NOU Norges offentlige utredninger 2006: 6

Når sikkerheten er viktigst

Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner

Innstilling fra utvalg oppnevnt ved kongelig resolusjon 29. oktober 2004.
Avgitt til Justis- og politidepartementet 5. april 2006.

Departementenes servicesenter
Informasjonsforvaltning

Oslo 2006

ISSN 0333-2306
ISBN 82-583-0874-2
ISBN 978-82-583-0874-1

Lobo Media AS

Til Justis- og politidepartementet

Regjeringen oppnevnte ved kongelig resolusjon av 29. oktober 2004 et offentlig utvalg for å utrede sikring av landets kritiske infrastruktur.

Utvalgets utredning ble ferdigstilt 31. mars 2006. Utvalget legger med dette frem sin utredning. Samtlige av utvalgets anbefalinger er enstemmige.

Oslo, 5. april 2006

Sven Ullring
leder

Gerd Bjørhovde	Toril Hofshagen	Jon Lea
Einar Ellingsen	Grethe Høiland	Anne M. Reinsnes
Kåre Petter Hagen	Willy Jensen	Bjørn Tørmo

Dagfinn Buset
Sekretariatsleder

Bjørn Nilsen

Øyvind Mandt

Kjetil Sørli

Achilles-saken

Overvåkingspolitiet offentliggjorde i desember 1983 at det i august 1979 i en oppbevaringsboks på Oslo Østbanestasjon hadde blitt funnet dokumenter med detaljerte planer om å sprenge kraftstasjoner, rørledninger og linjemaster. Det var også fotografier av 11 norske kraftanlegg. Dokumentene kunne tyde på at det var drevet målrettet sabotasjetrening mot 35 norske kraftanlegg. Av disse var 19 nevnt ved navn, og var blant de største og mest sentrale i den norske kraftforsyningen. Det var også laget en oversikt over samkjøringen av all elektrisk kraft i Norge og med overføringslinjene til Sverige markert. Til og med en overføringslinje som ennå ikke var bygget i 1979, var inntegnet. Dette tydet på at den eller de som hadde utarbeidet disse dokumentene, hadde detaljkunnskap og tilgang til opplysninger som ikke var vanlig kjent.

Tore Bjørgo. Norske dammer – i hvilken grad er de sannsynlige terror- og sabotasjemål? Revidert utgave, april 2003. Norsk Utenrikspolitiske Institutt.

Isstormen i Canada

I januar 1998 mistet 1,4 millioner kunder i Quebéc (Canada) strømmen etter hvert som området ble rammet av en kraftig isstorm. Kombinasjonen av underkjølt regn og kraftig vind gjorde at infrastrukturen iset ned, og mange kraftlinjer falt som følge av belastningen[...]. Selv om det lyktes kraftselskapet i området å gjenopprette forsyningen til de største brukergruppene innen én uke, opplevde en del kunder strømbrudd i opptil én måned. [...] Normalt samfunnsliv gikk [...] i stå. Økonomien stoppet opp, og folk kom seg ikke på jobb. Det oppstod problemer med oppbevaring og tilberedning av mat, hygiene og tilgang på kontanter. Om lag 10 % av befolkningen, i stor grad eldre og uføre, trengte hjelp som følge av kraftbruddet. Primært gjaldt dette innkvartering og pleie. Det oppstod store forstyrrelser i tilgangen på arbeidskraft. En av årsakene var at folk holdt seg hjemme for å ta vare på familien i stedet for å gå på jobb.

Håvard Fridheim, Janne Hagen og Stein Henriksen. En sårbar kraftforsyning Sluttrapport etter BAS3. FFI/RAPPORT-2001/02381.

Innhold

Del I **Utvalgets utredning** 13

1 **Sammendrag** 15
1.1 Kapittelinnhold 15
1.2 Utvalgets anbefalinger 17
1.2.1 Utvalgets anbefalinger i kapittel 5 – Ansvar for beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner 17
1.2.2 Utvalgets anbefalinger i kapittel 6 – Virkemidler 19
1.2.3 Utvalgets anbefalinger i kapittel 7 – Sikkerhetsloven og den forebyggende sikkerhetstjenesten 20
1.2.4 Utvalgets anbefalinger i kapittel 8 – Ivaretakelse av sikkerhets- og beredskapshensyn ved omreguleringer og omorganiseringer 21
1.2.5 Utvalgets anbefalinger i kapittel 9 – Offentlig eierskap 21
1.2.6 Utvalgets anbefalinger i kapittel 10 – Kartlegging av kritisk infrastruktur og sektorvise anbefalinger 22
1.2.6.1 Elektronisk kommunikasjon 22
1.2.6.2 Satellittbasert kritisk infrastruktur ... 23
1.2.6.3 Kraft 23
1.2.6.4 Vann og avløp 24
1.2.6.5 Olje og gass 25
1.2.6.6 Transport 25
1.2.7 Utvalgets anbefalinger i kapittel 11 – Kartlegging av kritiske samfunnsfunksjoner og sektorvise anbefalinger 25
1.2.7.1 Bank og finans 25
1.2.7.2 Matforsyning 25
1.2.7.3 Helse-, sosial- og trygdetjenester 25
1.2.7.4 Politi 26
1.2.7.5 Nød- og redningstjeneste 26
1.2.7.6 Kriseledelse 26
1.2.8 Utvalgets anbefalinger i kapittel 13 – Forskning og utredning 28

2 **Oppnevning, mandat og arbeid** ... 29
2.1 Oppnevning og sammensetning av utvalget 29
2.2 Mandat 29
2.3 Arbeidsmetode 30

3 **Sentrale begreper** 32
3.1 Kritisk infrastruktur og kritiske samfunnsfunksjoner 32
3.2 Rikets sikkerhet og vitale nasjonale interesser 34
3.3 Risiko 35
3.4 Sårbarhet 35
3.5 Trussel 36
3.6 Samfunnssikkerhet 36
3.7 Totalforsvar og sivilt-militært samarbeid 37
3.8 Beredskap og forebygging 38
3.9 Befolkningens trygghetsfølelse 38
3.10 *Safety* og *Security* – på norsk 38

4 **Sikkerhetsutfordringer** 40
4.1 Nye sikkerhetspolitiske utfordringer 40
4.2 Sikkerhetsutfordringer – kritisk infrastruktur og kritiske samfunnsfunksjoner 41
4.2.1 Klimaendringer/naturkatastrofer 41
4.2.2 Aldring i kritisk infrastruktur 42
4.2.3 Terrorisme og organisert kriminalitet 43
4.2.4 Omorganisering, omregulering og bortsetting 43
4.2.5 Globalisering 44
4.2.6 Elektronisk kommunikasjon 44
4.2.6.1 Angrep på datanettverk 45
4.2.7 Etterretningsvirksomhet 46
4.2.8 Gjensidige avhengigheter 46
4.3 Sentrale aktører og deres rapportering om sikkerhetsutfordringene 46

5 **Ansvar for beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner** 49
5.1 Myndighetsansvar fordelt på sektorer 49
5.2 Utviklingen av Justis- og politidepartementets samordningsrolle 51
5.3 Privat sektors samfunnsansvar 53
5.3.1 Ivaretakelse av samfunnsansvar 54
5.3.2 Samarbeid på tvers av offentlig og privat sektor 55
5.4 Utvalgets anbefalinger 56
5.4.1 Forslag knyttet til tydeliggjøring av Justis- og politidepartementets rolle 56
5.4.2 Forslag knyttet til tydeliggjøring av nasjonale mål/akseptnivå 57
5.4.3 Forslag knyttet til forholdet mellom NSM, PST og DSB 57
5.4.4 Forslag knyttet til prinsipper for god sikkerhetskultur 58

6 Virkemidler 60
6.1 Juridiske virkemidler 60
6.1.1 Lovgivning 60
6.1.2 Konsesjoner 61
6.1.3 Enerett- og monopolordninger 61
6.2 Organisatoriske virkemidler - tilsynsorganer 61
6.3 Økonomiske virkemidler 61
6.3.1 Avgifter og gebyrer 61
6.3.2 Kjøp av tjenester - tilskudd 62
6.4 Pedagogiske virkemidler 62
6.5 Eierstyring 62
6.5.1 Kontroll med eierstyring 63
6.6 Utvalgets anbefalinger 63
6.6.1 Forslag knyttet til lovregulering 63
6.6.1.1 Forslag knyttet til generell lov om beredskap 64
6.6.1.2 Behovet for å se næringslivets rolle under ett 66
6.6.1.3 Forslag knyttet til revisjon av sivilforsvarsloven 66
6.6.1.4 Forslag knyttet til forsyningsloven . 67
6.6.1.5 Forslag knyttet til plan- og bygningsloven 67
6.6.2 Forslag knyttet til tilsynsvirksomhet 68
6.6.3 Forslag knyttet til etablering av tilskuddsordning 69
6.6.4 Forslag knyttet til offentlige innkjøp 71
6.6.5 Forslag knyttet til bruk av standarder og standardiserte metoder 71
6.6.6 Forslag knyttet til samarbeid og informasjonsdeling 72

