Stein, BOGEN Lene, MØRKESTØL Kristin. 2007. Bakgrunnsstudie til metode for rangering og identifisering av kritiske samfunnsfunksjoner. FFI/RAPPORT-2007/00875

[2] St.meld. nr. 39 (2003-2004) *Samfunnssikkerhet og sivilt-militært samarbeid*. Uthevingene i sitatene er gjort av forfatterne.

2 Bakgrunn

2.1 Om BAS-prosjektene

Siden 1994 har Forsvarets forskningsinstitutt (FFI) gjennomført forskning med relevans for kritiske samfunnsfunksjoner og infrastrukturer, hovedsaklig i forskningsserien ”Beskyttelse av samfunnet” (BAS). Dette har vært gjennomført i samarbeid mellom FFI, Justis- og politidepartementet og det tidligere Direktoratet for sivilt beredskap (DSB), som fra 1. september 2003 inngikk i Direktoratet for samfunnssikkerhet og beredskap (også DSB).

Forskningen har tatt for seg sårbarheter i telekommunikasjoner (BAS2), kraftforsyning (BAS3) og transport (BAS4). I tillegg har FFI deltatt i en studie av sårbarhet i vannforsyningen (SIV) og andre konkrete oppdrag med hensyn til analyse av risiko og sårbarheter i forskjellige samfunnsfunksjoner. Fokus har vært på fysiske sårbarheter, men man har merket seg at det også fins betydelige sårbarheter knyttet til informasjonssystemer. Informasjonssystemer er ofte kritiske for funksjonen til de fysiske og organisatoriske systemene de er satt inn i og delvis styrer. Kritiske *informasjons*infrastruktur er derfor sett på som en egen kategori kritisk infrastruktur og studeres i prosjektet BAS5 – Sårbarhet i kritiske IKT-systemer. FFI har administrativ ledelse for prosjektet, som i tillegg til DSB og Nasjonal sikkerhetsmyndighet (NSM) samler deltakere fra flere akademiske institusjoner, departementer, direktorater og virksomheter.

2.2 Problemstilling og målsetning

Målsettingen for BAS5 er gitt i prosjektbeskrivelsen, hvor hovedmålet er å utvikle metodikker for analyse av infrastrukturer som er avhengige av informasjons- og kommunikasjonsteknologi (IKT), med særskilt fokus på systemer og infrastrukturer som er kritiske for det moderne samfunnet. Prosjektet har tre delmål:

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**

Målsettingen for denne rapporten fremgår særlig av siste delmål.

2.3 Avgrensinger og anvendelsesområder

Begrepet ” kritiske systemer og sektorer som er avhengige av IKT ” lar seg vanskelig avgrense. IKT-systemer er blitt allestedsnærværende som hjelpesystemer for alle kritiske samfunnsfunksjoner. Denne rapporten vil derfor beskrive en metode for en identifisering og rangering av alle kritiske samfunnsfunksjoner, herunder alle kritiske infrastrukturer, ikke bare kritiske *informasjons*infrastrukturer. Det er her valgt å bruke følgende strukturerende begreper:

- Kritiske samfunnsfunksjoner
    - Kritisk infrastruktur
        - Grunnleggende; i praksis elektrisk kraft og telekommunikasjon
        - Øvrige; i praksis vann og avløp, olje- og gassforsyning, transport, og bank og finans
    - Andre kritiske samfunnsfunksjoner

Denne strukturingen er basert på det skillet som er etablert mellom kritiske infrastrukturer og andre kritiske samfunnsfunksjoner i Infrastrukturutvalgets rapport[3].

En prinsipiell *identifisering* av hva som for vårt formål inngår i disse kategoriene er gjort i kapittel 5.2. Det er ikke spesielt vanskelig å identifisere hva som prinsipielt sett utgjør kritiske samfunnsfunksjoner ut fra nærmest intuitive betraktninger. Konkret og strukturert identifisering av et stort antall relevante anlegg, installasjoner, institusjoner og virksomheter utgjør imidlertid et større og mer ressurskrevende detektivarbeid. Et eksempel på et slikt arbeid er den såkalte Østfoldundersøkelsen, som gikk ut på å identifisere hvilke virksomheter som skal få kraft ved kraftrasjonering.[4]

I henhold til ordboka betyr *rangere* å plassere i rangorden (høy – lav) og å ordne i en bestemt rekkefølge. Denne rekkefølgen kan være prioritert. *Prioritere* vil si å sette opp i rangorden og gi noe eller noen i denne ordenen fortrinn fremfor andre. Vi tolker oppdraget slik at mulighet for prioritering er ønskelig, jf også sitat fra St.meld. 39 i kapittel 1. Dette er ikke en banal oppgave. Prioritering er en politisk og ikke en teknokratisk prosess.

Denne rapporten beskriver derfor et system for beslutningsstøtte, ikke et system for automatisk prioritering.

Dette betyr at relevante beslutningsmiljøer må involveres i bruken av metoden. Arbeidet kan ikke outsources til ekspertmiljøer, selv om disse med fordel kan delta i prosessen.

Det må formodes at samfunnsfunksjonens eventuelle kritikalitet er knyttet til sårbarhet i forhold til potensielle risikohendelser som kan ramme den, i tillegg til betraktninger om dens vesentlighet eller viktighet. *Det er derfor knapt mulig å prioritere kritiske samfunnsfunksjoner uten samtidig å gjøre seg opp en grunnleggende mening om hvilke risikoer og sårbarheter de er utsatt for eller utsetter andre for;* det vil si at det må forutsettes at det foretas risiko- og sårbarhetsvurdering (ROS-vurdering) på sektor- og virksomhetsnivå. Dette bør involvere realkompetansen innen hver sektor. Ved tverrfaglige utfordringer av den typen som inngår i den foreslåtte metoden må det

[3] NOU 2006:6 *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner.*

[4] Abel, Carl Georg. 2003. Utkast: *Beskrivelse: Planlegging og gjennomføring av roterende sonevis utkobling*; Abel, Carl Georg. 2003 Utkast: *Kvoterasjonering*; Abel, Carl Georg. 2003. Utkast: *Problemstillinger og samfunnskonsekvenser ved strømutkobling*. Se også SØRLI Kjetil, HENRIKSEN Stein, BOGEN Lene, MØRKESTØL Kristin. 2007. Bakgrunnsstudie til metode for rangering og identifisering av kritiske samfunnsfunksjoner. FFI/RAPPORT-2007/00875.

unngås at én sektor ”synser” på vegne av en annen sektor. En slik praksis ville ikke være i samsvar med det såkalte ansvarsprinsippet som ligger til grunn for offentlig forvaltning, med forankring i konstitusjonell praksis.

I denne sammenhengen er det ikke virksomhetsintern risiko og sårbarhet som er interessant, men den risiko og sårbarhet som virksomheten potensielt kan påføre samfunnet.

På nasjonalt nivå vil dette utgjøre et vesentlig aspekt av en nasjonal tverrsektoriell ROS-vurdering. En nasjonal ROS-vurdering er imidlertid et større arbeid enn det som ligger innefor rammen av BAS5. Metoden som blir presentert i denne rapporten har potensielle anvendelser for blant annet følgende problemstillinger:

- Hvem bør ha prioritert tilgang til teletjenester i krisesituasjoner?
- Hvem bør få vaksine i en pandemisituasjon og i hvilken rekkefølge?
- Hvilke IKT-systemer skal prioriteres ved kraftmangel?
- Hvilke virksomheter i et fylke skal prioriteres ved kraftrasjonering?
- 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?
- Hvilke virksomheter bør være underlagt Sikkerhetslovens bestemmelser?
- Hva bør bygges opp igjen først etter en naturkatastrofe?
- Hvilke samfunnsområder bør ha særlig oppmerksomhet omkring ROS-vurderinger?

Dette vil si at de prinsipielle beslutningssituasjonene som metoden kan være aktuell for, kan variere sterkt:

- Før krisen
    - ROS-vurdering (vite om faren)
    - Forebyggende arbeid (unngå faren)
    - Beredskapsplanlegging (møte krisen)
    - Øving (kunne kriser)
    - Kvalitetssikring
- Under krisen
    - Kriseavverging
    - Krisehåndtering (”få kontroll”)
    - Kriseavvikling
- Etter krisen
    - Normalisering
    - Gjenoppretting
    - Evaluering og læring

2.4 Målgruppe

Hvem som konkret er beslutningstagere for de nevnte problemstillingene vil variere. Den primære

og prinsipielle målgruppen for denne rapporten er imidlertid offentlige myndigheter og private virksomheter som har ansvar for beskyttelse av kritiske samfunnsfunksjoner. Dette gjelder offentlig myndighet med konstitusjonelt ansvar og ansvar for regulering og tilsyn, og offentlig og privat virksomhet som eier kritiske samfunnsfunksjoner og infrastrukturer. Disse deler som hovedregel et juridisk ansvar for å opprettholde samfunnsmessige viktige tjenester, også i krisesituasjoner og lignende. Dette innebærer grader av ansvar for forebyggende tiltak, krisehåndtering og gjenopprettelse av tjenesten, og planlegging for dette. Konkret ansvar vil variere med sektorlovgivningen. Siden det også er praktiske forskjeller mellom forskjellige samfunnssektorer, må metoden tilpasses den enkelte sektoren i nødvendig og mulig grad.

Metoden må kunne brukes av administrativt personale, eventuelt med støtte fra eksperter. Dette innebærer blant annet at den må være intuitivt forståelig for administrativt personale og ha relativt lav brukerterskel. Det vil være en fordel om metoden fremstår som et strukturert verktøy som kan brukes uten alt for mye veiledning. Det innses imidlertid at metoden vil kunne generere datamengder som vil gjøre det fordelaktig å bruke enklere tilrettelagt databaseverktøy. Dette er også et funn i den nevnte Østfoldundersøkelsen.

2.5 Krav forbundet med metoden

Metoden skal være risikobasert, det vil si at risiko- og sårbarhetsanalyser (ROS-analyser) eller -vurderinger er et vesenlig innspill til metoden. Dessuten skal den kunne sammenligne svært ulike risikofenomer fra ulike sektorer, det vil si at resultater fra forskjellige ROS-analyser skal presenteres i en standardisert form for denne metodens formål. Denne standarden er gitt i metoden og forutsetter en risikomatrise hvor sannsynlighet og konsekvens for uønskede hendelser tilknyttet samfunnsfunksjonene presenteres i scorer 1 – 5. Det som skal ligge bak scorene 1 – 5 er gjort eksplisitt i metoden. Resultater fra allerede eksisterende ROS-analyser omfortolkes til denne standarden.

Sammenligning av informasjon om risiko og sårbarhet på tvers av sektorgrenser vil utgjøre et vesentlig argument i eventuelle prioriteringsprosesser. ROS-analyser som gir innspill til metoden skal i så stor grad som mulig tilfredsstille grunnleggende generelle krav (basert på NIPP[5]) til:

- Troverdighet, herunder
  - Integritet og metodisk holdbarhet
  - Kompletthet, med hensyn til innhold
  - Forsvarlighet, med hensyn til logikk
- Sammenlignbarhet, herunder
  - Dokumenterte metoder
  - Gjennomsiktig og begripelig
  - Gjentakelig eller verifiserbart

[5] Department for Homeland Security. 2006. *Revised Draft, National Infrastructure Protection Plan v2.0 January 2006, Appendix 3A: NIPP Baseline Criteria for Assessment Methodologies.* http://www.ni2ciel.org/NIPC/Revised-Draft-NIPP-v2.0.pdf

- Nøyaktighet

3 Viktige begreper

Gjensidig avhengighet beskriver to eller flere prosesser eller systemer som i varierende grad er avhengige av hverandre for å kunne fungere, for eksempel elektrisk kraft og telekommunikasjoner.

Kritiske samfunnsfunksjoner er alle funksjoner som samfunnet er avhengig av for å dekke befolkningens grunnleggende behov, jf. Maslows behovspyramide (se kapittel 5.2).

Kritisk infrastruktur er de av de kritiske samfunnsfunksjonene som er mest sentrale for å holde samfunnet i gang, her i praksis elektrisk kraft, telekommunikasjoner, vann og avløp, olje- og gassforsyning, transport, og bank og finans. Infrastrukturutvalget definerer begrepet slik:[6]

- "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."

I forlengelsen av begrepet kritiske samfunnsfunksjoner dukker begrepet *samfunnskritiske IKT-systemer* opp. I BAS5 er dette begrepet i første rekke benyttet om IKT-systemer som er viktige for funksjonaliteten av ulike kritiske samfunnsfunksjoner. Det er imidlertid viktig å understreke at dette ikke bare dreier seg om teknologiske forhold, men også om menneskene som anvender teknologien, organisatoriske forhold rundt IKT-systemet osv.

Risiko uttrykker fare for tap av viktige verdier som følge av uønskede hendelser. En vanlig tilnærming er å se på risiko som en kombinasjon av *sannsynlighet* av og *konsekvens* for en uønsket hendelse. En annen tilnærming er at *risiko er en kombinasjon av mulige konsekvenser og tilhørende usikkerhet*. Denne tilnærmingen gjør det mulig å vurdere risiko som ikke har noen historikk. Man kan for eksempel tilnærme seg usikkerhet via et sårbarhetsperspektiv og via trusselbegrepet. I prosjektet er den siste definisjonen lagt til grunn for det metodiske arbeidet rundt risiko- og sårbarhetsanalyse.

Samfunnets grunnleggende verdier er knyttet til befolkningens grunnleggende behov, og er her praktisk definert som liv og helse, livsmiljøet, økonomien, styringsevnen, og politisk tillit.

Sikkerhet er et samlebegrep for beskyttelse mot ulike uønskede hendelser. Innenfor sikkerhetsbegrepet skjuler det seg mange dimensjoner, blant annet om de uønskede hendelsene er tilfeldigheter og ulykker eller om de skjer som resultat av overlegg. *Informasjonssikkerhet* defineres tradisjonelt ved hjelp av begrepene *tilgjengelighet, integritet og konfidensialitet.* Med dette menes at informasjonen skal være *tilgjengelig* for autoriserte brukere, at informasjonen bare skal kunne endres eller slettes av autoriserte brukere (*integritet*) og at informasjonen ikke skal kunne leses av andre enn autoriserte brukere (*konfidensialitet*).

Substitusjon og substitusjonsevne, beskriver evne til å erstatte én ressurs med en annen for eksempel dersom den første ikke skulle være tilgjengelig.