7 Sikkerhetsloven og den forebyggende sikkerhetstjenesten 75
7.1 Bakgrunn for Lov om forebyggende sikkerhetstjeneste 75
7.1.1 Lovens formål. Ansvar og utførelse . 75
7.1.2 Hva er forebyggende sikkerhetsarbeid? 76
7.1.3 Rikets sikkerhet og vitale nasjonale sikkerhetsinteresser 76
7.2 Om lovens virkeområde 76
7.2.1 Har loven et tilstrekkelig virkeområde i dag? 77
7.2.2 Privatrettslige virksomheter som er omfattet av sikkerhetsloven 77
7.3 De sentrale elementene som utgjør virkemidlene i loven 77
7.3.1 Personellsikkerhet 78
7.3.2 Hvem kan det kreves sikkerhetsklarering for? 78
7.3.3 Forskrift om informasjonssikkerhet 79
7.3.4 Forskrift om sikkerhetsgraderte anskaffelser 79
7.3.5 Om objektsikkerhet 79
7.4 Om forholdet til andre lover og (sektorvise) bestemmelser 80
7.5 Utvalgets anbefalinger 81
7.5.1 Forslag knyttet til objektsikkerhet 81
7.5.2 Forslag knyttet til sikkerhetslovens virkeområde 82
7.5.2.1 Virksomhetsklarering med hjemmel i sikkerhetsloven 83

8 Ivaretakelse av sikkerhets- og beredskapshensyn ved omreguleringer og omorganiseringer 84
8.1 Drivkreftene bak omregulering og privatisering 84
8.1.1 Knappe offentlige budsjetter og stadig økende etterspørsel etter offentlige tjenester 84
8.1.2 Den teknologiske utvikling 84
8.1.3 Internasjonalisering og globalisering. 85
8.2 Hensynet til sikkerhet og beredskap 85
8.3 Virkemiddelbruk for ivaretakelse av sikkerhet og beredskap i omregulerings- og omorganiseringsprosesser 86
8.4 Finansiering av beredskapstiltak 86
8.5 Utvalgets anbefalinger 86
8.5.1 Forslag knyttet til innføring av kontrollpunkter ved omreguleringer og omorganiseringer 86
8.5.2 Forslag knyttet til å holde sikkerhets- og beredskapsmessige oppgaver som en integrert del av virksomheten 88
8.5.3 Forslag knyttet til sammefallende omstillinger i en sektor 88

9 Offentlig eierskap 89
9.1 Utøvelse av det statlige eierskap 89
9.1.1 De konstitusjonelle forhold 89
9.1.1.1 Forvaltningen av det statlige eierskapet 89
9.1.1.2 Stortingets kontroll av det statlige eierskapet 89
9.1.1.3 Regjeringens forvaltning av eierskapet 90
9.1.1.4 Rolledelingen Regjering – Storting i eiersaker 90
9.1.2 Praktisk eierutøvelse – Beskrivelse av arbeidet rettet mot selskapene 90
9.1.2.1 Generelt 90
9.1.2.2 Valg av styre 91
9.1.2.3 Avkastningskrav og utbyttepolitikk .. 91

9.2 Generelle begrunnelser for statlig inngripen i markedsøkonomien 92
9.3 Privat eller offentlig eiet virksomhet? 92
9.4 Eierskap til kritisk infrastruktur 93
9.5 Eiermessig skille eller integrasjon mellom forvaltning av kritisk infrastruktur og konkurransevirksomhet? 95
9.6 Forholdet mellom regulering og eierskap som virkemiddel 96
9.7 Utvalgets anbefalinger 97

10 Kartlegging av kritiske infrastrukturer og sektorvise anbefalinger . 99
10.1 Elektronisk kommunikasjon 99
10.1.1 Overordnet beskrivelse av infrastruktur og samfunnsfunksjon 100
10.1.2 Særskilt om Internett 100
10.1.2.1 Sårbarheter 101
10.1.3 Beskrivelse av eierforhold og organisering 102
10.1.4 Utvalgets vurderinger og anbefalinger knyttet til virkemidlene 103
10.1.4.1 Eierskap som virkemiddel 103
10.1.4.2 Regulatoriske virkemidler 104
10.1.4.3 Økonomiske virkemidler 109
10.1.5 Nødnettet 109
10.2 Satellittbasert kritisk infrastruktur ... 111
10.2.1 Overordnet beskrivelse av infrastruktur og samfunnsfunksjon 111
10.2.2 Utvalgets vurderinger knyttet til virkemidlene 113
10.3 Kraft 113
10.3.1 Overordnet beskrivelse av infrastruktur og samfunnsfunksjon 114
10.3.2 Beskrivelse av eierforhold og organisering. 115
10.3.2.1 Produksjon (kraftverkene) 115
10.3.2.2 Distribusjon 116
10.3.2.3 Omsetning 116
10.3.2.4 Privat eierskap 116
10.3.2.5 Vertikal integrering 116
10.3.3 Utvalgets vurderinger og anbefalinger knyttet til virkemidlene 117
10.3.3.1 Eierskap som virkemiddel 117
10.3.3.2 Regulatoriske virkemidler 119
10.3.3.3 Økonomiske virkemidler 120
10.4 Vann og avløp (VA) 120
10.4.1 Overordnet beskrivelse av infrastruktur og samfunnsfunksjon 121
10.4.2 Beskrivelse av eierforhold og organisering 122
10.4.3 Utvalgets vurderinger og anbefalinger knyttet til virkemidlene 123
10.4.3.1 Eierskap som virkemiddel 123
10.4.3.2 Regulatoriske virkemidler 124
10.4.3.3 Økonomiske virkemidler 126
10.5 Olje og gass 126
10.5.1 Overordnet beskrivelse av infrastruktur og samfunnsfunksjon 127
10.5.2 Beskrivelse av eierforhold og organisering 127
10.5.2.1 Produksjon og omsetning 127
10.5.2.2 Transmisjon 129
10.5.3 Nye bruksområder for gass i Norge 129
10.5.4 Utvalgets vurderinger og anbefalinger knyttet til virkemidlene 129
10.5.4.1 Eierskap som virkemiddel 129
10.5.4.2 Regulatoriske virkemidler 130
10.5.4.3 Økonomiske virkemidler 131
10.6 Transport 131
10.6.1 Overordnet beskrivelse av infrastruktur og samfunnsfunksjon 132
10.6.2 Beskrivelse av eierforhold og organisering 132
10.6.3 Utvalgets vurderinger og anbefalinger 134

11 Kartlegging av kritiske samfunnsfunksjoner og sektorvise anbefalinger 136
11.1 Bank og finans 136
11.1.1 Beskrivelse av samfunnsfunksjonen 136
11.1.2 Beskrivelse av eierforhold og organisering 138
11.1.3 Utvalgets vurderinger og anbefalinger 139
11.2 Matforsyning 140
11.2.1 Beskrivelse av samfunnsfunksjonen 140
11.2.2 Beskrivelse av eierforhold og organisering 141
11.2.3 Utvalgets vurderinger og anbefalinger 141
11.3 Helse, sosial og trygdetjenester 142
11.3.1 Beskrivelse av samfunnsfunksjonen 142
11.3.2 Beskrivelse av eierforhold og organisering 143
11.3.3 Utvalgets vurderinger og anbefalinger 144
11.4 Politi 144
11.4.1 Beskrivelse av samfunnsfunksjonen 144
11.4.2 Organisering 145
11.4.3 Utvalgets vurderinger og anbefalinger 145
11.5 Nød- og redningstjeneste 146
11.5.1 Beskrivelse av samfunnsfunksjonen 146
11.5.2 Organiseringen av nød- og redningstjenestene 148
11.5.3 Utvalgets vurderinger og anbefalinger 149

11.5.3.1 Forslag knyttet til samvirkeprinsippet 149
11.5.3.2 Forslag til styrking av beredskapen ved ekstraordinære hendelser. 149
11.6 Kriseledelse 149
11.6.1 Beskrivelse av samfunnsfunksjonen 149
11.6.2 Nasjonal kriseledelse 150
11.6.2.1 Behovet for nasjonal kriseledelse 150
11.6.2.2 Beskrivelse av ansvarsforhold og organisering 150
11.6.2.3 Beredskapsutvalget 151
11.6.2.4 Kontaktgruppen 151
11.6.2.5 Kriseledelse ved terror- og sabotasjesituasjoner 151
11.6.3 Regional kriseledelse og regionalt sikkerhetsarbeid 153
11.6.4 Lokal kriseledelse og lokalt sikkerhetsarbeid 154
11.6.4.1 Kommunen som myndighet 154
11.6.4.2 Kommunen som tjenesteyter 154
11.6.4.3 Kommunen som samfunnsaktør 154
11.6.4.4 Kommunens rolle ved kriser 155
11.6.4.5 Kriseforebyggende arbeid og beredskap i kommunene 155
11.6.5 Utvalgets vurderinger og anbefalinger 156
11.6.5.1 Forslag knyttet til kriseledelsesapparatet 156
11.6.5.2 Forslag knyttet til trossamfunnenes rolle i forebygging og håndtering av kriser 157
11.6.5.3 Forslag knyttet til varsling av befolkningen 158

12 Beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner i andre land 159
12.1 USA 159
12.2 Canada 161
12.3 Sverige 162
12.4 Tyskland 163
12.5 Nederland 164
12.6 Storbritannia 165
12.7 Sveits 166
12.8 Singapore 167
12.9 EU – European Programme for Critical Infrastructure Protection - EPCIP 169
12.10 NATO 169

13 Forsknings- og utredningsaktiviteter 170
13.1 Sårbarhetsutvalgets utredning 170
13.2 Pågående og avsluttede aktiviteter .. 170
13.3 Utvalgets vurderinger og anbefalinger 172
13.3.1 Forslag knyttet til utvidelse av Forsvarets forskningsinstitutts mandat 172
13.3.2 Forslag knyttet til forskningsprogrammet SAMRISK 172
13.3.3 Forslag om å gi prioritet til sikkerhet og beredskap i forskningsprogrammer ved Norges forskningsråd 173
13.3.4 Forslag knyttet til Konsortium for forskning på terrorisme og internasjonal kriminalitet 173
13.3.5 Forslag knyttet til forskning på gjensidige avhengigheter i kritisk infrastruktur 173

14 Økonomiske og administrative konsekvenser 175
14.1 Generelt 175
14.1.1 Balansering av kostnader 175
14.2 Forslag som gjelder regulatoriske virkemidler 176
14.2.1 Forslag om å utarbeide en generell, sektorovergripende lov om beredskap 176
14.2.2 Forslag knyttet til sikkerhetsloven ... 176
14.2.3 Forslaget om lovbestemt offentlig eierskap i vann- og avløpssektoren ... 176
14.3 Forslag angående krav til teleoperatører 177
14.4 Forslag som gjelder organisatoriske virkemidler 177
14.5 Forslag som gjelder økonomiske virkemidler 177
14.5.1 Forslag om en økonomisk tilskuddsordning 177
14.5.2 Forslag knyttet til forskning og utredning 177

Litteraturliste 178

Møteliste 181

Forkortelser 183

Del II Vedlegg 185

Vedlegg
1 Hva er kritisk infrastruktur? 187
2 Notat – om definisjonen av kritisk infrastruktur 197
3 Sårbarhet i kritisk infrastruktur – utfordringer 203

4 Notat – Et blikk på begrepet samfunnssikkerhet for å operasjonalisere «nasjonal trygghetsfølelse» 221
5 Sikkerhet - Safety/Security 226
6 Risikobildet 231
7 Oppfølgingen av sårbarhetsutvalgets forslag 244
8 Statlige styringsvirkemidler-Sikkerhet og beredskap..... 254
9 Rammeverk for gjennomføring av risiko og sårbarhetsanalyser av samfunnskritisk infrastruktur 262
10 Ivaretakelse av sikkerhet og beredskap i fristillingsprosesser..... 268
11 Navigasjonssystemer og samfunnssikkerheten 282
12 Notat 2005-056 Kritisk infrastruktur og offentlig eierskap..... 289
13 Tabell over ytre etater (direktorater og tilsyn) som har ansvar for sikkerhet som en del av sin virksomhet..... 315

Vedlegg 1-12 er skrevet på oppdrag fra infrastrukturutvalget.

Del I
Utvalgets utredning

Kapittel 1
Sammendrag

Utbygging av ulike infrastrukturer og samfunnsfunksjoner var en forutsetning for fremveksten av det moderne velstandssamfunnet i etterkrigstiden. Samfunnet ble etter hvert svært avhengig av de ulike infrastrukturene og samfunnsfunksjonene. Trusselen fra den kalde krigen la rammen for sikkerhetstiltakene. Etter den kalde krigen ble utforming og bruk av infrastrukturene og samfunnsfunksjonene først og fremst drevet frem av markedskrefter, teknologisk utvikling og et ønske om effektiv og økonomisk drift. Etter hvert og delvis parallelt med dette økte bevisstheten om samfunnets teknologiske avhengighet, og begrepet «et sårbart samfunn» ble etablert med utgivelsen av sårbarhetsutvalgets rapport i 2000.[1] En del av sårbarhetsutvalgets anbefalinger ble fulgt opp, og bidro på den måten til å styrke samfunnet sikkerhets- og beredskapsarbeid.

Utfordringer knyttet til «et sårbart samfunn» er like aktuelle i dag som i 2000. «Nye» sikkerhetsutfordringer som terrorisme og konsekvenser av klimaendringer berører samfunnet som helhet, og er særskilte utfordringer for sikkerheten i virksomheter som har ansvar for kritiske infrastrukturer og kritiske samfunnsfunksjoner. Disse virksomhetene må ha evne til å håndtere både nye og gamle sikkerhetsutfordringer, enten disse skyldes utilsiktede eller tilsiktede uønskede hendelser.

Samfunnets raske endringstakt og høye krav til inntjening og produksjon, gjør at det er viktig å ha evne til å omstille seg til nye faglige, teknologiske og organisatoriske krav i en virksomhet. Samtidig må evnen til omstilling ikke bare avgrense seg til disse forholdene. Like viktig er det å ivareta hensynet til sikkerhet ved omstillinger. Virksomheter med en god sikkerhetskultur vil evne å ta inn over seg slike forhold. For politiske myndigheter er det viktig å sikre at summen av ulike omstillinger på tvers eller innenfor en sektor ikke reduserer den samlede sikkerheten for samfunnet.

Offentlig eierskap som virkemiddel for å sikre kritiske infrastrukturer og kritiske samfunnsfunksjoner må vurderes konkret innenfor hver enkelt virksomhet og sektor. Valg av eierskap må skje på grunnlag av en helhetsvurdering der ønskeligheten av offentlig kontroll veies opp mot eventuelle bedriftsøkonomiske fordeler ved privat eierskap. Hensynet til samfunnsmessig sikkerhet og beredskap må veie tungt for infrastrukturer og samfunnsfunksjoner som har karakter av å være kritiske.

Norge er i det daglige preget av god sikkerhet. Vi er vant til at de aller viktigste varene og tjenestene blir levert som forventet, og de er som regel trygge å forholde seg til. Det er etablert beredskap for å håndtere de fleste uønskede situasjonene som oppstår. Samfunnets evne til å håndtere dagligdagse ulykker og uhell er også god. Likevel gjør høy kompleksitet i og stor avhengighet av kritiske infrastrukturer og kritiske samfunnsfunksjoner det vanskelig å forutse hva som kan gå galt, og hvilke konsekvenser det kan få hvis noe svikter. I et slikt perspektiv vil konsekvensen av svikt måtte vektlegges mer enn sannsynligheten. Tiltak for å sikre kritiske infrastrukturer og kritiske samfunnsfunksjoner krever derfor grundig behandling og høy prioritet. Offentlige myndigheter må stille tydelige krav, føre effektive tilsyn og sikre god beredskap. Samtidig må den enkelte bedrift være bevisst sitt ansvar for sikkerheten. Ikke minst har også hver enkelt av oss et ansvar for å være forberedt på avbrudd i forsyningen av viktige tjenester og varer. Beskyttelse av kritiske infrastrukturer og kritiske samfunnsfunksjoner handler om å ivareta samfunnets grunnleggende behov og befolkningens trygghetsfølelse.

1.1 Kapittelinnhold

Utvalgets utredning består av to deler. Del 1 er utvalgets hovedrapport og kan leses uavhengig av Del 2. Del 2 inneholder utfyllende vedlegg til hovedrapporten.

Kapittel 2

Utvalget har hatt som mandat å kartlegge virksomheter som har betydning for rikets sikkerhet og vitale nasjonale interesser, det vil si kartlegge kritiske infrastrukturer og kritiske samfunnsfunksjo-

[1] NOU 2000:24 *Et sårbart samfunn. Ufordringer for sikkerhets- og beredskapsarbeidet i samfunnet.*

ner. Videre har utvalget hatt som mandat å kartlegge og vurdere virkemidler for sikring av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner. I mandatet fremgår det også at utvalget skal vurdere alle virksomheter med ansvar for kritiske infrastrukturer, men må spesielt se på de virksomheter som ikke er eiet eller kontrollert av det offentlige. Videre at utvalget skal vurdere offentlig eierskap knyttet til kritiske infrastrukturer og kritiske samfunnsfunksjoner samt utrede konsekvensene av forslagene.

Kapittel 3

En viktig innledende oppgave for utvalget var å identifisere kritisk infrastruktur. Dette er gjort ved å utarbeide en definisjon og ett sett med retningslinjer. Til sammen har disse lagt til rette for en skjønnsmessig vurdering av hva som er kritisk infrastruktur.

Definisjonen av kritisk infrastruktur er:

> *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.*

Til sammen er dette med på å understøtte rikets sikkerhet og landets vitale nasjonale interesser.

For begrepsmessig å konkretisere kritisk infrastruktur, skiller utvalget mellom kritisk infrastruktur og kritiske samfunnsfunksjoner. En presis tilnærming til hva kritisk infrastruktur er, innebærer å identifisere både kritisk infrastruktur og kritiske samfunnsfunksjoner. Tabell 1.1 viser en oversikt over hva utvalget har vurdert til å være kritisk infrastruktur og kritiske samfunnsfunksjoner.

Tabell 1.1

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

Utvalget har ikke eksplisitt vurdert de kritiske samfunnsfunksjonene som står i kursiv.