Sårbarhet uttrykker at et system har svakheter som muliggjør uønskede endringer eller hendelser, og som dermed gir systemet annerledes oppførsel enn tiltenkt ved systemets design og daglige virke. En annen definisjon er at sårbarhet er et uttrykk for et systems manglende evne til å fungere og oppnå sine mål når det utsettes for påkjenninger. 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.[6]

Tett kobling beskriver prosesser eller systemer som er avhengige av sentralisert driftsstyring for å kunne fungere rett i tid og rom, for eksempel jernbanedrift.

Trusselbegrepet knyttes ofte til viljeshandlinger, og omhandler da kapasitet og intensjon til å gjennomføre skadelige handlinger. Vurderinger av kapasitet og intensjon kan brukes som en teknikk for å redusere usikkerhet og si noe om "sannsynlighet" for en slik handling.

4 Prosess og ansvar

Metoden er delt i to hovedmomenter. Det første momentet behandles i dette kapitlet og er av vital betydning for gjennomføringen av metoden. Momentet gjelder utviklingen av en prosess som involverer sektorer og virksomheter med ansvar, og dermed beste kompetanse på sine områder. Det andre momentet tas opp i neste kapittel og gjelder utviklingen av standarder som tillater sammenligning av risiko og sårbarhet over sektorgrenser. Dette er momenter som utfyller hverandre og ikke suksessive faser. Metoden bør suppleres med bruk av databaseverktøy, ettersom metoden kan generere anselige mengder informasjon.

Så langt er vi kjent med at det er foretatt ROS-analyser på samfunnssektornivå for helsesektoren (HelseROS)[7] og samferdselssektoren (SAMROS). Den siste er basert på et underlagsdokument fra SINTEF.[8] Begge er primært prosessorienterte, det vil si at de legger avgjørende vekt på å involvere kunnskap fra relevante fagmiljøer i departementenes ansvarslinjer.

Metoden kan gjennomføres innenfor det enkelte departementets forvaltningsområde for departementets egne formål. Ansvarsprinsippet ligger til grunn for norsk offentlig forvaltning, det vil si at det enkelte departementet ivaretar sine egne tillagte sektorer og har eneansvar for disse overfor Stortinget ved sin minister. Gjennomføring av metoden slik den er intendert vil imidlertid

[6] NOU 2000:24. *Et sårbart samfunn.*
[7] Sosial- og helsedirektoratet, 2006. *Nasjonal ROS- og beredskapsanalyse innen helse*. Hovedrapport januar 2006.
[8] Hokstad, Per. 2005. Overordnet risiko- og sårbarhetsanalyse for samferdselssektoren. SINTEF rapport STF50 A05152, 2005.

kreve tverrfaglig involvering fra en rekke myndigheter og virksomheter med relevant ansvar. Det er et vesentlig poeng med metoden at den gjennomføres i alle relevante sektorer, og at det i dette arbeidet ligger at det utvikles et felles gode over departementsgrensene.

Imidlertid vil sektorer og virksomheter ha en primær interesse for å identifisere egen risiko, og ikke risiko for andre virksomheter, sektorer eller for samfunnet som helhet. I noen tilfeller kan det være sammenfall av interessert, i andre er det mindre åpenbart. Det tenderer til å være en inngrodd skepsis mot ressursbruk på "altruistiske" aktiviteter, det vil si de som er til fordel for andre. I prinsippet fins det en potensiell situasjon av type "fangens dilemma"[9] mellom aktører og sektorer, med uheldige virkninger for tverrsektoriell risikostyring. Innspill fra forskjellige virksomheter og sektorer er vitalt for vurdering på samfunnsnivå; rent bortsett fra argumentet om ansvarsprinsippet er det sektorene som har ekspertisen. Gjensidige avhengigheter mellom sektorer forsterker gjerne problemet.

Det vil være viktig at de respektive myndigheter bryter ut av "fangens dilemma" i denne sammenhengen. Om antall aktører er begrenset, kan de få til å forhandle frem felles risikovurderingsprosesser som er i felles interesse. Når antall aktører er stort, blir dette ikke gjennomførbart. Et stort antall aktører på forskjellige nivåer kan imidlertid forhandle frem enighet om å etablere et felles system, med:

- felles, anerkjent systemansvarlig
- felles (sosiale) prosedyrer
- felles metoderelaterte standarder

4.1 Felles, anerkjent systemansvarlig

Den mest farbare veien er at "noen" ivaretar dette på nasjonens vegne. Det antas at slik samordning kan forankres i Kgl. res. av 16. september 1994 om Justisdepartements samordningsfunksjon på beredskapssektoren og om Rådet for sivilt beredskap. Det vises også til at det allerede fins prinsipielt lignende ordninger for blant annet Forsvarssjefens nøkkelpunktdirektiv og for Sivilt beredskapssystem.

Det må forventes at metoden vil utgjøre en forholdsvis møysommelig og arbeidskrevende byråkratisk prosess. Prosessen må linjeforankres i de aktuelle departementene i henhold til ansvarsprinsippet og, noe avhengig av ambisjonsnivå, skyves nedover i fagetater og ut til relevante systemoperatører med fag- og systemkompetanse, jf prosessene i Samferdselsdepartementets ROS-analyse SAMROS.[10]

Det er imidlertid ikke å forvente at det praktiske nasjonale systemansvaret i forbindelse med

[9] En situasjon hvor det isolert sett ser ut til å lønne seg for den enkelte å opptre egoistisk, men dersom alle gjør det, taper alle.
[10] SØRLI Kjetil, HENRIKSEN Stein, BOGEN Lene, MØRKESTØL Kristin. 2007. *Bakgrunnsstudie til metode for rangering og identifisering av kritiske samfunnsfunksjoner*. FFI/RAPPORT-2007/00875.

samordning av metoden bokstavelig talt vil bli ivaretatt av Justisdepartementet. Dette vil involvere et betydelig arbeid i forbindelse med å gjennomføre metoden, vedlikeholde den og videreutvikle den. Departementet må forventes å delegere oppgaven, for eksempel til den underordnete etaten Direktoratet for Samfunnssikkerhet og beredskap (DSB). Oppgaven kan forankres i Kgl. res. av 24. juni 2005 om Direktoratet for samfunnssikkerhet og beredskap – det generelle koordineringsansvaret og ansvar for koordinering av tilsyn med aktiviteter, objekter og virksomhet med potensial for store ulykker. En analogi til denne eventuelle oppgaven er DSBs samordning av Sivilt beredskapssystem.

Antagelig bør oppgaven gjøres i samarbeid med Nasjonal sikkerhetsmyndighet (NSM), som Justisdepartementet har instruksjonsmyndighet overfor. Jf også Lov av 20. mars 1998 nr. 10 om Forebyggende sikkerhetstjeneste (Sikkerhetsloven) (jf §§ 1-3) med hensyn til NSMs generelle oppdrag.

Det må forventes at metoden vil generere beskyttelsesverdig informasjon, som må håndteres i henhold til gjeldende bestemmelser avledet fra Sikkerhetsloven.

Den som eventuelt får dette oppdraget må tildeles nødvendige ressurser, i form av forankret myndighet, personell og økonomi. Det vil si at oppdraget må forankres i relevante styringsdokumenter som St. prop. nr. 1, tildelingsbrev og annet.

4.2 Felles prosedyrer

Prosessen forutsetter at vesentlige hensyn som nevnt ovenfor med hensyn til oppdrag, fullmakter og ressurser er avklart, slik at det fins en legitim nasjonal systemeier.

Prosessen kan i prinsippet tenkes å involvere følgende samfunnsnivåer:

- samfunnssektorer (vertikal dimensjon)
    - departementer
    - etater
    - virksomheter
    - nøkkelpersoner eller objekter (for noen formål)
- hele samfunnet (horisontal dimensjon), på nivåene
    - lokal
    - fylke
    - nasjonal
    - (regional og global)

Følgende hovedlinjer i en prosess foreslås:

1. Systemadministrasjon
    a. Nasjonal systemeier utvikler, vedlikeholder og operasjonaliserer felles metode og verktøy og gir nødvendig veiledning.

    b. Nasjonal systemeier administrerer prosessen, inklusive revisjonssyklus, i forhold til ansvarlige departementer og eventuelt fylkesmennene.
2. Informasjonsinnhenting
    a. Ansvarlige departementer delegerer til underlagte etater, eventuelle samvirkegrupper eller bransjegrupper, som igjen involverer operative bransjeaktører, bransjeorganisasjoner, tjenesteleverandører, eiere av kritiske samfunnsfunksjoner og andre relevante aktører.
    b. Det gjennomføres ROS-vurdering for egen virksomhet med fokus på risiko og sårbarhet for samfunnet. Resultatet rapporteres oppover i ansvarskjeden til ansvarlig departement (eventuelt også til fylkesmennene) i felles format (se kapittel 4), slik at resultater fra flere virksomheter kan sammenlignes.
3. Sammenstilling på sektornivå
    a. Ansvarlig departement eller etat kan eventuelt utarbeide foreløpig resultat på stadium 2a ovenfor, avhengig av konkret formål, kompleksiteten i egen sektor og kunnskaper om dette.
    b. Ansvarlig departement sammenstiller resultatene for egen sektor og etablerer en sektorintern prioritet.
4. Tverrsektoriell sammenstilling
    a. Fylkesmannen sammenstiller eventuelt resultatene regionalt.
    b. Nasjonal systemeier sammenstiller forslag til nasjonal prioritert oversikt i en konsensusprosess som involverer ansvarlige departementer.

Gitt det store spennet av potensielt viktige formål som en slik prosess kan brukes til, synes det nødvendig å etablere *permanente arbeidsfora* med relativt hyppige møter, eksempelvis månedlige, både internt i det enkelte departement i forhold til underlagte virksomheter, men også mellom departementene under ledelse av nasjonal systemeier. Det bør etableres en agenda over viktige prioriteringssaker, jf for eksempel listen i kapittel 1.3.

De forskjellige punktene i en slik agenda bør sikres en viss revisjonssyklus, for eksempel årlig eller tilpasset det enkelte punktets endringstakt. Det antas, med bakgrunn i den foreslåtte prosessen, at det vil ta en del tid å utvikle metoden som et allment system, sannsynligvis flere år.

Det understrekes imidlertid nok en gang at prosesser av den beskrevne typen er vesentlige for gjennomføringen av denne typen oppgaver.

4.3 En eksemplifisering av utfordringen

La oss anta at den konkrete problemstillingen er å etablere en liste over abonnenter som bør gis prioritet for mobiltelefoni på grunn av deres funksjon i samfunnet. Formålet med prioriteringen er å sikre viktige samband i en krisesituasjon. En slik prioriteringsfunksjon innebærer at de aktuelle abonnentene stiller først i køen for ledig summetone, eventuelt kan bryte andre samtaler for å komme frem. Via den foreslåtte metoden kan man for eksempel gjøre følgende:

- Identifisere kritiske brukere
- Finne ut hvilke scenarier denne prioriteringen potensielt er viktig for
- Sile fra abonnenter som har substitusjonsmuligheter, for eksempel kan nås på fasttelefoni eller har andre mobile samband

La oss videre anta at et aktuelt scenario er et større havari i elektrisitetsforsyningen, hvor det er nødvendig å sende et antall mannskaper ut felten for å reparere. Siden dette er et potensielt farlig arbeid på grunn av sterkstrøm, er det viktig at disse personene har samband, slik at man vet når strøm kan være slått på eller må være slått av. La oss også anta et annet scenario, med pandemisk influensa, hvor det kan være viktig å kunne kontakte leger i allmennpraksis og annet helsepersonell.

Problemet er at det uten vanskeligheter kan identifiseres minst 100 potensielle krisescenarier på lignende generalitetsnivå, og at disse til sammen, i en norsk sammenheng og etter diverse avgrensinger, kan tenkes å generere en mulig prioritert abonnementsmasse på cirka 100.000 personer over alle samfunnssektorer. Dette blir av forskjellige grunner, både tekniske og økonomiske, for mange til at det blir en reell prioritering. 5.000 abonnenter er et mer realistisk grunnlag for prioritering. Det vil si at det må kunne etableres en tverrsektoriell og rimelig rettferdig prioriteringsordning, basert på funn i standardiserte ROS-vurderinger, som er i stand til å finne de som er de aller mest verdige trengende, fordi de ”eier” den aller største risikoen. Oppgaven er stor og ressurskrevende og har et visst anstrøk av *mission impossible*, dersom det er forventninger til at den kan løses gjennom noen enkle grep.

Utfordringen blir ikke særlig forskjellig hvis problemstillingen for eksempel er å finne frem til hvilke IKT-systemer som er mest kritiske for samfunnet. Eksemplet illustrerer at denne type problemstilling, det vil si prioritering av knappe ressurser for beredskapsformål, er komplisert. Utfordringene knyttet til dette er sannsynligvis sterkt undervurdert.

5 Felles metoderelaterte standarder

Dette kapitlet beskriver forutsetningene for en metode for identifikasjon og rangering i praksis. Metoden er risikobasert, det vil si at det må gjennomføres eksterne risiko- og sårbarhetsanalyser for de hendelsene og samfunnsfunksjonene som blir med videre i metoden.[11] En del konkretiseringer av begreper er her gitt à priori, dette gjelder særlig hva som konkret legges i begrepene

- Kritisk samfunnsfunksjon
- Risikohendelse

[11] Alternativet til en gjennomanalysert risikobasert prioriteringsprosess ville for eksempel være å bruke antagelsesbaserte tommelfingerregler for prioritering av denne typen:

1. Systemvern for den primært rammede samfunnsfunksjonen
2. Samfunnsledelse
3. Andre kritiske samfunnsfunksjoner (sekundærskader)

..og håpe at det ville gå bra.

- Sårbarhet
- Sannsynlighet
- Konsekvens

Det må imidlertid understrekes at slike konkretiseringer ikke er endelige, og at utvikling av en metode av denne typen er en iterativ prosess. Det vil si at metoden må modifiseres etter at det er samlet en del erfaring ved eventuell bruk av den. Dette vil først skje etter at BAS5-prosjektet er formelt avsluttet.