Utvalget understreker at listen over de kritiske infrastrukturene og kritiske samfunnsfunksjonene ikke er ment å være en endelig og objektiv liste. Det er fordi en liste av nødvendighet vil måtte utarbeides med et formål. Formålet med utvalgets liste er å vurdere overordnede virkemidler for å sikre kritisk infrastruktur og samfunnskritiske funksjoner. Listen er derfor av overordnet karakter. Kapittel 3 har også en gjennomgang av sentrale begreper knyttet til beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner.

Kapittel 4

Kritisk infrastruktur og kritiske samfunnsfunksjoner står overfor en rekke sikkerhetsutfordringer. Det gjelder både overfor tilsiktede og utilsiktede uønskede hendelser. Utvalget har sett nærmere på følgende sikkerhetsutfordringer: Klimaendringer og naturkatastrofer, aldring i kritisk infrastruktur, terrorisme og organisert kriminalitet, omorganisering, omregulering og bortsetting, globalisering, sikkerhetsutfordringer knyttet til elektronisk kommunikasjon, etterretningsvirksomhet og gjensidige avhengigheter.

Kapittel 5

Ansvarsprinsippet står sentralt for håndtering av ulike sikkerhetsutfordringer i kritisk infrastruktur og kritiske samfunnsfunksjoner. Utvalget drøfter myndighetsansvar fordelt på sektorer, Justis- og politidepartementets samordningsrolle, privat sektors samfunnsansvar, herunder ivaretakelse av samfunnsansvar, og samarbeid mellom offentlige og private aktører.

Kapittel 6

Ulike virkemidler kan iverksettes for å ivareta god sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner. Utvalget drøfter overordnet ulike virkemidler slik som *juridiske*, eksempelvis gjennom lover, forskrifter, konsesjoner, lisenser, prisreguleringer. Videre drøftes *organisatoriske* virkemidler, eksempelvis utskilling av kommersielle enheter, selskapsdannelser og etablering av tilsynsorganer. Utvalget drøfter også *økonomiske* virkemidler, for eksempel tilskudd, kjøp av varer og tjenester, skat-

ter og avgifter. Også *pedagogiske* virkemidler samt virkemidler knyttet til *eierskap* blir drøftet.

Kapittel 7

Sikkerhetsloven har som formål å redusere risiko for sikkerhetstrusler som følge av spionasje, sabotasje og terrorhandlinger gjennom forebyggende defensive tiltak. Disse tiltakene gjennomføres i det alt vesentlige i virksomhetene lokalt, gjennom utvelgelse av informasjon og objekter som trenger beskyttelse ut fra en vurdering av deres betydning for rikets sikkerhet og selvstendighet og andre vitale nasjonale sikkerhetsinteresser. Utvalget beskriver formålet med loven og ulike utfordringer knyttet til sikkerhetslovens virkeområde og forholdet til andre lover og sektorvise bestemmelser.

Kapittel 8

Ulike drivkrefter har ligget bak omorganiseringer og omreguleringer av virksomheter som kan sies å være en del av kritisk infrastruktur og kritiske samfunnsfunksjoner. Utvalget drøfter overordnet hvordan hensynet til sikkerhet og beredskap er ivaretatt. Drøftingene blir sett i lys av knappe offentlige budsjetter og stadig økende etterspørsel etter offentlige tjenester, den teknologiske utviklingen, internasjonalisering og globalisering.

Kapittel 9

Det store innslaget av offentlig eierskap i norsk økonomi har vært motivert ut fra verdimaksimerende mål og andre samfunnsmessige mål på sentralt og sektorpolitisk nivå. Utvalget drøfter offentlig eierskap som virkemiddel for ivaretakelse av sikkerhet og beredskap i kritisk infrastruktur og kritiske samfunnsfunksjoner.

Kapittel 10 og 11

Det fremgår av utvalgets mandat at utvalget skal kartlegge virksomheter som antas å ha betydning for rikets sikkerhet og vitale nasjonale interesser. Med dette som bakgrunn har utvalget tolket mandatet til å omfatte en kartlegging av kritisk infrastruktur og kritiske samfunnsfunksjoner. I kapittel 3 blir kritisk infrastruktur og kritiske samfunnsfunksjoner identifisert. I kapittel 10 og 11 begrunner utvalget hvorfor disse er kritiske, i tillegg til å gi en overordnet beskrivelse samt beskrivelser av eierforhold og organisering.

Kapittel 12

I kapittel 12 redegjøres det for arbeidet med å beskytte kritisk infrastruktur og kritiske samfunnsfunksjoner i USA, Canada, Sverige, Tyskland, Nederland, Storbritannia, Sveits, Singapore samt i EU og NATO.

Kapittel 13

Forskning og utredning gir viktige innspill til arbeidet med å beskytte kritisk infrastruktur og kritiske samfunnsfunksjoner. Fremstillingen i dette kapittelet er ikke en uttømmende redegjørelse, men skal bidra til å gi et overblikk over relevant forskning og utredning på området.

Kapittel 14

Kapittelet inneholder en vurdering av økonomiske og administrative konsekvenser av utvalgets forslag.

1.2 Utvalgets anbefalinger

Kapittel 2, 3, 4 og 14 er i hovedsak av drøftende og redegjørende karakter. Utvalgets anbefalinger er gjort i kapittel 5, 6, 7, 8, 9, 10, 11 og 13.

Samtlige av utvalgets anbefalinger er enstemmige.

1.2.1 Utvalgets anbefalinger i kapittel 5 – Ansvar for beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner

Forslag knyttet til tydeliggjøring av Justis- og politidepartementets rolle

Utvalget mener at Justis- og politidepartementet på mange måter er innrettet til å være det «sikkerhetsdepartement» som sårbarhetsutvalget foreslo.

Utvalget vil påpeke viktigheten av å tydeliggjøre Justis- og politidepartementets rolle og ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner, samt viktigheten av å prioritere denne delen av departementets generelle ansvar for samfunnets sivile sikkerhet og beredskap. Dette innebærer at departementet må innta en tydeligere koordinerende rolle for å påse at hensynet til rikets sikkerhet og vitale nasjonale interesser blir ivaretatt på tvers av sektorene. Dette er ikke minst viktig for å unngå uklarheter på departementalt nivå og gi klare signaler med hensyn til mål og akseptnivå knyttet til sikkerhet og beredskap.

Utvalget mener at viktige koordineringsoppgaver for Justis- og politidepartementet vil være å:

– Være rådgivende myndighet i spørsmål knyttet til sikkerhet og beredskap i kritisk infrastruktur og kritiske samfunnsfunksjoner.

- Være pådriver og tilrettelegger for samarbeid og informasjonsdeling mellom virksomheter med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner.
- Etablere og videreutvikle oversikt over kritisk infrastruktur og kritiske samfunnsfunksjoner i Norge, gjennom en felles metode og system for utpeking og klassifisering av kritisk infrastruktur og kritiske samfunnsfunksjoner.
- Bidra til koordinering mellom arenaer for samarbeid og informasjonsdeling knyttet til kritisk infrastruktur og kritiske samfunnsfunksjoner.
- Systematisere og koordinere trussel-, risiko- og sårbarhetsinformasjon knyttet til kritisk infrastruktur og kritiske samfunnsfunksjoner, herunder å etablere et system for innhenting og formidling av relevant informasjon. Dette må skje på basis av informasjon fra andre myndigheter og i samarbeid med de andre fagdepartementene.
- Kunne opptre som nasjonalt kontaktpunkt og nasjonal representant ved internasjonalt samarbeid knyttet til beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner.
- Ta initiativ til avklaring av ansvarsforhold i de tilfeller dette ikke er gjort eller ansvarsforholdene synes uklare.
- Gjennom et samarbeid med aktuelle myndigheter, utarbeide felles målsetninger og strategier knyttet til kritisk infrastruktur og kritiske samfunnsfunksjoner.
- Frembringe tverrsektorielle problemstillinger eller forslag uten en bestemt ansvarlig adressat.
- Koordinere igangsettingen og oppfølgingen av tverrsektoriell forskningsaktivitet innen sikkerhet og beredskap, herunder BAS-studiene og SAMRISK.

Forslag knyttet til tydeliggjøring av nasjonale mål/ akseptnivå

1. Det må innarbeides som premiss i aktørenes risiko- og sårbarhetsanalyser at risiko mot og sårbarheten innen kritisk infrastruktur og kritiske samfunnsfunksjoner er i sterk utvikling. Det er viktig at gjeldende risikovurderinger gjennomgås med sikte på at det er tatt tilstrekkelig høyde for usikkerhet om risiko og sårbarhet («føre var» - prinsipp).
2. Justis- og politidepartementet bør gi nærmere retningslinjer for gjennomføring av risiko- og sårbarhetsanalyser innenfor de ulike sektorene. Det bør på sikt undersøkes om at sikringsnivået innen de ulike sektorene er godt nok samordnet, særlig med tanke på gjensidig avhengighet mellom sektorene.
3. Det bør utvikles et forpliktende program for regelmessige risiko- og sårbarhetsanalyser tilknyttet kritisk infrastruktur og kritiske samfunnsfunksjoner. Dette antas også å være en viktig betingelse for at Justis- og politidepartementet skal kunne presentere faste redegjørelser for Regjering og Storting om sikkerhets- og beredskapsnivået i samfunnet. Ved å etablere et system med regelmessige samlede fremstillinger av risiko, sårbarhet og sivile beskyttelsesbehov, som igjen kobles til de regelmessige forsvarsanalysene, skapes et:
   - Grunnlag for tverrsektorielle avveininger innenfor det sivile samfunnssikkerhetsfeltet.
   - Grunnlag for en risikobasert prioritering av Forsvarets støtte til det sivile samfunn.
   - Grunnlag for en helhetlig analyse og politikk for det sivile og militære sikkerhetsarbeid.

Forslag knyttet til forholdet mellom NSM, PST og DSB

Utvalget mener at Justis- og politidepartementet gjennom en koordinert styring av Politiets sikkerhetstjeneste (PST), Nasjonal Sikkerhetsmyndighet (NSM) og Direktoratet for samfunnssikkerhet og beredskap (DSB), kan legge forholdene til rette for bedre brukertilpasning og faglige synergieffekter, samt bidra til å tydeliggjøre ansvarsforholdene mellom direktoratene.

Utvalget viser til ansvarsdelingen mellom Justis- og politidepartementet og Forsvarsdepartementet hva gjelder de faglige rapporteringslinjene til NSM, og understreker at dette ikke må begrense Justis- og politidepartementets muligheter til å se NSMs myndighetsutøvelse i sivil sektor i sammenheng med det øvrige sivile sikkerhets- og beredskapsarbeidet. Utvalget stiller spørsmål ved hvorvidt det i praksis er mulig å skille klart mellom etatsstyringsansvar og faglig ansvar.

Forslag knyttet til prinsipper for god sikkerhetskultur

Utvalget har utarbeidet et sett med prinsipper for å oppnå en god sikkerhetskultur i en virksomhet. De er:

1. Godt lederskap og god virksomhetsstyring må påse at sikkerhets- og beredskapstiltakene følges opp av alle innenfor organisasjonen. Sikkerhets- og beredskapsarbeidet må ha høy status innenfor organisasjonen, og understøttes av alle.
2. Sikkerhet og beredskap bør inngå som en integrert del av virksomhetens drift og må omfatte både fysiske og IT-relaterte tiltak.

3. Sikkerhets- og beredskapstiltakene må baseres på trussel-, risiko- og sårbarhetsinformasjon og vurderes som en del av virksomhetens risikostyring. I denne forbindelse bør virksomheten ha system for jevnlige evalueringer og oppdateringer av sikkerhets- og beredskapsnivået. Dette forutsetter at virksomheten setter seg mål eller standarder for sikkerhets- og beredskapsarbeidet.
4. Virksomheten bør ha system for kompetansebygging innen sikkerhet og beredskap, herunder kursing, trening og øvelsesaktiviteter.
5. Virksomheten bør ha system for deling av relevant informasjon, både internt og eksternt.
6. Det bør systematisk opprettholdes fullstendige lister over roller og ansvar innenfor organisasjonen.
7. Virksomheten bør ha planer for å opprettholde drift gjennom tiltak som kan iverksettes ved økt trusselnivå, tiltak som kan iverksettes for å håndtere og redusere konsekvensene av alvorlige uønskede situasjoner og tiltak som kan gjenopprette normal drift etter en slik hendelse.

Utvalget vil anbefale at det utarbeides en informasjonshåndbok hvor det fremgår hva de ulike myndighetsorganene kan tilby av råd og veiledning knyttet til sikkerhet og beredskap. Denne informasjonshåndboken bør utarbeides i nært samarbeid med næringslivet.

1.2.2 Utvalgets anbefalinger i kapittel 6 – Virkemidler

Forslag knyttet til lovregulering

Utvalget påpeker mangler ved dagens reguleringsordninger og gir forslag til en generell lov om beredskap for å sikre kritisk infrastruktur og kritiske samfunnsfunksjoner. Det er viktig å få til en så rask og smidig gjennomføring av kravene som mulig, og viser at videre fremdrift kan ses i sammenheng med utredning fra en arbeidsgruppe under ledelse av Justis- og politidepartementet som har levert forslag til ny lov om sivilforsvar, sivile beskyttelsetiltak og beredskapsplikt. Forslaget innebærer krav til risiko- og sårbarhetsanalyser, drifts- og leveransesikkerhet, beredskapsplaner, informasjonsdeling og samarbeid, tilsyn og sanksjonsmuligheter.

Forslag knyttet til tilsynsvirksomhet

Utvalget er generelt opptatt av at ansvarsforholdene knyttet til sikkerhet og beredskap i kritisk infrastruktur og kritiske samfunnsfunksjoner er avklart, ikke minst at dette er ryddig når det gjelder forholdet mellom tilsynsorgan og tilsynsobjekt.

Utvalget tror det kan være uheldig at et departement både innehar det faglige ansvar for et sektortilsyn samtidig som departementet er eier av virksomheter som dette sektortilsynet fører tilsyn med innenfor sektoren. Etter utvalgets mening er det også et spørsmål om alle sektortilsynene i tilstrekkelig grad har tilpasset ressursbruken i forhold til endringer i sikkerhetssituasjonen. Utvalget er opptatt av betydningen av at tilsynene i sin virksomhet finner en god balanse når det gjelder å måle og fange opp forbedringsbehov i virksomhetenes samlede risikohåndtering, dvs. alt fra små uhell og ulykker med stor sannsynlighet og over til store sammenbrudd og katastrofer med liten sannsynlighet.

Med bakgrunn i ovennevnte vil utvalget anbefale at tilsynsvirksomheten på området kritisk infrastruktur og kritiske samfunnsfunksjoner utredes nærmere. Formålet med en slik utredning bør være å sikre at tilsynsvirksomheten på dette området er mest mulig mål- og resultatorientert i forhold til sikkerhets- og beredskapsbehovene. Utvalget vil anbefale at det i denne sammenheng vurderes en samordning av tilsynsvirksomheten og en prinsipiell drøfting av forholdet mellom tilsyn som ivaretar overordnede interesser og tilsyn som ivaretar sektorinteresser (horisontale vs. vertikale tilsyn).

Dernest anbefaler utvalget at det utarbeides en nasjonal strategi for tilsynsvirksomheten knyttet til sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner.

Forslag knyttet til etablering av tilskuddsordning

Utvalget mener at det er behov for en statlig tilskuddsordning. Ordningen må være rettet mot tiltak som klart faller utenfor virksomhetenes eget ansvar og som anses nødvendig av hensyn til rikets sikkerhet og vitale nasjonal interesser. En tilskuddsordning vil bøte på mangler i dagens system gjennom:

- Å sikre at tverrsektorielle tiltak uten en hovedinteressent blir igangsatt og fulgt opp.
- Å bidra til å finansiere den statlige delen i en risikofordeling mellom offentlige og private interessenter.
- Å finansiere nødvendige sektorovergripende tiltak og følge opp sektorovergripende infrastrukturer.
- Å ivareta et helhetlig perspektiv og følge opp tiltak ut i fra både hensynet til sikkerhet mot villede og ikke-villede uønskede hendelser.

Forslag knyttet til offentlige innkjøp

Etter utvalgets mening bør det være et krav at det ved offentlige innkjøp skal vurderes sikkerhets- og beredskapsmessige konsekvenser ved bortfall av de varer og tjenester som leveres. Det må herunder også stilles krav til sikkerhet og beredskap i forhold til underleverandører.

Forslag knyttet til bruk av standarder og standardiserte metoder

Utvalget anbefaler at det etableres et forprosjekt som beskriver nærmere hvordan standarder kan bidra til sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner i Norge. I denne sammenheng vil det være viktig å delta aktivt i forhold til internasjonalt standardiseringsarbeid. Arbeidet bør i størst mulig grad bidra til å forenkle oppfølgingen av regelverk på området, og dette forutsetter at myndighetene må bidra aktivt i forhold til å definere mål, rammer og nivå på sikkerhetstilstanden for slike standarder.

Forslag knyttet til samarbeid og informasjonsdeling

Utvalget anbefaler en styrking av samarbeid og informasjonsdeling knyttet til sikkerhet og beredskap, særlig mellom virksomheter med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner. Dette gjelder både innenfor, og på tvers av, offentlig og privat sektor. Utvalget vil også understreke viktigheten av bransjesamarbeid på dette området, herunder den viktige rollen organisasjonene kan spille i dette arbeidet.

Utvalget anbefaler at det etableres et tettere og mer forpliktende samarbeid mellom de sentrale myndighetene med ansvar for overordnede trussel-, risiko og sårbarhetsvurderinger. Dette samarbeidet må i det minste inkludere Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Direktoratet for samfunnssikkerhet og beredskap (DSB). Det kan tenkes ulike løsninger for samarbeid og informasjonsformidling, alt etter hvor viktig informasjonen er eller hvor mye det haster med å formidle den.