5.1 Forutsetning for metoden: Risiko- og sårbarhetsvurdering

Denne metoden er ikke en metode for risiko- og sårbarhetsanalyse (ROS-analyse) i den enkelte virksomhet eller for konkrete funksjoner eller systemer i den enkelte virksomhet. Det er snarere slik at metoden forutsetter at slike analyser finner sted og "snylter" på *resultatene* av dem. I denne metoden stilles det heller ikke krav til at det benyttes en bestemt metodikk for ROS-analyser. Momenter som er relevante for å velge og å bruke ROS-metode kan finnes i artikler og rapporter tilknyttet BAS5.[12]

Det er et store forskjeller mellom ROS-metoder, blant annet med hensyn til kompleksitet, ressursbruk og læringsterskel. Som en generell observasjon med hensyn til valg av metode, synes det å være bedre å velge en enkel, men tilstrekkelig metode som faktisk blir gjennomført, enn en ideell og i alle henseender "korrekt" metode som viser seg å være for komplisert i praktisk bruk og som forblir ubrukt.

Det stilles følgende *krav* til den videre prosessen:

- Metoden for risiko- og sårbarhetsanalyse eller -vurdering skal tilfredsstille generelle kvalitetskrav som for eksempel de som er gjengitt i kapittel 2.5 ovenfor, særlig med hensyn på troverdigheten til analyseresultatet
- Metoden skal benytte seg av de typologier for kritiske samfunnsfunksjoner og uønskede hendelser med mer som gjengis nedenfor, eller videreutviklede versjoner av disse
- Alle vurderte eller analyserte hendelser skal gis et referansenummer i det formatet som beskrives i kapittel 5.2, mao. [samfunnskritisk funksjon] / [hendelse]
- Resultatene fra alle vurderinger og analyser skal for den beskrevne metodens formål tilpasses et standardisert format som beskrives nedenfor, slik at risiko kan sammenlignes
    - Nye vurderinger og analyser tilpasses dette formatet i utgangspunktet
    - Eksisterende vurderinger og analyser omfortolkes til dette formatet

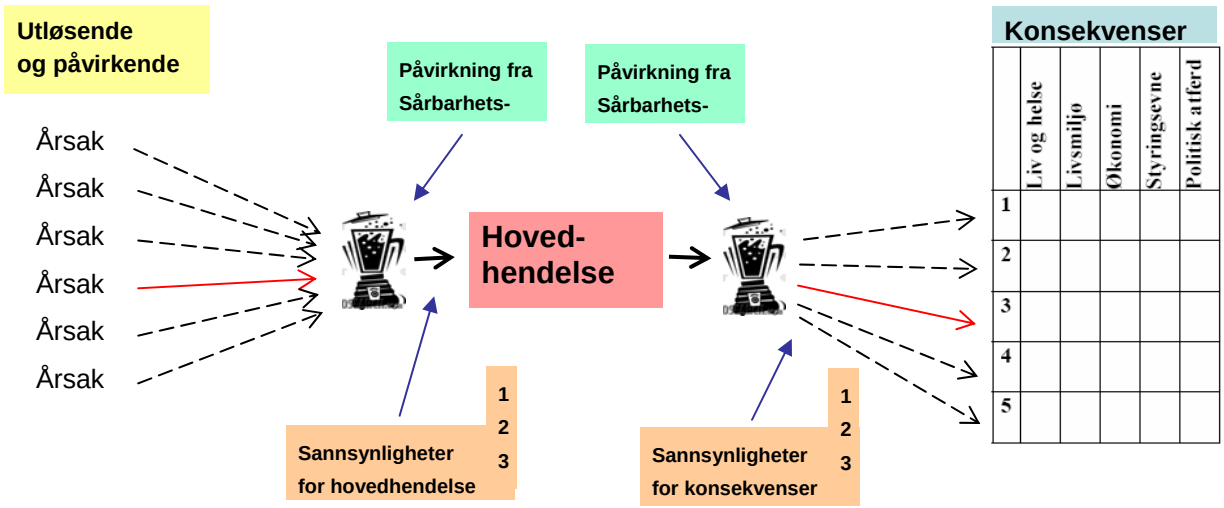
Det understrekes at standardisert presentasjon av resultater fra ROS-analyser er av avgjørende betydning for å kunne bruke ROS-analyse som grunnlag for prioriteringsprosesser som overskrider virksomhets- og sektorgrenser.

[12] Se spesielt SEROS rapport 91892. 2007. Utvikling av metodikk for risikoanalyse av samfunnskritisk IKT.

Dette standardiserte formatet er ikke støpt i betong. Det er et forslag, og kan eventuelt endres i løpet av tidlige faser i de prosesser som beskrives i kapittel 4. Det er imidlertid vesentlig og arbeidssparende at det foreligger et omforent standardisert format *før* det iverksettes noe omfattende arbeid.

Siden ROS-analyse og -vurdering er viktig for identifikasjons- og rangeringsmetoden, tas likevel enkelte aspekter ved selve ROS-analysen opp her, primært med tanke på operasjonalisering av sentrale begreper.

Gangen i en ROS-analyse illustreres ofte i en såkalt Bow Tie[13]-modell. En variant av denne modellen er gjengitt i Figur 5.1 nedenfor[14], tilpasset identifikasjons- og rangeringsmetoden. Figuren illustrerer egentlig en sekvens av hendelser: forårsakende hendelse, hovedhendelse og konsekvens (følgehendelse).



Figur 5.1 Bow Tie-modell, illustrerer ROS-analyse

De viktigste begrepene her er:

- Kritisk samfunnsfunksjon
- Hendelse (hovedhendelse og årsak, utløsende og påvirkende hendelse)
- Sårbarhetsfaktor
- Sannsynlighet
- Konsekvens

Disse vil bli operasjonalisert for denne metodens formål i de følgende kapitlene.

[13] Bow tie = tversoversløyfe, pop. ”propell”
[14] I figuren symboliserer ”mixeren” konkrete ROS-metodiske grep eller beregninger, som varierer fra metode til metode. Dette tas ikke opp ytterligere her.

5.2 Samfunnsfunksjoner som er relevante og av vesentlig betydning

Hvorfor er noen av samfunnets funksjoner kritiske? Det må være fordi at de kan avledes fra, støtte, og være vesentlige eller viktige for sentrale samfunnsmessige behov eller samfunnsverdier. Her blir det lagt vekt på samfunnsverdier som i vesentlig grad støtter opp under befolkningens og samfunnets basisbehov, avledet fra og tilpasset i forhold til de to basisnivåene i Maslows behovspyramide[15], se Figur 5.2.

Figur 5.2 Maslows pyramide

Det vil si at det er hensynet til å sikre de fysiske og materielle behovene som dominerer denne fremstillingen. *Konsekvensene* av å miste samfunnsfunksjoner som støtter disse er potensielt større enn det vi aksepterer. I denne metoden vil slike samfunnsmessige behov eller samfunnsverdier bli brukt for å strukturere konsekvenssiden av risikomatrisen, se forøvrig Figur 5.1, høyre side, og Tabell 5.1.

Ofte vil risikoanalytikere søke å redusere og omskrive forskjellige typer potensielle tap til potensielle *økonomiske* tap. Her er det tatt et valg på ikke å gjøre dette. I denne metoden er det valgt å fokusere på samfunnsverdier som er utledet av Maslows to basisnivåer, som vist i Tabell 5.1.

[15] Abraham H. Maslow, 1908-1970, humanistisk psykolog.

Verdi	Viktige komponenter, stikkord
Liv og helse	Helsetjenester, ernæring, bolig, basisbehov
Livsmiljøet	Beboelighet, ufarlighet, bærekraft
Økonomi	Finans-, realøkonomi, materielle ressurser
Styringsevne	Redning og krisehåndtering, nasjonal handlefrihet, myndighetsutøvelse, territorial kontroll
Politisk atferd/tillit	Demokratisk rettstat, befolkningens trygghetsfølelse, sosial kapital, fellesskap, tillit til politiske og sosiale systemer

Tabell 5.1 Viktige samfunnsverdier

Denne listen er også avledet fra tilsvarende lister i Sårbarhetsutvalget og Infrastrukturutvalget sine rapporter[16].

Årsaken til dette valget er blant annet at det er visse typer trusler som spesifikt er rettet mot for eksempel staten og dens styringsevne og mot politiske dimensjoner, og hvor eventuelle effekter på for eksempel liv og helse eller økonomi bare er brekkstenger på veien mot målet. I slike tilfeller har økonomiske tap begrenset relevans.

Det å la være å redusere alle potensielle tap til økonomiske tap fører med seg problemer med å sammenligne alvorligheten bak forskjellige typer tap. Det er her tatt et valg på slike sammenligninger som vil bli presentert senere i rapporten.

Det antas her at mulig svikt i forskjellige kritiske samfunnsfunksjoner vil påvirke disse samfunnsmessige behovene eller samfunnsverdiene negativt. Den grunnleggende listen over kritiske samfunnsfunksjoner som brukes i denne metoden er gitt i Tabell 5.2 nedenfor, og er et utgangspunkt for en detaljert hierarkisk oversikt over mulige kritiske samfunnsfunksjoner. Listen er delt i 3 hovedinndelinger[17], Kritisk infrastruktur, grunnleggende, Kritisk infrastruktur, øvrige, og Andre kritiske samfunnsfunksjoner.

[16] 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.*

[17] Grunnlag for utarbeidelse av listen er tilsvarende lister i EU, Canada og Nederland. Hovedinndelingen er inspirert av, men ikke identisk med, Infrastrukturutvalgets inndeling.

Nivå 1 Hovedkategori	Nivå 2 Sektorer	Referanse-nummer
Kritisk infrastruktur, grunnleggende (S)	Elektrisk kraft (1)	S1
	Elektronisk kommunikasjon (2)	S2
Kritisk infrastruktur, øvrig (K)	Vann og avløp (1)	K1
	Olje- og gassforsyning (2)	K2
	Transport (3)	K3
	Bank og finans (4)	K4
Andre kritiske samfunnsfunksjoner (A)	Matforsyning (1)	A1
	Renovasjon (2)	A2
	Helse-, sosial- og trygdetjenester (3)	A3
	Politi og Nød- og redningstjenester (4)	A4
	Offentlig ledelse (5)	A5
	Medier, nyhetsformidling (6)	A6
	Industrier, viktige og/ eller med potensial for store ulykker (7)	A7
	Nasjonale nøkkelsymboler (8)	A8

Tabell 5.2: Kritiske samfunnsfunksjoner, grovkategorisering

Til grunn for denne inndelingen ligger argumentasjonen i Infrastrukturutvalget vedrørende definerende kriterier for kritiske samfunnsfunksjoner, det vil si at følgende forhold i varierende grad skal være til stede for at noe skal kunne defineres som en kritisk infrastruktur:[18]

- Sterke gjensidige eller asymmetriske *avhengigheter* i forhold til *andre kritiske samfunnsfunksjoner*, eller tilsvarende mellom interne underfunksjoner. Dette synes særlig å være tilfelle innen kategorien *Kritisk infrastruktur, grunnleggende*.
- Vanskelig å finne *alternativer* til eller substitutter for funksjonen eller systemer underlagt den dersom den eller de skulle falle ut, for eksempel kraftforsyning fra nett.
- Tett *kobling*, det vil si at strukturelle forhold gjør at drift av funksjonen eller systemer under den må sentralstyres for at den skal kunne virke trygt. Eksempel på dette er jernbanedrift, som krever streng operativ trafikkstyring fra en sentral, i motsetning til veitrafikk, som vanligvis kan gjennomføres uten slik styring[19].

Implisitt i det siste punktet ligger også en forestilling om at en kritisk infrastruktur er fundert på et sentralstyrt fysisk eller logisk nettverk som er virksomhetskritisk. Disse punktene kan også ses på som sårbarhetspåvirkende faktorer (se kapittel 5.4).

Det understrekes at denne oversikten utgjør en avgrensing i forhold til mange andre viktige samfunnsfunksjoner og i vesentlig grad forholder seg til menneskelige basisbehov for fysisk trygghet slik de er illustrert i Maslows behovspyramide. For eksempel er hele oppvekst- og utdanningssektorene ikke tatt med her.

Som hovedregel skal virksomhet som inngår i hovedkategorien *Kritisk infrastruktur* anses som

[18] NOU 2006:6. *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner.*
[19] Perrow, Charles. 1999. *Normal Accidents. Living with High-Risk Technologies.* Princeton University Press.

virksomhet som er kvalifisert til prioritering. Det vil imidlertid og sannsynligvis være undersektorer og delsystemer innen forskjellige sektorer som ikke kan regnes som samfunnskritiske og ikke skal prioriteres. Dette må derfor analyseres i større detalj av eier av delsystem.

Virksomheter som inngår i hovedkategorien *Andre kritiske samfunnsfunksjoner* må også vurderes av eier av delsystem, da det kan finnes komponenter i dem som berettiger høyere prioritering enn andre komponenter eller funksjonen generelt.

Konkrete prioriteringer av ressurser i forhold til forskjellige beslutningssituasjoner[20] forbundet med kritiske samfunnsfunksjoner kan kreve et detaljeringsnivå som antydet i Appendiks B. I Appendiks B ligger detaljkunnskapen hos virksomhetseiere, og den enkelte systemansvarlige må for den samfunnsfunksjon man selv har ansvar for, føye til de nødvendige detaljer på mer detaljerte, underliggende hierarkiske nivåer i en utvidet oversikt. Erfaringer fra den såkalte Østfoldundersøkelsen tilsier at dersom problemstillingen er en praktisk konkret fordeling av knappe ressurser i en krisesituasjon, for eksempel rasjonering av elektrisk kraft, så må man gå til et detaljert nivå og identifisere og få informasjon fra relevante ressurspersoner, i dette tilfellet på tvers av hele samfunnet, for å få tilstrekkelig informasjon til å kunne gjennomføre tiltaket.[21] Relevante ressurspersoner vil som regel si mennesker på operatør- eller saksbehandlernivå med stor detaljkunnskap om praktisk drift av egen virksomhet. Dette vil i praksis si å opprette et personregister, og kan være konsesjonsbelagt. Detaljert informasjon kan også være beskyttelsesverdig og kan kreve en sikkerhetsmessig verdivurdering.

I rubrikken ”referansenummer” i Tabell 5.2 legges det til et siffer for hvert nivå som detaljeres. Dette er eksemplifisert i tabellene.

[20] Ref kapittel 1.3 – avgrensinger og anvendelsesområder.
[21] Abel, Carl Georg. 2003. Utkast: *Problemstillinger og samfunnskonsekvenser ved strømutkobling*.

Referansenummer:

Gitt den potensielt store datamengden som vil bli generert i denne metoden, er det viktig at samfunnsfunksjoner og tilhørende uønskede hendelser gis referansenumre som gjør det mulig å spore dem gjennom metoden. Bruk av referansenummer vil dessuten lette bruk av databaser. Det er valgt å bruke hierarkisk oppbygde referansenumre som gjenspeiler den hierarkiske oppbygningen av de listene som blir brukt. Referansenummeret vokser med ett siffer for hvert nivå listen blir detaljert. Hvert nivå kan maksimalt gis et spenn fra 1 til 9.

Et referansenummer vil referere til informasjon om samfunnsfunksjonen i nødvendig detalj, for eksempel S1xx for samfunnsfunksjonen, pluss informasjon om den uønskede hendelsen, for eksempel TU5yy for hendelsen. Et fullstendig referansenummer i dette eksemplet vil se slik ut: S1xx/TU5yy, det vil si en hendelse som har noe med elektrisk kraft (S1) og en teknologisk ulykke med strukturell kollaps (TU5) å gjøre (se nedenfor). Alternativt kan referansenummeret for samfunnsfunksjonen også inneholde informasjon som identifiserer hvem som har ansvar og gjennomfører analysen, for eksempel slik S1xxNVExx, hvor NVE står for Norges vassdrags- og energidirektorat.

5.3 Hendelser som kan påvirke samfunnsfunksjonene negativt.

Risiko knyttet til antatt kritiske samfunnsfunksjoner lar seg ikke avlede direkte. Selv om det i dagligtalen ofte forekommer at systemer eller gjenstander beskrives som ”risikable”, er dette strengt tatt ikke riktig. For eksempel er farligheten av et skytevåpen for det meste avhengig av at det skapes en hendelse, at noen plukker det opp og “fomler” med det eller skyter med det. Man må derfor gå veien via analyse av risiko for potensielle *uønskede hendelser* med mulige konsekvenser som kan ramme viktige verdier, herunder de samfunnskritiske funksjonene. Slike hendelser kan grovinndeles i hovedkategoriene[22]

- Fare (hazard), det vil si potensialet for ulykker (av mer eller mindre kjent karakter)
- Trussel (threat), det vil si potensialet for bevisste ondsinnede handlinger eller handlinger som utøveren vet at ikke er i ”vår” (den kritiske samfunnsfunksjonens) interesse. Ofte er dette definert som *evne* ganger *vilje* til å gjennomføre handlingen.

En liste over potensielle hendelser er gitt i Tabell 5.3, som også er hierarkisk oppbygd med referansenummer. Hovedkategorien *Trussel* er markert i rødt.

[22] Aven, Terje. 2006. *A unified framework for risk and vulnerability analysis and management covering both safety and security security*. Reliability Engineering and System Safety, to appear.

	Nivå 1	Nivå 2	Referanse-nummer
Fare	Naturkatastrofe (N)	Meteorologisk (M)	NM
		Geologisk/Geoteknisk (G)	NG
		Brann, naturlig (B)	NB
		Kosmisk (K)	NK
	Medisinsk/biologisk katastrofe (B)	Planter og dyr (P)	BP
		Mennesker (M)	BM
	Teknisk katastrofe (T)	Ulykkesbasert (U)	TU
		Leveransesvikt (i kritisk infrastruktur) (L)	TL
	Dysfunksjonelle menneskelige handlinger (D)	Individuelle (I)	DI
		Kollektive (K)	DK
Trussel	(Ondsinnet) handling mot Norge, norske borgere eller interesser (O)	Kriminalitet (K)	OK
		Terrorisme (T)	OT
		Sikkerhetspolitisk utfordring i fred (S)	OS
		Krigføring (M)	OM

Tabell 5.3 Hendelsestypologi, hierarkisk, grovinndeling

Denne listen kan også detaljeres i flere hierarkiske nivåer, se Appendiks C.

Det vil være et forhold mellom nødvendig konkretiseringsnivå for hendelsestypologien og for kritiske samfunnsfunksjoner. En uønsket hendelse for en gitt konkret samfunnskritiske funksjon må nødvendigvis angis forholdsvis konkret og kan med fordel pensles ut i en scenariebeskrivelse.[23]

Forholdet mellom kritiske samfunnsfunksjoner og (uønskede) hendelser kan være komplisert, for eksempel:

- Flere årsakshendelser kan påvirke hverandre før de leder til den uønskede hovedhendelsen
- Kritiske samfunnsfunksjoner (og hendelser i dem) kan, mer eller mindre direkte, påvirke sannsynligheten for at hovedhendelsen i det hele tatt skjer og eventuelt moderere den
- Gitt at hovedhendelsen skjer, kan kritiske samfunnsfunksjoner påvirke sannsynligheten for forskjellige konsekvensutfall for viktige samfunnsverdier og eventuelt moderere disse (for eksempel kan nødstrøm slå inn og erstatte vanlig kraftforsyning)

Dessuten fins det et skille mellom hvor viktig en kritisk samfunnsfunksjon er i utgangspunktet og i hvilken grad den evner å påvirke utfallet av den aktuelle hendelsen.

Videre betraktninger rundt disse forholdene hører hjemme i den egentlige ROS-analysen, og vil

[23] Begrepet scenario brukes her om en hendelse som er beskrevet i et detaljert manus, med tidfestede og stedfestede episoder eller "innspill" som bygger opp under utviklingen av hendelsen, jf "øvelsesscenario". Scenariebegrepet beskriver en dynamisk utvikling, mens hendelsesbegrepet er kategoriserende.

ikke utpensles videre her.

5.4 Sårbarhetsfaktorer

Sårbarhet er av vesentlig betydning for å identifisere og rangere kritiske samfunnsfunksjoner. Sårbarhetsfaktorer påvirker både sannsynlighet og konsekvens. Slike faktorer tas svært ofte opp i den litteraturen det er referert til i Bakgrunnsrapporten[24] og fokuserer der nærmest unisont på konsekvenssiden av risiko. Fokus er også her sårbarhetsfaktorer når de påvirker konsekvens. Sårbarheter må vurderes *før* det kan konkluderes på potensielle konsekvenser, da for eksempel om eventuelle sårbarhetsreduserende tiltak vil influere sterkt på disse.

Sårbarhetsfaktorer kan påvirke hverandre, for eksempel ved at manglende beredskapsforberedelser i virksomhet innen kritisk samfunnsfunksjon kan vanskeliggjøre substitusjonstiltak ved bortfall av tjenesteleveranse og påvirke konsekvensene av dette. Det er derfor vanskelig å finne en enkelt beregnelig sammenheng mellom sårbarhetsfaktorer og konsekvenser, som mange lignende identifikasjons- og rangeringsmetoder legger opp til. Eventuelle metoder for slik beregning er del av en ROS-analyse og tas ikke opp her.

Vi referer særlig til Klinke og Renn (2002) og Anton et al 2004 som inspirasjon for den følgende oversikten over utvalgte sårbarhetsfaktorer som bør vurderes i en slik sammenheng:[25]

- Den *uønskede hendelsens* kontekst, forventninger for
  - Rom
    - Sted
    - Geografisk omfang
    - Befolkningstetthet
  - Tid
    - Utetemperatur (årstid)
    - Tid på døgnet
    - Varighet
- Iboende egenskaper ved den aktuelle *kritiske samfunnsfunksjonen*
  - Systemarkitektur
    - Avhengigheter i forhold til andre kritiske samfunnsfunksjoner
    - Substitusjonsmuligheter, erstatning av komponenter, omgåelse av feil
    - Grad av kobling
  - Virksomhetskultur
    - Kultur
    - Beredskapsforberedelser

[24] SØRLI Kjetil, HENRIKSEN Stein, BOGEN Lene, MØRKESTØL Kristin. 2007. *Bakgrunnsstudie til metode for rangering og identifisering av kritiske samfunnsfunksjoner.*, FFI/RAPPORT-2007/00875.
[25] Her er det strengt talt bare iboende egenskaper ved den kritiske samfunnsfunksjonen som stemmer med definisjonen på sårbarhet, men den uønskede hendelsens kontekst er tatt med, ettersom det ofte figurerer i forestillinger om sårbarhet.

I Tabell 5.4 nedenfor er dette detaljert og gitt en score, slik at score (1) er mest positivt og angir lav sårbarhet, mens score (5) er mest negativt. Formålet med en slik score er å forenkle vurdering av sårbarhetsfaktorenes innflytelse på risiko.

Sårbarhets-faktor	Påvirkning, grad av sårbarhet	Utfyllende kommentarer
Sted	(1) **Svært liten**	**Åpent lende**
	(2) **Liten**	**Transporttrasé**
	(3) **Middels**	**Gate i (stor)by, tett bygningsmasse, rasfarlig område etc**
	(4) **Stor**	**I / ved farlig installasjon, fabrikk etc**
	(5) **Svært stor**	**Terminal for persontrafikk eller tunnel**
Geografisk omfang	(1) **Lokal/kommune**	**+ Bydel i storby og tilsvarende**
	(2) **Fylke**	**+ Storby, stor forstadskommune**
	(3) **Landsdel**	**Begrenset til 1 av de 5 landsdelene**
	(4) **Nasjonal**	**+ Hovedstaden**
	(5) **Internasjonal**	**Hvis Norge rammes**
Befolknings-tetthet pr 1 km² rute (SSBs rutenett)	(1) **1 - 4**	**Isolert gårdsbebyggelse**
	(2) **5 - 29**	**Spredt gårdsbebyggelse**
	(3) **30 - 199**	**Åpen boligbebyggelse, fortettet gårdbebyggelse**
	(4) **200 - 499**	**Spredt forstad, mindre tettsted**
	(5) **500 - 15200**	**By, fortettet forstad, større tettsted**
Utetemperatur	(1) **+20 °C – +30 °C**	**Ingen oppvarmingsbehov, noe kjølebehov**
	(2) **+5 °C – + 20 °C**	**Noen oppvarmingsbehov**
	(3) **-5 °C – +5 °C, > +30 °C**	**Betydelig oppvarmingsbehov; alt. stort kjølebehov**
	(4) **-20 °C – -5 °C**	**Stort oppvarmingsbehov**
	(5) **< -20 °C**	**Oppvarming er kritisk overlevelsesfaktor**
Tid på døgnet	(1) **Natt**	**Stille**
	(2) **Kveld**	**De fleste er hjemme**
	(3) **Arbeidstid**	**De fleste er på arbeidsplass**
	(4) **Tidlig morgen**	**Morgenstell, frokost, travelhet**
	(5) **Rushtid**	**Til og fra arbeid, skole etc**
Varighet	(1) **< 1 dag**	**Rask normalisering vanlig**
	(2) **< 1 uke**	**Normalisering innen tilsvarende tid (ytterligere 1 uke eller 2)**
	(3) **> 1 måned**	**Normalisering tar vesenlig mer tid enn ytterligere 1 måned**
	(4) **> 3 måneder**	**Normalisering tar 6 mndr til 1 år i tillegg**
	(5) **Kvasi permanent**	**Normalisering tar mer enn 1 år til flere år, tiår**
Avhengighet av eller for annen kritisk samfunns-funksjon	(1) **Svært liten**	**Små avhengigheter**
	(2) **Liten**	**Middels asymmetrisk avhengighet**
	(3) **Middels**	**Middels symmetrisk avhengighet**
	(4) **Stor**	**Sterk asymmetrisk avhengighet**
	(5) **Svært stor**	**Sterk symmetrisk avhengighet**
Substitusjons-muligheter for infrastruktur	(1) **Svært stor**	**Kan erstattes uten problemer**
	(2) **Stor**	**Kan erstattes med visse problemer**
	(3) **Middels**	**Kan erstattes gjennom omfattende innsats**
	(4) **Liten**	**Kan vanskelig erstattes**
	(5) **Svært liten**	**Uunnværlig**
Grad av kobling	(1) **Svært liten**	**Anarkisk**
	(2) **Liten**	**Enkelt regelsett tilstrekkelig for virksomhetens funksjon**
	(3) **Middels**	**Komplisert regelsett nødvendig for virksomhetens funksjon**
	(4) **Stor**	**Operative styringsfunksjoner nødvendig**

Sårbarhets-faktor	Påvirkning, grad av sårbarhet	Utfyllende kommentarer
	(5) **Svært stor**	**Sterkt sentralstyrt med liten avvikstoleranse**
Kultur	(1) **Svært gunstig**	**Åpenhet, ydmykhet, satsingsvilje, realkompetanse, ærlighet**
	(2) **Gunstig**	**Samarbeidsklima, ser muligheter, bevissthet**
	(3) **Middels**	**Forsiktighet, utsettelser, naivitet, ukunnskap**
	(4) **Lite gunstig**	**Preget av forsvarsreaksjoner, angst, isolasjon**
	(5) **Svært ugunstig**	**Preget av maktkamp, hubris, lukkethet, uærlighet**
Beredskaps-forberedelser	(1) **Svært gunstig**	**Jevnlige målrettede øvelser**
	(2) **Gunstig**	**Omfattende effektive tiltak**
	(3) **Middels**	**God risikobevissthet, noen tiltak**
	(4) **Lite gunstig**	**U(nder)kommunisert risiko**
	(5) **Svært ugunstig**	**Manglende bevissthet om mulig risiko**

Tabell 5.4 Noen sårbarhetspåvirkende faktorer

5.5 Sannsynlighet og konsekvens

Sannsynlighet og konsekvens er de mest sentrale begrepene i en ROS-analyse. Det må gjøres klart at man vurderer sannsynlighet og konsekvens for én eksplisitt hendelse som påvirker én eksplisitt kritisk samfunnsfunksjon, og at hver eneste slik hendelse må analyseres separat.

Det er videre av avgjørende betydning for muligheten til å rangere kritiske samfunnsfunksjoner at presentasjon av resultatene fra ROS-analyser og -vurderinger, uansett metodevalg for disse, gjøres i et standardisert format. I denne metoden gjøres dette slik:

- Dimensjonene sannsynlighet og konsekvens presenteres i en skala 1 – 5, hvor 1 er laveste score og 5 er høyeste
- Hva som ligger bak scorene 1 – 5 gjøres eksplisitt

Dette detaljeres i Tabell 5.5 og Tabell 5.6 nedenfor. Det er her lagt vekt på sannsynligheter og konsekvenser for samfunnet og sentrale samfunnsverdier tilpasset et norsk, nasjonalt nivå, det vil si et samfunn med ca 4,5 millioner mennesker, og ikke for enkelte virksomheter.