Et slikt samarbeid kan for eksempel etableres innenfor rammene av Koordinerings- og rådgivningsutvalget for etterretnings- og sikkerhetstjenestene (KRU). Det kan vurderes en ordning med sekondering fra de aktuelle myndighetsorganene i KRUs permanente sekretariat. En annen løsning kan være å etablere et permanent samordningsorgan på direktoratsnivå bestående av personell som sekonderes fra NSM, DSB og PST. Det bør vurderes om organet skal forankres administrativt i et av de tre direktoratene. Det bør være et mål å se fysisk og logisk sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner i sammenheng. Representasjon fra andre samarbeidende tjenester kan også vurderes, for eksempel Post- og teletilsynet, Norges vassdrags- og energidirektorat, mv.

Det anbefales at det etableres møteplasser der offentlige og private virksomheter kan treffes for å drøfte hva det aktuelle trussel-, risiko- og sårbarhetsbilde har å si for deltakerne, hvilke handlingsalternativer som kan og bør iverksettes, samt oppfølgingen av iverksatte tiltak. Utvalget har ikke vurdert eksisterende møteplasser for denne typen samarbeid, men anbefaler at de tre etterretnings- og sikkerhetstjenestene samt DSB vurderer dette sammen.

1.2.3 Utvalgets anbefalinger i kapittel 7 – Sikkerhetsloven og den forebyggende sikkerhetstjenesten

Forslag knyttet til objektsikkerhet

Utvalget anbefaler at nødvendige endringer i sikkerhetsloven som gjelder objektsikkerhet bør gjennomføres, og at arbeidet med å gi utfyllende forskriftsbestemmelser på dette området samt utvikle standarder og standardiserte metoder bør gjennomføres.

Utvalget mener at identifisering av hvilke private virksomheter som bør omfattes av sikkerhetsloven må skje gjennom en prosess med et samarbeid mellom virksomhetene, deres organisasjoner og myndighetene. Utgangspunktet for dette vil være risiko- og sårbarhetsanalyser som eventuelt vil avdekke mulige skjermingsverdige objekter i virksomhetens besittelse.

Utvalget vil foreslå at det i sikkerhetsloven og forskiftene til denne loven gis utfyllende bestemmelser om objektsikkerhet.

Forslag knyttet til sikkerhetslovens virkeområde

Utvalget mener et dokumentert behov for å tilvirke skjermingsverdig informasjon i seg selv kan være et grunnlag for å gjøre loven gjeldende for den aktuelle virksomheten.

Utvalget anbefaler at sikkerhetslovens virkeområde utvides ved enkeltvedtak i samsvar med dagens regulering, og at Justis- og politidepartementet har denne fullmakten.

1.2.4 Utvalgets anbefalinger i kapittel 8 – Ivaretakelse av sikkerhets- og beredskapshensyn ved omreguleringer og omorganiseringer

Forslag knyttet til bruk av liste over kontrollpunkter ved omreguleringer og omorganiseringer

Utvalget har utarbeidet en liste over kontrollpunkter for hvilke hensyn som må tas ved omreguleringer og omorganiseringer av offentlig virksomhet. Listen gjengis i kapittel 8.

Forslag knyttet til sammefallende omstillinger i en sektor

Etter det utvalget har grunn til å tro, blir sikkerheten ikke alltid ivaretatt tilfredsstillende ved omstillinger. Statens Havarikommisjon for transport har vist til det samme for luftfartssektoren når de skriver at: «[...] operatørers og luftfartsmyndigheters prosesser for å ivareta sikkerheten ved innføring av endringer og omstillingsprosesser inneholder en rekke forhold som bør forbedres før de kan sies å være tilstrekkelige for dette formålet.»[2] Utvalget ønsker å understreke at sikkerhetshensyn må ivaretas under omstillingsprosesser i kritisk infrastruktur og kritiske samfunnsfunksjoner.

Utvalget ønsker videre å peke på at omstillinger i tilsynsorganer kan føre til at evnen til å utføre tilsyn blir redusert i en periode. Det vil derfor etter utvalgets mening være uheldig å omstille et tilsynsorgan samtidig som sentrale operatører i samme sektor omstilles. Det vil kunne føre til en dobbelt svekkelse av sikkerheten. Utvalget anbefaler derfor at omstillinger i et tilsynsorgan ikke må falle sammen i tid med omstillinger hos sentrale operatører i samme sektor.

Forslag knyttet til å holde sikkerhets- og beredskapsmessige oppgaver som en integrert del av virksomheten

Utvalget anbefaler at sikkerhets- og beredskapsarbeid som knytter seg til kjerneoppgaver i kritisk infrastruktur og kritiske samfunnsfunksjoner holdes som en integrert del av virksomheten. Det vil si at disse oppgavene ikke settes ut til andre virksomheter.

1.2.5 Utvalgets anbefalinger i kapittel 9 – Offentlig eierskap

Behovet for sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner er i utgangspunktet uavhengig av organiseringen av eierskapet til de underliggende systemer, installasjoner, anlegg og produksjonsfasiliteter. Spørsmålet er imidlertid om offentlig eierskap kan gjøre det enklere og i noen tilfelle kan være en forutsetning for at det offentlige på en tilfredsstillende måte skal kunne ivareta ansvaret for en intakt og velfungerende infrastruktur som anses som helt nødvendig for å opprettholde kritiske samfunnsfunksjoner, samfunnets grunnleggende behov og befolkningen trygghetsfølelse.

Utvalget har festet seg ved tre ulike generiske trekk ved kritisk infrastruktur som kan tale for offentlig eierskap som den mest hensiktsmessige måten å ivareta det offentlige ansvaret på. Det er for det første en kritisk avhengighet av infrastrukturen når det gjelder å opprettholde et tjenestetilbud rettet mot tilfredsstillelse av grunnleggende behov. For det andre at det ikke finnes tjenlige alternativer som kan erstatte infrastrukturen om den skulle falle ut. Den blir dermed helt nødvendig for forsyningssikkerhet av kritiske tjenester og for opprettholdelse av samfunnskritiske funksjoner. Disse to egenskapene, kritisk avhengighet og absolutt nødvendighet, som er to relaterte aspekter ved kritikalitetskriteriet, har som konsekvens at funksjonssvikt, uansett grunn, i verste fall vil kunne føre til katastrofale og i noen tilfelle irreparable konsekvenser for individer og samfunn. Siden det offentlige uansett eierskap vil sitte med sluttansvaret for å organisere reserveløsninger og oppretting i tilfelle slik funksjonssvikt, tilsier det at det offentlige også må ha full kontroll over bruk og vedlikehold av kritisk infrastruktur. En slik kontroll sikres best ved offentlig eierskap. En tredje egenskap er tett kobling. Dette kan gjelde mellom ulike komponenter innenfor ett og samme system slik at svikt i én komponent fører til at hele systemet svikter. En annen variant av tett kobling kan skyldes avhengighet mellom systemer slik at svikt i ett system, har negative virkninger for funksjonaliteten i andre systemer og at det dermed får sektorovergripende konsekvenser. Tett kobling, enten det er innenfor et system eller mellom systemer, taler for sentralisert styring og nasjonal kontroll. Begge deler sikres best ved offentlig eierskap.

Disse generiske trekkene ved kritisk infrastruktur er i varierende grad til stede innenfor flere samfunnssektorer. Utvalget mener at offentlig eierskap som virkemiddel derfor må vurderes konkret innenfor hver enkelt virksomhet og sektor. Det er viktig at valg av eierskap skjer på grunnlag av en helhetsvurdering der ønskeligheten av offentlig kontroll veies opp mot eventuelle bedriftsøkonomiske fordeler ved privat eierskap. Utvalget vil

[2] SL RAP 35/2005. *Flysikkerhet i norsk luftfart under omstillingsprosesser*. Havarikommisjonen for sivil luftfart og jernbane.

likevel understreke at ved denne avveiningen må hensynet til samfunnmessig sikkerhet og beredskap veie tungt for infrastruktur som har karakter av å være kritisk (jf. kriteriene ovenfor).

1.2.6 Utvalgets anbefalinger i kapittel 10 – Kartlegging av kritisk infrastruktur og sektorvise anbefalinger

1.2.6.1 Elektronisk kommunikasjon

Forslag knyttet til eierskap som virkemiddel

Standardmodellen i den vestlige verden var å organisere telesektoren i vertikalt integrerte monopoler. Det som taler mot vertikalt skille mellom nett og nettbasert tjenesteproduksjon i dag, er tap av synergigevinster mellom oppstrøms- og nedstrømsvirksomheten.

Ikke i noen land det er naturlig å sammenligne seg med har det gamle «stamnettet», som utgjør kjernen i telesystemene mange steder, blitt løftet ut og organisert som statlig foretak i løpet av omorganiseringsprosessen.

Også for Norges del er utviklingen kommet så langt at den i praksis må betraktes som irreversibel. I de aller fleste land finner en derfor at de tidligere offentlige telemonopolene driver tjenesteproduskjon i konkurranse med private operatører samtidig som de fortsatt kontrollerer de deler av nettet som antas å være naturlig monopol, og som konkurrerende aktører er avhengige av tilgang til.

Når vertikal integrasjon er mest hensiktsmessig og nedstrømsmarkedet i tillegg er et konkurransemarked (slik som telesektoren), taler regulatorisk ryddighet for privat eierskap til den integrerte virksomheten. Ved dette unngår en mistanke om at myndighetene ikke klarer å etablere tilstrekkelig armlengde mellom sin eierrolle og regulatørrollen.