Kolonnen "beskrivelse" er av vesentlig betydning for denne metoden, fordi den gjør det eksplisitt hva som menes med scorene 1 – 5. Dette gjør det mulig å sammenligne score for forskjellige hendelser med noenlunde visshet om hva de betyr.

Beskrivelsene for de forskjellige scorene i tabellene er relativt arbitrære, uten at det dermed skal sies at de er grepet ut av luften. De er inspirert av tilsvarende beskrivelser andre steder. Poenget har vært å splitte informasjon fra et kontinuum opp i relativt lett håndterlige diskrete kategorier. Dersom disse skalaene benyttes for andre samfunnsnivåer enn det nasjonale, for eksempel fylke eller kommune, må de justeres for dette.

I Tabell 5.5 er det gitt en skala for *sannsynlighet.*[26] Sannsynlighet brukes her som et konvensjonelt begrep som også har i seg begrepsinnehold av *usikkerhet* eller *mulighet*, og ikke bokstavelig og utelukkende som en projisering av en historisk trend.

Nevnelse	Beskrivelse
(1) **Svært lite sannsynlig**	**Mindre enn 1 gang pr 1000 år**
(2) **Lite sannsynlig**	**1 gang pr 100-1000 år**
(3) **Noe sannsynlig**	**1 gang pr 10-100 år**
(4) **Sannsynlig**	**1 gang pr 1-10 år**
(5) **Svært sannsynlig**	**Mer enn 1 gang pr år**

Tabell 5.5 Sannsynlighetsskala

Kildene til usikkerhet kan være forskjellige, for eksempel:

- At vi vet for lite om det fenomenet vi analyserer
- At vi mangler konkrete empiriske data
- Uklare sammenhenger mellom sårbarhetsfaktorer og sannsynlighet
- Uklare sammenhenger mellom kritiske samfunnsfunksjoner og sannsynlighet
- Begrensninger i det metodiske ambisjonsnivået for analysen

I tillegg, og særlig for risikokategorien trussel, vil manglende relevant historikk (empiriske data) utgjøre en usikkerhetsfaktor og kreve andre tilnærminger, for eksempel analyse av aktuelle aktørers vilje og evne til å realisere trusselen. Dette kan kreve en omfattende verbal begrunnelse av et gitt score på skalaen ovenfor.

Det må vurderes i hvilken grad man kan leve med slike årsaker til usikkerhet. Vi sitter igjen med en visst inntrykk, fra blant annet HelseROS og SAMROS, av man faktisk er villig til å akseptere stor grad av usikkerhet omkring sannsynlighet, vel å merke for ROS-analyser som foretas på samfunnsnivå. Her synes det å være en tendens til å dikotomisere; enten er hendelsen sannsynlig, og blir behandlet videre[27], eller så er den usannsynlig, og ignoreres. Det samme er ikke nødvendigvis tilfelle i forhold til analyser av mer konkrete teknologiske systemer.

Man kan eventuelt velge å håndtere ekstrem usikkerhet ved å bruke score 3 som en de facto vet ikke-kategori.

Som tidligere nevnt er det ikke gitt at hovedhendelsen fører til en bestemt konsekvens. Det må vurderes om og i hvilken grad sårbarhet påvirker de potensielle konsekvensene, før det trekkes en konklusjon. I Tabell 5.6 er konsekvensene delt i hovedkategorier som de samfunnsverdiene som er presentert tidligere i rapporten. Se kapittel 4.7 vedrørende omtale av sannsynlig konsekvens versus verste konsekvens.

[26] Identisk med den som er brukt i HelseROS

[27] ..med for syns skyld en eventuelt noe tilfeldig score i en skala som den ovenfor.

Nevnelse	Beskrivelse av potensielle tap for Liv og helse
(1) **Avgrenset**	**1-2 døde, Inntil 10 skadet**
(2) **Viss fare**	**Inntil 10 døde, Inntil 50 skadet**
(3) **Alvorlig**	**Inntil 60 døde, Inntil 300 skadet**
(4) **Kritisk**	**Inntil 300 døde, Inntil 1500 skadet**
(5) **Katastrofalt**	**Mer enn 300 døde, Mer enn 1500 skadet**
Nevnelse	**Beskrivelse av potensielle tap for Livsmiljø**
(1) **Avgrenset**	**Mindre miljøendringer**
(2) **Viss fare**	**Større miljøendringer**
(3) **Alvorlig**	**Moderate helseskadelige miljøendringer**
(4) **Kritisk**	**Store helseskadelige miljøendringer**
(5) **Katastrofalt**	**Ødeleggelse av menneskelig habitat**
Nevnelse	**Beskrivelse av potensielle tap for Økonomi**
(1) **Avgrenset**	**Inntil 0,002 % av BNP (34 mill kr.)**
(2) **Viss fare**	**Inntil 0,02 % av BNP (340 mill kr.)**
(3) **Alvorlig**	**Inntil 0,2 % av BNP (3,4 mia kr.)**
(4) **Kritisk**	**Inntil 2 % av BNP (34 mia kr.)**
(5) **Katastrofalt**	**Mer enn 2 % av BNP (over 34 mia kr.)**
Nevnelse	**Beskrivelse av potensielle tap for Styringsevne**
(1) **Avgrenset**	**Ingen eller mindre forstyrrelser**
(2) **Viss fare**	**Kortere forstyrrelser**
(3) **Alvorlig**	**Betydelige forstyrrelser**
(4) **Kritisk**	**Alvorlige forstyrrelser**
(5) **Katastrofalt**	**Kritiske forstyrrelser, permanente endringer**
Nevnelse	**Beskrivelse av potensielle tap for Politisk tillit/atferd**[28]
(1)**Avgrenset**	**Ingen vesentlige effekter**
(2)**Viss fare**	**Passivt konstruktivt, lojalitet, tilpasning**
(3)**Alvorlig**	**Aktivt konstruktivt, uro, protest, krav om endringer**
(4)**Kritisk**	**Passivt destruktivt, ikke-deltagelse, substitusjonsadferd**
(5)**Katastrofalt**	**Aktivt destruktivt, politisk exit, vold, systemdelegitimering, systemendring**

Tabell 5.6 Konsekvensskalaer

Poenggivning for konsekvensene for forskjellige samfunnsverdier er søkt harmonisert til en viss grad, men at det her ikke er tatt sikte på en direkte sammenlignbarhet. Årsaken til dette er at det ikke fins noen mekanisk sammenheng mellom konsekvenser for forskjellige samfunnsverdier. For eksempel vil ikke score 2 for liv og helse, inntil 50 døde og 200 skadet, nødvendigvis kunne kobles direkte til et økonomisk tap på inntil 1,7 milliarder kroner.

I forskjellige sammenhenger er det av andre forsøkt beregnet hva et tapt menneskeliv koster samfunnet. Gjennomsnittskostnaden for tap av liv ved forskjellige former for ulykker kalles ofte for ”statistisk liv”. Verdien av et statistisk liv kan være beregnet ut fra forskjellige forutsetninger i forskjellige samfunnssektorer, og kan variere mellom 10 millioner kroner og opptil 100 millioner kroner avhengig av sektor. Et vanlig generalisert ”kompromiss” synes imidlertid å være 25

[28] Basert på Hirschman, Albert O, Exit, Voice, and Loyalty. 1970. *Responses to Decline in Firms, Organizations, and States*. Harvard University Press 1970. Videreutviklet av Caryl Rusbult m fl mht begrepet Neglect. (Rusbult, C. E., Zembrodt, I. M., & Gunn, L. K. 1982. *Exit, voice, loyalty, and neglect: Responses to dissatisfaction in romantic involvements.* Journal of Personality and Social Psychology, 43, 1230-1242

millioner kroner.[29] Disse beregningene er basert på erfaringsdata. Forutsetningene for slike beregninger kan for eksempel være tap av livsinntekt, som er mest relevant i forhold til et forsikringsoppgjør, eller samfunnets betalingsvilje i forhold til å forhindre dødsfallet. Denne betalingsviljen kan være svært variabel. De viktigste påvirkningsfaktorene for betalingsviljen synes å være de scenariene et eventuelt dødsfall skjer i, og hvor mange samtidige dødsfall som kan oppstå i disse scenariene. Kostnaden pr dødsfall i ulykker stiger gjerne hvis det er flere dødsfall på en gang.

Det må også understrekes at disse beregningene kun er gyldige i den konteksten de er laget for, det vil si forholdsvis ordinære ulykker med et begrenset antall døde og skadete, og begrenset til verdien av menneskeliv. Ved ulykker med tap av menneskeliv er det gjerne også involvert varierende grader av materielle tap. Det er i forlengelsen av dette vesentlig vanskeligere å finne gode korrelasjoner mellom døds- og skadetall og økonomisk tap i store katastrofesituasjoner, blant annet fordi situasjonen som oftest er mer kompleks og også involverer vesentlige økonomiske tap forbundet med andre verdier enn liv og helse. Det synes også å være forskjeller mellom farescenarier og trusselscenarier når det gjelder sammenligning mellom samfunnsverdier. Det kan for eksempel vises til at betalingsviljen for å unngå krig på norsk territorium og okkupasjon, med de skader som vil følge av det, har vært høy i perioden etter annen verdenskrig. Samtidig viser all erfaring at den økonomiske (og moralske) verdien av det enkelte menneskeliv synker under krig. Det vil si at det relative forholdet mellom samfunnsverdier endrer seg med scenariet.

5.6 Noen dilemmaer

Gitt at det fins en rekke mulige sårbarhetsfaktorer, hvordan bestemmer man hva som er sårbarhetsfaktorenes samlede påvirkning på hver samfunnsverdi/konsekvenstype for den uønskede hendelsen? Gitt at det også fins en rekke mulige samfunnsverdier/konsekvenstyper, hvordan bestemmer man den samlede konsekvensen av den uønskede hendelsen?

Omfanget av dette dilemmaet kan illustreres som i Tabell 5.7.

[29] 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).*

Samfunnsverdi/ konsekvenstype Sårbarhetsfaktor	Liv og helse	Livsmiljø	Økonomi	Styringsevne	Politisk tillit/atferd	
Sted						
Geografisk omfang						
Befolkningstetthet pr 1 km² rute (SSBs rutenett)						
Utetemperatur						
Tid på døgnet						
Varighet						
Avhengighet av eller for annen infrastruktur						
Substitusjonsmuligheter for infrastruktur						
Grad av kobling						
Kultur						
Mental forberedelse						
	>>>>>>>>>>>>>>>>>>>>>>>>>>>					**?**

Tabell 5.7 Konsekvens modifisert av sårbarhet

Selv om det forutsettes en forenklende strukturering av informasjon, er det her mye informasjon om sårbarheter og konsekvenser som skal presses i én konklusjon om samlet konsekvens. Det er tenkbart at man kunne plotte inn forholdet mellom sårbarhet og konsekvens i en slik tabell. Dette blir imidlertid alt for enkelt hvis det gjennomføres mekanisk og ukritisk, ettersom det ikke fins noen enkle sammenhenger mellom de kategoriene og verdiene som er satt for henholdsvis samfunnsverdier/ konsekvenstyper og sårbarhetsfaktorer, og heller ikke dem i mellom.

Det kan imidlertid og for eksempel tenkes enkle regler, for eksempel

- At det beregnes en gjennomsnittverdi for score fra alle sårbarhetsfaktorer
- At score for den forventede konsekvensen for hver samfunnsverdi justeres tilsvarende avviket fra gjennomsnittlig score på sårbarhetsfaktorene, for eksempel når forventet score for konsekvens er 3 og score for sårbarhetsfaktorene er 2, blir konsekvens justert til 3 – 1 = 2.
- At det beregnes en gjennomsnittsverdi for score for alle justerte konsekvenser

Eventuelt kan det utarbeides mer kompliserte regler. Dette må uansett modereres med en subjektiv, men kritisk vurdering. Det må også vurderes om det i enkelte sammenhenger kan være ønskelig å vite og vise at forskjellige sårbarhetsfaktorer har forskjellige virkninger for forskjellige konsekvenstyper. For eksempel kan *varigheten* av en uønsket hendelse være forskjellig for og ha annen grad av konsekvens for *politisk tillit* enn det den har for *liv og helse.*[30]

Et annet viktig dilemma er i hvilken grad det er ønskelig å illustrere et skille mellom en forventet, det vil si mest sannsynlig, konsekvens og et mulig verste tilfelle.

Det er ofte mer interessant å finne ut hva som kan gå riktig galt enn hva som kan gå bedre enn ventet. Da legger man konsekvent fokus på verste antatte konsekvens og gjør dette eksplisitt. Gitt at en vesentlig og normal forventning i konteksten samfunnssikkerhet er å unngå å bli utsatt for verste tilfelle, kan det være en nyttig tilnærming. I denne tilnærmingen ligger det en fare for urealistisk overdrivelse av all risiko, særlig hvis det i tillegg fører til at man får prioritet for en knapp sårbarhetsreduserende ressurs. Dette gir en viss risiko for å gjøre ROS-analyse til en meningsløs og unødvendig eksersis.

I denne metoden anbefales det at man legger mest sannsynlig konsekvens til grunn, eventuelt at man både tar utgangspunkt i dette og i verste tilfelle og tydelig illustrerer forskjellen.

5.7 Presentasjon av resultater fra ROS-analyse, risikomatrise

Uansett valg av ROS-metode, skal resultatene fra den enkelte ROS-analysen som gjennomføres for prioriteringsformål som beskrevet i denne rapporten kunne plottes inn i en risikomatrise slik som den i Figur 5.3. Det er relevant referansenummer [S1xx/TU5yy i eksemplet] som skal plottes inn, som illustrert i matrisen.

Matrisen er her delt i 5 risikoklasser, markert med (tall) og farger, i utgangspunktet:

- Meget lav, (1), hvit
- Lav, (2), grønn
- Middels, (3), gul
- Høy, (4), oransje
- Meget høy, (5), rød

[30] Det kan for eksempel vises til den såkalte Bijlmerkrisen utenfor Amsterdam 4. oktober 1992, da et fraktfly styrtet i en boligblokk. Umiddelbart førte dette til 43 døde. Denne delen av krisen ble ryddet av veien raskt. Imidlertid hadde flyet utarmet uran ombord. Flyet var ellers lastet med militært utstyr, blant annet av toksisk art. Denne delen av krisen tok det nærmere 10 år å lukke.

SANNSYN-LIGHET, Usikkerhet, Mulighet	(5) **Mer enn 1 gang pr år**	2	3	4	5	5
	(4) **1 gang pr 1-10 år**	2	3	3	4	5
	(3) **1 gang pr 10-100 år**	1	2	3	3 S1xx/TU5yy	4
	(2) **1 gang pr 100-1000 år**	1	2	2	3	3
	(1) **Mindre enn 1 gang pr 1000 år**	1	1	1	2	2
		(1) **Avgrenset**	(2) **Viss fare**	(3) **Alvorlig**	(4) **Kritisk**	(5) **Katastrofalt**
		KONSEKVENSER, samlet vurdering for alle samfunnsverdier og vurdert mot sårbarhetsfaktorer				

Figur 5.3: Risikomatrise

Denne typen fargemarkering er relativt ”konvensjonell” og finnes i mange varianter. Poenget med den er å gi en lett oppfattelig advarsel om risikonivåer. Det må imidlertid advares på det sterkeste mot å applisere formelen ”risiko = sannsynlighet x konsekvens” mekanisk, særlig hvis det fører til at hendelser med svært lav sannsynlighet, men ekstreme konsekvenser, vurderes som lav risiko. Denne typen risiko kategoriseres ofte ikke som lavrisiko, men som høyrisiko eller ekstremrisiko. Det tilrås derfor at man regner med at det bokstavelig talt er en politisk nulltoleranse for hendelser med ekstreme konsekvenser, selv om de har lav sannsynlighet. Dette er markert i matrisen ved at hendelser med sannsynlighet (1)-(3) og konsekvenser (5) har *blå* farge.

Risikomatrisen gir en enkel illustrasjon av risiko definert som sannsynlighet ”ganger” konsekvens. Dette gir rask oversikt, forutsatt at ROS-analysen ellers er troverdig og gjennomsiktig. Det må understrekes at risikomatrisen i seg selv ikke utgjør en ROS-analyse. Meningen med den er å illustrere resultatet av ROS-analysen.

Ulempen med bruk av risikomatrisen, gitt at det her brukes 5 konsekvenskategorier som påvirkes av 11 sårbarhetsfaktorer, er at informasjon om sårbarhet og konsekvens presses inn i ett enkelt punkt og at man dermed mister mye informasjon, blant annet om kvaliteten av konsekvensvurderingen. Risikomatrisen må derfor suppleres med andre måter å vise resultater av ROS-analysen, se punktet om databaser nedenfor.

Ved bruk av referansenumre kan flere hendelser plottes inn i matrisen for å oppnå en visuell sammenlignbarhet, for eksempel

- Enklest: flere uønskede hendelser analysert for én samfunnskritisk funksjon

- Etter omkombinering av data: flere kritiske samfunnsfunksjoner som forventes å bli innblandet i én uønsket hendelse
- Noe uoversiktlig: flere (alle) kritiske samfunnsfunksjoner og flere (alle) uønskede hendelser kombinert

5.8 Databasebehandling

Denne metoden kommer til å generere store mengder data når det i prinsippet blir innrapportert risikoinformasjon med et stort antall hendelser som representerer et stort antall virksomheter fra alle kritiske samfunnsfunksjoner. Både for å få bedre oversikt og for å omkombinere data som nevnt ovenfor for spesifikke formål, vil det være nødvendig å bruke en enkel database for å forenkle arbeidet. I tillegg til innplotting i risikomatrise bør derfor data registreres skjematisk, helst rett inn i databasen.

Tabell 5.8 gir et utgangspunkt for utvikling av slik database. Tabellen er her laget i Word, men bør ”oversettes” til databasens arbeidsprogram. Databasen bør være søkbar og sorterbar på de fleste variablene, slik at man for eksempel kan få opp lister over:

- Kritiske samfunnsfunksjoner med prioritert risiko underlagt et bestemt departements eller en etats ansvarsområde
- Prioritert oversikt over uønskede hendelser innen en bestemt samfunnsviktig funksjon
- Prioritert oversikt over samfunnsviktige funksjoner som kan tenkes å rammes av en gitt uønsket hendelse
- Oversikt over hendelser med (lav sannsynlighet og) høy konsekvens

		Registrering							
Ansvar for gjennomføring av **ROS-analysen**	Virksomhet								
Ansvarskjede for samfunnsfunksjonen (bruk gjengse forkortelser)	Departement								
	Etat								
	Virksomhet								
	Stilling eller person								
		Nivå							
		1	**2**	**3**	**4**	**5**	**6**	**(7)**	**(8)**
Referansenummer for **samfunnsfunksjon**									
Referansenummer for **hendelse**									
Kort verbal beskrivelse av konkret scenario for hendelse									

		Score (lav – høy)				
		1	**2**	**3**	**4**	**5**
Sårbarhet	Sted					
	Geografisk omfang					
	Befolkningstetthet pr 1 km² rute (SSBs rutenett)					
	Utetemperatur					
	Tid på døgnet					
	Varighet					
	Avhengighet av/for annen kritisk samfunnsfunksjon					
	Substitusjonsmuligheter for infrastruktur					
	Grad av kobling					
	Kultur					
	Mental forberedelse					
	Samlet vurdering					
Sannsynlighet (usikkerhet, mulighet)						
Konsekvens	Liv og helse					
	Livsmiljø					
	Økonomi					
	Styringsevne					
	Politisk tillit/atferd					
	Samlet vurdering					
Risikovurdering, samlet						
Kort verbal risikovurdering						

Tabell 5.8: Utgangspunkt for database, innregistrering av én hendelse

Hvis Tabell 5.8 ”legges på siden”, kan det lages en tabell som kan angi en prioritetsrekkefølge, se

Tabell 5.9. I en database kan denne tabellen sorteres etter alle registrerte variable, slik at man får en prioriteringsrekkefølge i henhold til de variable man velger å legge vekt på. Man kan for eksempel velge å legge vekt på:

- Alle hendelser med potensielt katastrofale konsekvenser (score 5)
- ...som er tilknyttet en gitt samfunnsfunksjon
- ...som ligger under et gitt departements ansvarsområde
- ...som har en gitt type og grad av sårbarhet

Prioritet	**Ansvar**				**Ref. nr.**	**Ref. nr.**	**Sårbarhet**											**Sannsynlighet**	**Konsekvens**						**Risikovurdering**
	Departement	**Etat**	**Virksomhet**	**Stilling, person**	**Samfunnsfunksjon**	**Hendelse**	**Sted**	**Geografisk omfang**	**Befolkningstetthet**	**Utetemperatur**	**Tid på døgnet**	**Varighet**	**Avhengighet**	**Substitusjonsmuligheter**	**Kobling**	**Kultur**	**Ment forberedelse**	**Samlet vurdering**		**Liv og helse**	**Livsmiljø**	**Økonomi**	**Styringsevne**	**Politisk tillit**	**Samlet vurdering**	
1	**(x)**				**(x)**									**(x)**											**(5)**	
2																										
3																										
osv																										

Tabell 5.9: Prioriteringsoversikt, prinsipiell[31]

Dette gir ikke noen endelig prioritering. Det gir imidlertid sterke argumenter i den diskusjonen om prioritering som vil oppstå, og som grunnleggende er av politisk karakter. Det må antas at ”bevisbyrden” da vil ligge på de som eventuelt ønsker å fravike de anbefalinger om prioritering som denne metoden vil kunne fremskaffe.

[31] En lignende oversikt brukes i det britiske systemet for nasjonal ROS: se HM Government, London 2005. *Emergency Preparedness: Guidance on Part 1 of the Civil Contingencies Act 2004, its associated Regulations and non-statutory arrangements*, Annex 4 A-F (November 2005).

6 Metoden i punkter[32]

6.1 Forankring av prosess

- Metoden må prinsipielt forankres hos alle relevante departementer
- Metoden må forankres i styringsdokumenter og sikres ressurser
- Det må etableres en prosessorganisering som sikrer gjennomføring av metoden, herunder etablering av en nasjonal koordinator.
- Det må etableres permanente fora for koordinering av prosessen
- Når prosessen er forankret og organisert, skal det utvikles en database til støtte for metoden

6.2 Definisjon av omfang

- Relevante problemstillinger for bruk av metoden må etableres og prioriteres, jf listen i kapittel 2.3, det fokuseres èn problemstilling om gangen
- Det må klargjøres hvilke kritiske samfunnsfunksjoner som er aktuelle for de forskjellige problemstillingene, jf Tabell 5.2 og Appendiks B
- Til disse må det fastsettes hva som er nødvendige detaljeringsnivåer for innsamling av informasjon, for eksempel om det er tilstrekkelig for formålet å identifisere undersektorer, eller om man må identifisere virksomheter eller konkrete nøkkelpersoner
- For hver problemstilling må det etableres fullstendig liste over de kritiske samfunnsfunksjonene som er identifisert
- Alle de kritiske samfunnsfunksjonene på denne lista holdes på samme detaljeringsnivå, jf Tabell 5.2 og Appendiks B
- Det må foretas en vurdering av vesentligheten av det som står på lista, jf Infrastrukturutvalgets kriterier for identifikasjon av kritiske infrastrukturer og den valgte problemstillingen

6.3 Identifikasjon av hovedhendelser for analyse

- Til hver identifisert og vesentlig kritisk samfunnsfunksjon skal det identifiseres hovedhendelser (den uønskede hendelsen) som kan påvirke den negativt
- Tabell 5.3 og Appendiks C er utgangspunkt for valg av aktuelle hovedhendelser
- Avhengig av problemstilling velges detaljeringsnivå for hovedhendelsene
- Det settes opp liste over valgte hovedhendelser
- Alle hovedhendelser på lista holdes på samme detaljeringsnivå, jf Tabell 5.3 og Appendiks C
- Den enkelte hovedhendelsen bør gis en kritisk vurdering før man går videre med den

6.4 Momenter til gjennomføring av ROS-analyse

- Det skal gjennomføres ROS-analyse for hver identifisert hovedhendelse

[32] Basert på innspill fra Jørn Vatn, NTNU

- Konkret valg av metode er opp til den enkelte, tilpasset problemstilling, analysenivå og annet
- Resultatet av den enkelte ROS-analysen skal presenteres i en standardisert form som gjengitt nedenfor

6.5 Om vurdering av sårbarhet

- Sårbarhet skal vurderes for hver hovedhendelse
- Vurdering av sårbarhet skal baseres på Tabell 5.4
- Tabell 5.4 angir 11 forskjellige sårbarhetsfaktorer
- Sårbarhet skal vurderes før det trekkes konklusjoner om konsekvens
- Som hovedregel vil de angitte sårbarhetsfaktorene virke på konsekvens etter hovedhendelsen
- Ha oppmerksomhet på at noen av dem av og til er relevante før hovedhendelsen
- Vurderingen skal støttes av kvalitativ argumentasjon

6.6 Om vurdering av sannsynlighet

- Sannsynlighet skal vurderes for hver hovedhendelse
- Vurdering av sannsynlighet skal baseres på Tabell 5.5
- Tabell 5.5 er skalert til nasjonalt nivå
- Vurder hvilke kritiske samfunnsfunksjoner (i tillegg til den som er direkte knyttet til hovedhendelsen) som kan påvirke sannsynlighet for hovedhendelsen og eventuelt hvor mye
- Vurder sårbarhetsfaktorer som kan påvirke før hovedhendelsen
- Vurder historikk for hovedhendelsen i Norge og internasjonalt når dette fins
- Bruk trusselkomponentene evne og vilje (til å utøve ondsinnede handlinger) som vurderingskriterier der det er relevant
- Vær særlig oppmerksom på mulig dynamikk i fare- og trusselbilder
- Vurderingen skal støttes av kvalitativ argumentasjon

6.7 Om vurdering av konsekvens

- Konsekvens vurderes ut fra at hovedhendelsen inntreffer
- Konsekvens skal vurderes for hver hovedhendelse
- Vurdering av konsekvens skal baseres på tabell 6
- Tabell 5.6 er skalert til nasjonalt nivå
- Tabell 5.6 angir 5 forskjellige konsekvenstyper basert på fundamentale samfunnsverdier
- Disse konsekvenstypene skal vurderes separat
- Det skal likevel foretas en samlet vurdering av konsekvens
- Vurder hvilke kritiske samfunnsfunksjoner (i tillegg til den som er direkte knyttet til hovedhendelsen) som kan påvirke konsekvens av hovedhendelsen og eventuelt hvor mye
- Vurder om hovedhendelsen truer andre kritiske samfunnsfunksjoner enn den som er i fokus (vurder egen ROS-analyse for dette)
- Vurder sårbarhetsfaktorer som kan påvirke etter hovedhendelsen, inklusive tiltak som er

egnet til å redusere sårbarhet eller alvorlighetsgrad av konsekvens
- Vurdering historiske konsekvenser i Norge og internasjonalt når informasjon om dette fins
- Vurderingen skal støttes av kvalitativ argumentasjon

6.8 Synliggjøring av risikobildet i risikomatrise

- Resultatet av ROS-analysen plottes inn i risikomatrise som gitt i Figur 5.3
- Forskjeller i konsekvenskategorier kan illustreres ved å gi hver konsekvens sin egen matrise, alternativt å markere dette i samme matrise på en gjenkjennelig måte
- Det kan være formålstjenlig å plotte resultater fra flere ROS-analyser inn i samme matrise; med måte; dette kan bli uoversiktlig

6.9 Innføring i database

- Resultatet av ROS-analysen føres inn i database
- Retningslinjer for dette vil først foreligge når databasen er utviklet
- Et databaseverktøy kan settes opp til å foreta beregninger av i hvilken grad kritiske samfunnsfunksjoner påvirker hovedhendelsen, til støtte for og forenkling av vurderinger omkring dette

6.10 Sammenligning på tvers

- En database vil være et nyttig og nødvendig verktøy for å prioritere på tvers av samfunnssektorer basert på ROS-analysene
- Databasen må være satt opp slik at man kan velge hvilke av de registrerte variablene man ønsker å prioritere etter

6.11 Forslag til prioritering

- Med utgangspunkt i resultatene fra ROS-analysene og databasen over disse skal det settes opp forslag til prioritering med hensyn til tiltak

7 Oppsummering, anbefalinger og videre arbeid

7.1 Oppsummering

Behovet for å prioritere ulike hensyn i samfunnet er ikke av ny dato. Spesielt gjelder dette innenfor arbeidet med nasjonal beredskap, hvor begrensede ressurser har måttet blitt fordelt der de kan gi størst virkning. Eksempler på beredskapsproblemstillinger innenfor prioritering er utpeking av nøkkelobjekter i samfunnet som må beskyttes av militære styrker i en krisesituasjon, klassifisering av objekter innenfor kritiske infrastrukturer for å avklare hvilke som skal underlegges de hardeste sikkerhetskravene, og utpeking av sektorer som skal prioriteres med

vaksiner i tilfelle en pandemi brer seg. Muligheten for prioritering er også et vesentlig aspekt av en nasjonal tverrsektoriell ROS-vurdering, hvor ulike sektorer, virksomheter eller til og med personer og stillinger kan ses mot hverandre.