Utvalget mener at det i prinsippet ville være mest logisk med et klarere skille mellom samfunnsoppdraget knyttet til infrastrukturen på den ene siden og den kommersielle nettbaserte tjenesteproduksjonen (nedstrømsvirksomheten) på den andre. Etter utvalgets vurdering taler imidlertid de spesielle forholdene som knytter seg til denne sektoren for privat eierskap til den integrerte virksomheten.

Utvalget mener det er viktig at eierskap til infrastruktur som er kritisk for landet bør være under kontroll av norske eiere. Dette vil gjøre at norske interesser i størst mulig grad ligger til grunn for strategiske beslutninger. Om nødvendig bør dette sikres ved at det offentlige har tilstrekkelig eierandeler i de aktuelle selskapene.

Forslag knyttet til nasjonal autonomi for elektroniske kommunikasjons- og nettjenester

Dersom utviklingen i telemarkedet fortsetter uten at nasjonale reserveløsninger etableres, vil avhengigheten av utlandet øke. Det vil bli både ressurskrevende og vanskelig å etablere nødvendige beredskapsløsninger, dersom dette utsettes ytterligere. Utvalget mener at når avtaler om nasjonale reserveløsninger er etablert, kan kravet om autonom drift av telesystemer slik det er utformet i forskriften i dag frafalles. Nødvendige lovhjemler som sikrer slike reserveløsninger må være på plass.

Forslag knyttet til regulering av brukere av Internett

Utvalget anbefaler følgende:

1. At alle Internettilbydere blir pålagt å levere sikkerhetsprogramvare som en del av Internettabonnementet til privatpersoner.
2. At alle utstyrsleverandører av trådløse nett plikter å levere utstyret med tilfredsstillende sikkerhetsinnstillinger og gode veiledninger på norsk.
3. At det i regi av Samferdselsdepartementet utredes nærmere om:
   a) alle, både privatpersoner og virksomheter, skal være pliktige til å benytte oppdatert sikkerhetsprogramvare når de kobler seg til Internett.
   b) Internettilbydere skal bli pålagt å kontrollere at alle deres kunder benytter seg av oppdatert sikkerhetsprogramvare, og hvilke inspeksjons- og sanksjonsmuligheter som er teknisk og økonomisk realistiske.
   c) det kan utarbeides IKT-sikkerhetsstandarder som alle virksomheter som knytter seg til Internett blir pålagt å følge.

Forslag knyttet til organiseringen av IT-sikkerhetsarbeidet

Utvalget anbefaler at antall fagdepartementer med overordnet ansvar for IT-sikkerhet bør reduseres, og ideelt sett mener utvalget at dette ansvaret bør ligge til ett departement. Utvalget vil foreslå en samordning av Samferdselsdepartementets og Fornyings- og administrasjonsdepartementets ansvar på dette fagområdet.

Forslag knyttet til økonomiske virkemidler

Utvalget mener kjøp av tjenester og tilskudd til spesielle oppgaver for sikring av kritisk infrastruktur vil være et nødvendig virkemiddel sammen med regulatoriske bestemmelser. Det vises i denne

sammenheng også til utvalgets forslag om en tilskuddsordning.

Forslag knyttet til nødnettet

Utvalget er sterkt opptatt av at utbyggingen av nødnettet må fullføes slik det er planlagt og at nødvendige bevilgninger tildeles.

1.2.6.2 Satellittbasert kritisk infrastruktur

Generelle vurderinger

Innsikt i utvikling og drift av Galileosystemet oppnås best gjennom aktiv og målrettet deltakelse i nedsatte komiteer og arbeidsgrupper samt faste staber innen EU og ESA[3]. Deltakelse gir dessuten mulighet til å påvirke løsninger.

Utvalget mener at Norge bør vurdere å slutte seg til PRS-delen[4] av Galileo-systemet, siden sivile offentlige brukere ikke vil få tilgang til tilsvarende informasjon fra GPS i fremtiden og fordi Galileo PRS vil ha mer robuste signaler. Deltakelse i Galileo PRS krever statlige kontrollmekanismer.

Dersom Norge skulle få tildelt Galileo bakkeinfrastruktur (på Svalbard) vil det være viktig å fastsette hvilke lokale sikringstiltak som er nødvendig for å beskytte nettopp bakkeinfrastrukturen.

1.2.6.3 Kraft

Forslag knyttet til eierskap som virkemiddel

Statkraft AS ivaretar den konkurransebaserte produksjonen av kraft (kraftverk), mens Statnett SF har ansvaret for sentralnettet som har karakter av naturlig monopol, og har dessuten det nasjonale systemansvaret. En kan derfor si at vi her har vertikal separasjon mellom enerettsvirksomheten som består i å forvalte det landsdekkende overføringsnettet og konkurransevirksomheten i kraftproduksjon og -distribusjon til sluttbrukere.

I fravær av tilfredsstillende økonomiske og juridiske reguleringsmekanismer for samfunnsøkonomisk riktige nettinvesteringer er eierskapet til Statnett SF sannsynligvis et egnet virkemiddel for å ivareta sikkerhetshensyn i kraftsystemet på lang sikt. De viktigste funksjonene i Statnett i det henseende er selve systemansvaret (den løpende systemdriften) og muligheten til både å fatte beslutninger om hvilke investeringer som skal gjøres, og finansiere investeringene selv. Det betyr likevel ikke at private (eller for den saks skyld kommunale) investeringer i overføringskapasitet i sentralnettet bør utelukkes, men Statnett bør ha et helhetsansvar.

Ut fra sikkerhets- og beredskapshensyn er det vanskelig å se at det vil være noe å vinne på privatisering av sentralnettet, siden det er mulig å konkurranseutsette enkeltfunksjoner om det skulle være ønskelig.

I og med at utvalget ikke anser distribusjonsnettet som fullt så kritisk som sentralnettet, er det grunn til å anta at argumentet for offentlig eierskap er svakere, men det er behov for supplerende virkemidler i form av kvalitetskrav, leverings- og tilknytningskrav, oppføling av forskrifter osv. Eventuelt kan staten definere beredskapsbehov og sørge for tilstrekkelig finansiering via inntektsrammene eller statlige overføringer (i noen grad skjer dette allerede i dag gjennom beredskapsforskriften og inntektsrammereguleringen).

Forslag knyttet til hjemfall

Utvalget vil sterkt anbefale at hjemfallsinstituttet videreføres på en slik måte at dagens offentlige, nasjonale eierskap til kraftressursene på sikt ikke svekkes.

Forslag knyttet til strømrasjonering

Det er en kjent problemstilling at distribusjonsnettet i Norge (og i de fleste andre land) har en slik nettstruktur at det er svært vanskelig å prioritere levering av strøm til enkeltvirksomheter under slike forhold. Utvalget mener likevel at myndighetene må arbeide for å finne frem til løsninger som kan ivareta dette behovet så langt som mulig.

Samtidig bør det vurderes hvordan det kan sikres at kritiske samfunnsfunksjoner blir understøttet av reserveaggregater i større utstrekning enn hva som er tilfelle i dag. Det må muligens også vurderes å stille krav om etablering av nødstrømsaggregater for enkelte spesielt kritiske samfunnsfunksjoner.

Forslag knyttet til regulatoriske virkemidler

Kraftsektoren er den sektoren som kanskje har kommet lengst med hensyn til innføring av reguleringsmekanismer for sikring av den kritiske infrastrukturen. Utvalget mener at hensynet til sikkerhet og nasjonale interesser i forbindelse med dereguleringsprosessen innenfor denne sektoren er ivaretatt på en god måte.

Utvalget har imidlertid registrert at forholdet til sikkerhetsloven ikke er tilstrekkelig avklart hos flere av de store aktørene. Dette gjelder også for

[3] ESA, *European Space Agency*
[4] PRS, *Public Regulated Service*

Statkraft og Statnett. Heller ikke kommunalt eide aksjeselskaper er omfattet av sikkerhetsloven, og kan dermed ikke skjerme informasjon eller objekter i henhold til bestemmelsene i loven. De har heller ikke hjemmel til å foreta sikkerhetsklarering av nøkkelpersonell i den utstrekning det anses formålstjenlig.

Forslag knyttet til økonomiske virkemidler

Analyser av nettselskapenes tilpasning til KILE[5]-ordningen tyder på at ordningen gir signaler som tas hensyn til i selskapenes beslutninger om investeringer og vedlikehold. Det er ikke gitt at ordningen gir tilstrekkelige virkemidler til at leveringskvaliteten og beredskapen holdes på et akseptabelt nivå. KILE er primært et *langsiktig* virkemiddel for å stimulere til investeringer og vedlikehold, og kan ha gode samfunnsøkonomiske egenskaper med hensyn til leveringssikkerheten hvis ordningen er hensiktsmessig utformet. I denne sammenheng bør det vurderes hvorvidt inntektsrammereguleringen også kan brukes som middel for å sikre vedlikehold av nødvendig kompetanse og til å pålegge selskapene til enhver tid å holde oppdaterte kartdata over sine nett.