Innenfor IKT-sikkerhetsområdet kan det også defineres behov for å prioritere mellom ulike forhold. Dette kan gjøres blant ulike IKT-systemer, mao. at de mest samfunnskritiske IKT-systemene identifiseres og rangeres slik at man kan styre ressurser og bidra til økt sikkerhet på de riktige stedene. Et annet forhold er å prioritere brukerne av ulike IKT-systemer, for å se hvilke av disse som bør tas hensyn til i knapphetssituasjoner. Prioriteringsproblematikken knyttet til IKT kan derfor ikke bare inkludere IKT-systemene i seg selv, men må også inkludere brukerne som er avhengige av systemene.

Opprinnelig målsetting for BAS5 var å utvikle og anvende metodikk for *identifisering og rangering* av kritiske samfunnsfunksjoner og IKT-systemer. I henhold til bokmålsordboka[33] betyr *rangere* å ordne i en bestemt rekkefølge. Denne rekkefølgen kan være prioritert. *Prioritere* vil si å sette opp i rangorden og gi noe eller noen i denne ordenen fortrinn fremfor andre. BAS5-målsettingen har blitt tolket slik at mulighet for prioritering er ønskelig. Beskrivelsen i avsnittene over tilsier også dette. Dette er imidlertid ikke en enkel oppgave. Prioritering av samfunnskritiske funksjoner og virksomheter er en politisk og ikke en teknokratisk prosess. Blind anvendelse av en metodikk er derfor lite hensiktsmessig – det må også være klart hva prioriteringen skal anvendes til og hvilke ulike hensyn som skal tas i ulike prioriteringssituasjoner.

BAS5 har derfor gjort følgende:

- Prosjektet har utviklet en metode for identifisering og rangering av *alle* kritiske samfunnsfunksjoner, herunder alle kritiske infrastrukturer, og ikke bare kritiske IKT-systemer.
- Prosjektet har *beskrevet et system for beslutningsstøtte, og ikke et system for automatisk prioritering*. Dette betyr at relevante beslutningsmiljøer må involveres i bruken av metoden. Arbeidet kan ikke settes bort til ekspertmiljøer, selv om disse med fordel kan delta i prosessen.

Det er lagt vekt på at rapporten skal være relativt kortfattet. Det er lagt vekt på å fremstille én valgt løsning som etter forfatternes mening er den løsningen som vil føre frem.

I BAS5-prosjektet er ulike samfunnsfunksjoners kritikalitet knyttet til sårbarheten overfor ulike hendelser som kan ramme dem, i tillegg til betraktninger om deres vesentlighet eller viktighet for samfunnet. *Det er derfor knapt mulig å prioritere kritiske samfunnsfunksjoner uten samtidig å gjøre seg opp en grunnleggende mening om hvilke risiko de er utsatt for eller utsetter andre for.* Det vil si at det må forutsettes at det foretas risiko- og sårbarhetsvurdering (ROS-vurdering) på sektor- og virksomhetsnivå.

Metoden som er utviklet beskriver hovedtrekkene for beslutningstøtte i situasjoner hvor det kan

[33] Bokmålsordboka, Universitetsforlaget

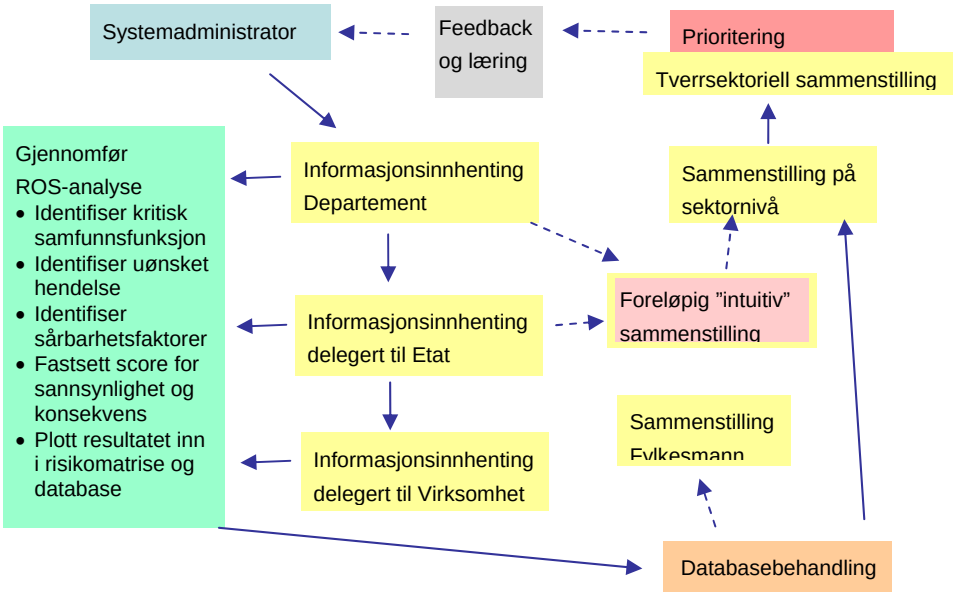
være nødvendig å prioritere mellom forskjellige kritiske samfunnsfunksjoner. Metoden er risikobasert, og inneholder to hovedaspekter:

- Det utvikles og forankres en permanent løpende prosess som involverer ansvarlige departementer og alle andre som har ansvar og kunnskap innen egen sektorer
- Til støtte for denne prosessen brukes en teknikk som er ROS-basert, da antagelser om kritikalitet bør forutgås av nærmere analyse og vurdering

Prosessen krever følgende:

- At "noen" pekes ut til å samordne den på nasjonalt nivå, på tvers av ansvarsgrenser
- At det ordinære ansvarsprinsippet utnyttes for å strukturere arbeidet
- At det etableres tverrsektorielle felles prosedyrer, inklusive permanente fora med tett møtefrekvens
- At det etableres tverrsektorielle standarder

Prosessen kan illustreres som i Figur 7.1.



Figur 7.1 Prosessoversikt. Heltrukne linjer angir hovedsteg i prosessen.

Metoden skal kunne prioritere på tvers av forskjellige samfunnssektorer. Dette krever et standardiserende grep på metodens teknikker. Konkret valg av metodikk for ROS-analyse er overlatt til den enkelte sektor eller virksomhet, tilpasset dennes forutsetninger. Innrapportering av resultater fra ROS-analyse skal derimot foretas i et rigid standardisert format. Denne standardiseringen omfatter:

- En hierarkisk organisert liste over kritiske samfunnsfunksjoner
- En hierarkisk organisert liste over uønskede hendelser

Den hierarkiske organiseringen tillater at listen enkelt suppleres ved behov. Dessuten fremstår

denne typen organisering som et ”trekkspill” i forhold til hvilket generalitetsnivå det er ønskelig å legge seg på for forskjellige formål, fra svært konkrete problemstillinger som krever identifikasjon av nøkkelpersoner, til mer generell prioritering mellom sektorer.

Dessuten standardiseres følgende:

- 11 sårbarhetsfaktorer i 5 konkretiserte trinn hver
  - Sted
  - Geografisk omfang
  - Befolkningstetthet
  - Utetemperatur (årstid)
  - Tid på døgnet
  - Varighet
  - Avhengigheter i forhold til andre kritiske samfunnsfunksjoner
  - Substitusjonsmuligheter, erstatning av komponenter, omgåelse av feil
  - Grad av kobling
  - Kultur
  - Mental forberedelse

- Sannsynlighet i 5 konkrete trinn
  - Mindre enn 1 gang pr 1000 år
  - 1 gang pr 100-1000 år
  - 1 gang pr 10-100 år
  - 1 gang pr 1-10 år
  - Mer enn 1 gang pr år

- 5 konsekvenskategorier i 5 konkrete trinn hver
  - Liv og helse
  - Livsmiljøet
  - Økonomi
  - Styringsevne
  - Politisk atferd/tillit

- Risikomatrise 5 x 5, 5 risikokategorier

Det forutsettes dessuten at det utvikles en enkel standard database for å håndtere disse informasjonene på tvers av virksomheter og samfunnssektorer. Dette vil muliggjøre sortering av data etter ønsket variabel tilpasset den konkrete problemstillingen. Arbeidet med å spesifisere hvordan en slik database kan bygges opp har startet opp i BAS5.

Metodikken har foreløpig ikke vært anvendt (annet enn i mindre tester). Det kan selvfølgelig reises flere innvendinger mot dette, ikke minst fordi flere prosjektrådsmedlemmer har ønsket konkrete prioriteringslister innenfor utvalgte områder. Dels har dette vært et spørsmål om

kapasitet. Arbeidet med å utvikle metodikken viste seg raskt å være vesentlig mer komplekst og arbeidskrevende enn opprinnelig antatt. Den viktigste årsaken er likevel at prosjektet på flere områder ser store problemer med å utvikle statiske lister, som er allmenngyldige på tvers av ulike scenarier. Et eksempel er ønsket om å innføre en prioriteringsordning innen mobiltelefoni, slik at viktige aktører i krisesituasjoner er sikret tilgang i perioder der kapasiteten ikke er tilstrekkelig. Hvilke aktører som er involvert vil imidlertid variere sterkt fra krise til krise. En liste som er satt opp basert på et typisk akutt redningsscenario (f.eks. en større trafikkulykke) er ikke nødvendigvis den riktige i en situasjon der en infrastruktur svikter (f.eks. at et område mister strømmen i lengre tid). Selv innenfor en hovedklasse av scenarier kan aktørtypen variere, avhengig av forhold som scenariets geografiske omfang, varighet, andre samtidige hendelser i samfunnet osv. På forhånd oppsatte prioriteringslister kan derfor virke mot sin hensikt.

7.2 Anbefalinger og videre arbeid

Metoden som er presentert har potensielle anvendelser for et bredt spekter av problemstillinger. Eksempler på slike er:

- Hvem bør ha prioritert tilgang til kommunikasjonstjenester i krisesituasjoner?
- Hvem bør få vaksine i en pandemisituasjon og i hvilken rekkefølge?
- Hvilke virksomheter skal prioriteres ved kraftrasjonering?
- Hvor lønner det seg å sette inn investeringer for å forebygge kriser?
- Hvilke installasjoner bør prioriteres for fysisk beskyttelse?
- Hvilke virksomheter bør være underlagt Sikkerhetslovens bestemmelser?
- Hva bør bygges opp igjen først etter en naturkatastrofe?
- Hvilke samfunnsområder bør ha særlig oppmerksomhet omkring ROS-vurderinger?

Det anbefales *ikke* at metodikken anvendes til å utvikle generelle, fastsatte prioriteringslister som forventes å ha allmenn gyldighet og lang varighet. Prioriteringer kan imidlertid gi mening innenfor flere konkrete problemstillinger, hvor mange rammebetingelser er lagt. Det anbefales derfor at metoden testes ut i forlengelsen av BAS5. Dette kan være mulig i forhold til en kommende ROS-analyse i Stavangerområdet, og også i forhold til eventuelle ROS-prosesser i ulike departementer.

Metodikken er utarbeidet uten at en spesifisert ”eier” står klar til å ta den i bruk. Imidlertid er det enkelte tverrsektorielle direktorater innenfor samfunnssikkerhetsarbeidet, spesielt DSB eller NSM, som kanskje er de mest åpenbare kandidatene til å ta arbeidet med metodikken videre. Det anbefales derfor at DSB og NSM utnytter oppdukkende anledninger til å presentere metoden og forsøker å få til en tverrfaglig prosessforankring.

I tillegg bør modellen suppleres med utvikling av prosesser og teknikker som er spesielt rettet mot oppdagelse og persepsjon av hittil ukjent risiko, for eksempel scenarieteknikker, *foresight*-teknikker eller *horizon scanning*-teknikker.

Det foreslåtte hierarkiet over hendelser bør utvikles videre og underkastes nærmere analyse med

hensyn på å identifisere de viktigste og mest fruktbare scenariene og sile fra scenarier som er mindre plausible.[34]

[34] Eksempelvis morfologisk analyse

Appendix A Litteraturliste

Abel, Carl Georg. 2003. Utkast*: Beskrivelse: Planlegging og gjennomføring av roterende sonevis utkobling*.

Abel, Carl Georg. 2003 Utkast: *Kvoterasjonering*.

Abel, Carl Georg. 2003. Utkast: *Problemstillinger og samfunnskonsekvenser ved strømutkobling*.

Anton, et. al. 2003 *The vulnerability assessment & mitigation methodology (VAM)*. Rand.

Aven, Terje. 2007. A unified framework for risk and vulnerability analysis and management covering both safety and security security. Reliability Engineering and System Safety 92, 745-754

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

Department for Homeland Security. 2006. *Revised Draft, National Infrastructure Protection Plan v2.0 Januar 2006, Appendix 3A: NIPP Baseline Criteria for Assessment Methodologies.* http://www.ni2ciel.org/NIPC/Revised-Draft-NIPP-v2.0.pdf

HM Government, London 2005. *Emergency Preparedness: Guidance on Part 1 of the Civil Contingencies Act 2004, its associated Regulations and non-statutory arrangements*, Annex 4 A-F (November 2005).

Hirschman, Albert O, Exit, Voice, and Loyalty. 1970. *Responses to Decline in Firms, Organizations, and States*. Harvard University Press 1970. Videreutviklet av Caryl Rusbult m fl mht begrepet Neglect. (Rusbult, C. E., Zembrodt, I. M., & Gunn, L. K. 1982. *Exit, voice, loyalty, and neglect: Responses to dissatisfaction in romantic involvements.* Journal of Personality and Social Psychology, 43, 1230-1242.

Hokstad, Per. 2005. *Overordnet risiko- og sårbarhetsanalyse for samferdselssektoren*. SINTEF rapport STF50 A05152, 2005.

Hokstad, Per. Jersin, Erik. Rossnes, Ragnar. Steiro, Trygve. Tinmannsvik, Ranveig K. 2002. *Risiko på tvers (RPT).*

Klinke & Renn. 2002. *A New Approach to Risk Evaluation and Management: Risk-based, Precaution-based, and Discourse-based Strategies.* Risk Analysis, 22(6), 1071-1094.

Sosial- og helsedirektoratet. 2006. *Nasjonal ROS- og beredskapsanalyse innen helse*. Hovedrapport januar 2006.

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.*

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

Samfunnssikkerhet og risikoforskning (SAMRISK). Innstilling fra en utredningsgruppe nedsatt av Norges forskningsråd. 29. april 2005.

SEROS rapport 91892. 2007. *Utvikling av metodikk for risikoanalyse av samfunnskritisk IKT*.

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

SØRLI Kjetil, HENRIKSEN Stein, BOGEN Lene, MØRKESTØL Kristin. 2007. *Bakgrunnsstudie til metode for rangering og identifisering av samfunnskritiske funksjoner.* FFI/RAPPORT-2007/00875.

Wiencke, H.S. Aven, T. Hagen, J. 2006. *A framework for selection of methodology for risk and vulnerability assessments of infrastructures depending on ICT*. ESREL 2006, pp. 2297-2304.

Appendix B Samfunnskritiske funksjoner, hierarkisk utvidet liste

Nivå 1 Hoved-inndeling	Nivå 2 Sektorer	Nivå 3 Undersektorer	(Nivå 4 Evt klasser)	(Nivå 5 Adresser, koordinater)	(Nivå 6 Stillinger, personer)	Referanse-nummer
Kritisk infrastruktur, grunnleggende (S)	Elektrisk kraft (1)	Produksjonsanlegg (1)	Kl 1			S111
			Kl 2			S112
			Kl 3			S113
		Stamnettet (2)	Kl 1			S121
			Kl 2			S122
			Kl 3			S123
		Fordelings- og distribusjonsnett (3)	Kl 1			S131
			Kl 2			S132
			Kl 3			S133
		Dammer, demninger (4)				S14
		Styringssentraler og SCADA-systemer (5)				S15
		Mobile reservesystemer (6)				S15
	Elektronisk kommunikasjon (2)	Fast telefoni og kabelsystemer (1)	Nasjonale sentraler			S211
			Noder			S212
			Viktige sentralbord og andre viktige brukerapplikasjoner			S213
		Mobiltelefoni (2)	Nasjonale sentraler			S221
			Noder			S222
			Basestasjoner			S223
		Internett (3)	NIXer og tilsvarende			S231
			Internett Service Providers			S232
		Lukkede sambandssystemer for myndigheter (4)	Forsvarets digitale nett			S241
			Redningsnett			S242
		Radiokommunikasjon (5)	Luftkontrollsentraler			S251
			Kystradio			S252
			Kringkasting			S253
		Satelittbaserte infrastrukturer, jordstasjoner (6)	For Meteorologi, Kommunikasjon, Kringkasting, Navigasjon, Miljøovervåking			S26
		Mobile reservesystemer (7)				S27
Kritisk infrastruktur, øvrig (K)	Vann og avløp (1)	Vannkilder (1)				K11
		Reservesystemer for vann (2)				K12
		Renseanlegg (3)				K13
		Distribusjonsnett (4)				K14
		Kloakksystem (5)				K15
		Styringssentraler og SCADA-systemer (6)				K16
	Olje- og gassforsyning	Offshore installasjoner (1)				K21

Nivå 1 Hoved-inndeling	Nivå 2 Sektorer	Nivå 3 Undersektorer	(Nivå 4 Evt klasser)	(Nivå 5 Adresser, koordinater)	(Nivå 6 Stillinger, personer)	Referanse-nummer
	(2)	Rørledninger (2)				K22
		Landterminaler og raffinerier (3)				K23
		Depoter (4)				K24
		Styringssentraler og SCADA-systemer (5)				K25
	Transport (3)	Flyplasser (1)				K31
		Jernbanestasjoner og -terminaler (2)				K32
		Vegtransportterminaler (3)				K33
		Sjøterminaler, havner (4)				K34
	Bank og finans (4)	Nasjonale clearingsystemer (1)				K41
		Betalingsformidlings-systemer (2)				K42
		Systemer for verdipapiravregning (3)				K43
Andre kritiske samfunns-funksjoner (A)	Matforsyning (1)	Systemer for logistikk (1)				A11
		Hygiene og sikkerhet (2)				A12
	Renovasjon (2)	Avfallstransport (1)				A21
		Avfallsdeponi (2)				A22
	Helse-, sosial- og trygdetjenester (3)	Spesialisthelsetjenestens hospitaler (1)				A31
		Primærhelsetjenester (2)				A32
		Sosialtjenester (3)				A33
		Medisinalforsyning (4)				A34
		Laboratorier (5)				A35
		Trygdesystemer (6)				A36
	Politi og Nød- og redningstjenester (4)	Politiregistre (1)				A41
		HRS; LRS; politikammer (2)				A42
		AMK (3)				A43
		Brannvakt (4)				A44
	Offentlig ledelse (5)	Storting (1)				A51
		Regjering og administrasjon, Kriseledelse (2)				A52
		Domstolene (3)				A53
		Forsvarets ledelse (4)				A54
	Medier, nyhetsformidling (6)	Radio- og TVselskaper (1)				A61
		Presse, trykt (2)				A62
		Internettaviser (3)				A63
		Offentlige informasjonstjenester (4)				A64

Nivå 1 Hoved-inndeling	Nivå 2 Sektorer	Nivå 3 Undersektorer	(Nivå 4 Evt klasser)	(Nivå 5 Adresser, koordinater)	(Nivå 6 Stillinger, personer)	Referanse-nummer
	Industrier, viktige og/ eller med potensial for store ulykker (7)	Kjemiske anlegg og depoter (1)				A71
		Atomreaktorer og nukleærdeponier (2)				A72
		Forsvarsindustri (3)				A73
		Styringssentraler og SCADA-systemer (4)				A74
	Nasjonale nøkkelsymboler (8)	Vernede bygninger, kulturinstitusjoner og monumenter (1)				A81
		Mobile gjenstander, ”umistelige” (2)				A82
		Evenementer, institusjonaliserte (3)				A83
		Personer, institusjonaliserte (4)				A84

Vurderinger på nivå 5 og 6, muligens nivå 4, kan potensielt inneholde GRADERT informasjon.

Appendix C Hendelsestypologi, hierarkisk utvidet liste

Nivå 1	Nivå 2	Nivå 3	Nivå 4	(Nivå 5 Konkretiserte scenarier)	Referanse-nummer
Naturkatastrofe (N)	Meteorologisk (M)	Sterk vind (1)	Storm, orkan (1)		NM11
			Trombe, tornado (2)		NM12
		Flom (2)	Vårflom (1)		NM21
			Stormflom (2)		NM22
			Springflo (3)		NM23
		Klimaendring med heving av værmessige gjennomsnittsverdier (3)	Heving av havnivå (1)		NM31
			Temperaturøkning (2)		NM32
			Nedbørøkning (3)		NM33
	Geologisk/ Geoteknisk (G)	Snøras (1)	Snøras over infrastruktur (1)		NG11
			Snøras over bebyggelse (2)		NG12
		Fjell-, jordras (2)	Ras over infrastruktur (1)		NG21
			Ras over bebyggelse (2)		NG22
			Ras ned i vann (3)		NG23
		Jordskjelv (3)	Under 5 Richter i Norge (1)		NG31
			5 Richter eller mer i Norge (2)		NG32
		Tsunami (4)	Nasjonalt omfang, Norge (1)		NG41
			Regionalt omfang, rammer nordmenn i utlandet (2)		NG42
			Globalt omfang (3)		NG43
		Vulkanisme (5)	Rammer nordmenn i utlandet (1)		NG51
			Nedfall i Norge (2)		NG52
		Calderaeksplosjon (6)	Regionalt omfang, rammer nordmenn i utlandet (1)		NG61
			Globalt omfang, nedfall i Norge, verdensøkonomien rammes (2)		NG62
	Brann, naturlig (B)	Skog-, lyng-, gressbrann (1)	Brann ved infrastruktur (1)		NB11
			Brann ved bebyggelse (2)		NB12
	Kosmisk (K)	Meteoritt (asteroide) (1)	Nasjonalt omfang (1)		NK11
			Regionalt omfang (2)		NK12
			Globalt omfang (3)		NK13
		Komet (2)	Landsdels omfang (1)		NK21
			Nasjonalt omfang (2)		NK22
Medisinsk/ biologisk katastrofe (B)	Planter og dyr (P)	Overførbar sykdom (1)	Zoonotisk (mellom dyr og menneske) (1)		BP11
			Ikke-zoonotisk (2)		BP12
	Mennesker (M)	Pandemi (1)	Influensa (1)		BM11
			SARS (2)		BM12
			Hemoragisk feber, smittsom (3)		BM13
Teknisk katastrofe (T)	Ulykkesbasert (U)	Utslipp av farlige stoffer (1)	Giftige kjemikalier (1)		TU11
			Seveso-anlegg (2)		TU12
			Atomreaktor (3)		TU13
			Andre radiologiske kilder (4)		TU14
			Biologisk utslipp (5)		TU15
			Maritim forurensing (6)		TU16
		Storbrann (2)	Gassterminal (1)		TU21
			Oljeraffineri (2)		TU22

Nivå 1	Nivå 2	Nivå 3	Nivå 4	(Nivå 5 Konkretiserte scenarier)	Referanse-nummer
			Drivstoffdepot (3)		TU23
			Rørledning på land (4)		TU24
			Oljeinstallasjon til sjøs (5)		TU25
		Eksplosjon (3)	Gassterminal (1)		TU31
			Oljeraffineri (2)		TU32
			Drivstoffdepot (3)		TU33
			Rørledning på land (4)		TU34
			Oljeinstallasjon til sjøs (5)		TU35
		Transportulykke (4)	Passasjerskip som synker eller brenner (1)		TU41
			Havneulykke (2)		TU42
			Flystyrt (3)		TU43
			Flystyrt i tettbygd område (4)		TU44
			Togulykke (5)		TU45
			Vegulykke, kjedekollisjon (6)		TU46
			Farlig gods (7)		TU47
		Strukturell kollaps (5)	Dambrudd (1)		TU51
			Broer (2)		TU52
			Bygninger (3)		TU53
	Leveransesvikt (i kritisk infrastruktur) (L)	Vannmangel (1)	Vannkilde (1)		TL11
			Vannverk og rensing (2)		TL12
			Ledningsnett (3)		TL13
		Matmangel (2)	Produksjon (1)		TL21
			Import (2)		TL22
			Distribusjon (3)		TL23
		Bortfall av avløp og renovasjon (3)	Kloakk (1)		TL31
			Overflatevann (2)		TL32
			Søppelbortkjøring (3)		TL33
		Bortfall av transporttjenester (4)	Luft (1)		TL41
			Bane (2)		TL42
			Veg (3)		TL43
			Sjø (4)		TL44
		Bortfall av finanstjenester (5)	BBS (1)		TL51
			VPS (2)		TL52
		Bortfall av energitilførsel (6)	Produksjon (1)		TL61
			Transformasjon (2)		TL62
			Hovednett (3)		TL63
			Regionalt og lokalt distribusjonsnett (4)		TL64
		Bortfall av IKT (7)	Fasttelefoni (1)		TL71
			Mobiltelefoni (2)		TL72
			Internettjenester (3)		TL73
Dysfunksjonelle menneskelige handlinger (D)	Individuelle (I)	Psykotiske (1)	Handlingslammelse i kritisk situasjon (1)		DI 11
			(Kriminell) Voldsbruk (2)		DI 12
		Uaktsomme (2)	Holdningssvikt, rigiditet (1)		DI 21
			Godtroenhet, selvfornøydhet (2)		DI 22
	Kollektive (K)	Systemsvikt (1)	Manglende kommunikasjon av målsetninger (1)		DK11
			Manglende kompetanseutvikling (2)		DK12

Nivå 1	Nivå 2	Nivå 3	Nivå 4	(Nivå 5 Konkretiserte scenarier)	Referanse-nummer
		Organisasjonssvikt (2)	Feil eller manglende plassering av ressurser (1)		DK21
			Manglende utarbeidelse av målsetninger (2)		DK22
		Målkonflikt (3)	Utsettende (forsinkende) atferd (1)		DK31
			Forfølging av irrelevante mål (2)		DK32
(Ondsinnet) handling mot Norge, norske borgere eller interesser (O)	Kriminalitet (K)	Organisert kriminalitet (1)	Smugling (1)		OK11
			Narkotika- og våpenomsetting (2)		OK12
			Menneskehandel (3)		OK13
			Datakriminalitet (4)		OK14
		Sabotasje (2)	Attentat mot installasjon (1)		OK21
			Voldelig protestaksjon, ”oppløp” (2)		OK22
			Hærverk (3)		OK23
			Datahærverk (4)		OK24
		Spionasje (3)	Politisk (1)		OK31
			Militær (2)		OK32
			Industriell (3)		OK33
	Terrorisme (T)	Konvensjonell terrorisme (1)	Attentat mot enkeltperson (1)		OT11
			Gisseltaking (2)		OT12
			Sprengstoffattentat mot folkeansamling (3)		OT13
		CBRN-terrorisme (2)	Kjemisk angrep (1)		OT21
			Biologisk angrep (2)		OT22
			Radiologisk angrep (3)		OT23
			Nukleært angrep (4)		OT24
	Sikkerhets-politisk utfordring i fred (S)	Nordområdene (1)	Ressursøkonomisk (1)		OS11
			Militær (2)		OS12
		Europeisk/Atlantisk (2)	Politisk/økonomisk press (1)		OS21
			Politisk/organisatorisk tilbakeslag (2)		OS22
		Global (3)	PKO/PSO-relatert		OS31
			Politisk/organisatorisk tilbakeslag (2)		OS32
	Krigføring (M)	Fysisk krigføring (1)	I Norge (1)		OM11
			Norges nærområder (2)		OM12
			Rammer norske interesser (3)		OM13
		Datanettoperasjoner (CNO) (2)	Distribuert angrep (1)		OM21
			Målrettet angrep (2)		OM22
			Målrettet angrep mot kritisk infrastruktur (3)		OM23

NB: flere av disse kan inngå i kjeder av årsak og virkning.