At reinvesterings- og vedlikeholdstakten i nettselskapene har falt sterkt de senere årene – til et nivå som forutsetter en levetid på mer enn hundre år for komponenter i nettene – er sentrale forhold som etter utvalgets mening bør vies oppmerksomhet fra myndighetenes side.

1.2.6.4 Vann og avløp

Forslag knyttet til eierskap som virkemiddel

VA-sektoren er karakterisert ved at det er sterk synergi mellom selve infrastrukturvirksomheten (tekniske anlegg) og konkurransevirksomheten (leveranse av vann og borttransport av avløp), noe som taler for vertikal integrasjon av disse virksomhetene.

VA-tjenestene fremstår derfor som naturlige monopolvirksomheter, og man vil ikke kunne oppnå reell konkurranse om slike tjenester, som normalt er det viktigste argumentet for privatisering. I valget mellom offentlig monopol og privat monopol er det således mye som taler for offentlig eierskap til VA-infrastrukturen.

Utvalget anbefaler at VA-virksomheten ut fra et sikkerhets- og beredskapsperspektiv skal være i offentlig eie. Det hersker noe usikkerhet med hensyn til om det kan komme overnasjonale føringer når det gjelder liberarlisering av VA-tjenestene. Utvalget vil derfor anbefale at offentlig eierskap til VA-infrastrukturen blir regulert gjennom lov i Norge. Konkurranseutsetting av driftsoppgaver samt organisering av VA-virksomheten i private andelslag må fortsatt være tillatt, forutsatt at hensynet til sikkerhet og beredskap blir tilfredsstillende ivaretatt.

Forslag knyttet til myndighetsoppfølging og koordinering

Utvalget anbefaler at det etableres en samordningsgruppe for vannsektoren, med en representativ sammensetning, med tilstrekkelige ressurser og med mandat til blant annet å samordne arbeidet med regelverk og tilsyn, gjennomføre risikovurderinger, vurdere sikkerhetsnivå og kartlegge behovet for nødvendige tiltak.

Utvalget mener at Mattilsynet må trappe opp sitt arbeid som tilsyns- og godkjenningsmyndighet innen vannforsyning, for å sikre etterlevelse av kvalitets- og sikkerhetskrav. Mattilsynet må også sørge for en snarlig oppfølging av prioriterte tiltak i handlingsplanen for en sikrere vannforsyning.

Utvalget mener det er viktig at Mattilsynet følger nøye med på utviklingen på laboratorieområdet og går inn med statlige virkemidler dersom de beredskapsmessige hensyn innen vannforsyningssektoren ikke blir godt nok ivaretatt i et fullt ut konkurranseeksponert marked.

Forslag knyttet til VA-organisering og kompetanse

Utvalget mener at det bør gjennomføres en utredning om aktuelle incitamenter for å stimulere til mer robuste enheter innen VA-sektoren, herunder tiltak for å sikre nødvendig kompetanse. Utvalget foreslår at det som del av utredningen vurderes behov for en veiledende bransjestandard for kompetanse- og bemanningsbehov i VA-sektoren. Det er også viktig å følge med på rekrutteringssituasjonen og løpende vurdere behovet for tiltak.

Forslag knyttet til beredskapsevne

Kriser i vannforsyningssektoren vil av natur normalt ha lokale virkninger og må håndteres av lokal kriseledelse i kommuner, vannverk og Mattilsyn, eventuelt i samarbeid med andre aktører. Utvalget mener at det vil være nyttig å få etablert en sentral krisestøtteenhet etter svensk modell, som kan rykke ut og bistå det enkelte vannverk i en krisesituasjon.

Utvalget mener at det bør gjøres en kartlegging av beredskapsevne og -behov innen avløpssektoren for å se om dagens håndtering er tilfredsstillende, eller om det er behov for å styrke innsatsen.

[5] KILE, Kvalitetsjusterte inntektsrammer ved ikke levert energi

Forslag knyttet til økonomiske virkemidler

Utvalget vil advare mot at man forlater dagens selvkostregime for VA-sektoren til fordel for en inntektsrammestyring, uten en grundig vurdering av hvilke konsekvenser det kan få for den langsiktige sikkerheten ved VA-tjenestene.

1.2.6.5 Olje og gass

Forslag knyttet til eierskap som virkemiddel

En betydelig del av petroleumsvirksomheten på den norske kontinentalsokkelen skjer i regi av aktører med privat og/eller utenlandsk eierskap. Det er derfor uansett behov for et effektivt sikkerhetsregelverk med tilstrekkelige sanksjonsmuligheter. En rekke slike virkemidler er tilgjengelige i dagens lovverk og forskrifter. Offentlig eierskap er i beste fall et partielt virkemiddel for å ivareta sikkerhetshensyn, og vil være mindre viktig som virkemiddel dersom det generelle sikkerhetsregelverket og håndhevingen av det fungerer godt nok.

Forslag knyttet til regulatoriske virkemidler

Utvalget mener at de regulatoriske virkemidlene som er tatt i bruk er gode bidrag også i forhold til å ivareta de sikkerhetshensyn og nasjonale interesser som skal vurderes i denne sammenheng. Utvalget mener imidlertid at det er behov for å vurdere tilsynsvirksomheten på området for å avklare gråsoner.

Forslag knyttet til økonomiske virkemidler

Utvalget ser ikke behov for at staten skal gå inn med spesielle økonomiske virkemidler i forhold til å gjennomføre konkrete sikkerhetstiltak. Rettighetshaverne bør selv bekoste det som er nødvendig for å oppfylle kravene i lover og forskrifter.

1.2.6.6 Transport

Tilgjengelige transportsystemer er vitalt for samfunnets normale drift. Det tilsier at det offentlige utøver stor grad av kontroll over infrastrukturen.

Utvalget ønsker å peke på viktigheten av at de sikkerhets- og beredskapsmessige funksjonene ikke løsrives fra det ordinære driftsansvaret. God sikkerhet og beredskap oppnås kun ved at disse er integrert.

Innføringen av ISPS[6]-kravene kan innebære en uforholdsmessig stor økonomisk belastning på den enkelte havn, noe som tilsier at utgiftene til oppfølging av disse kravene må kunne finansieres gjennom offentlig-privat samarbeid. Det vises i denne sammenheng til utvalgets forslag knyttet til innføring av en statlig tilskuddsordning, jf. kapittel 6.6.3.

Utvalget anbefaler at Samferdselsdepartementet, Nærings- og handelsdepartementet, Fiskeri- og kystdepartementet og Justis- og politidepartementet samarbeider om å tydeliggjøre behovet for å velge den sikreste fremføringsveien og transportgrenen til virksomheter som har behov av transport av farlig gods.

1.2.7 Utvalgets anbefalinger i kapittel 11 – Kartlegging av kritiske samfunnsfunksjoner og sektorvise anbefalinger

1.2.7.1 Bank og finans

Utvalget har sett på tiltak som retter seg mot de kritiske infrastrukturene som de aller fleste kritiske samfunnsfunksjonene er avhengige av. Utvalget ønsker derfor å understreke viktigheten av at bank- og finanssektoren i sine ROS-analyser tar høyde for at de i stor grad er avhengig av ekstern infrastruktur for opprettholdelse av funksjonsdyktighet.

1.2.7.2 Matforsyning

Det er rimelig å forvente en viss robusthet i den enkelte husholdning, og at den enkelte må kunne klare seg selv noen dager før myndighetene iverksetter tiltak. I forbindelse med årtusenskiftet, produserte det daværende Direktoratet for sivilt beredskap en brosjyre med råd om hva husholdningene burde ha av matvarer og andre livsnødvendigheter. Med etableringen av en ny nasjonal kriseweb ser utvalget det som naturlig at spørsmålet om en slik brosjyre på nett blir vurdert.

Utvalget vil understreke viktigheten av å opprettholde en tilfredsstillende nasjonal matvareproduksjon ut fra et sikkerhetsperspektiv.

Utvalget anbefaler at det innenfor det formaliserte samarbeidet mellom Nærings- og handelsdepartementet og de største matvaredistributørene arbeides for å identifisere sårbarhet i kritisk infrastruktur som matforsyningen er avhengig av, slik at svakheter kan videreformidles til rette fagmyndighet og så langt som mulig minimaliseres.

1.2.7.3 Helse-, sosial- og trygdetjenester

Utvalget mener at sykehuseiere må være i dialog med leverandører av infrastruktur for å sørge for tilstrekkelig robuste leveranser og melde fra om at de skal være prioriterte brukere i forhold til gjenoppretting ved bortfall av tjenesten. Sykehus må

[6] ISPS-koden, *International Ship and Port Facility Code*

for eksempel ha planer og systemer for nødvannforsyning, nødstrøm og elektroniske kommunikasjonstjenester dersom det skulle oppstå brudd i ordinær tilgang.

Vaksiner og medisiner vil være knapphetsgoder ved fare for eller utbrudd av alvorlige epidemier og pandemier. Ved slike situasjoner vil helsevesenet, i samarbeid med andre myndigheter også ha viktige oppgaver i forhold til å prioritere bruk av medisiner. I den sammenheng bør leverandører av kritiske infrastrukturtjenester (som forsyning av strøm, vann og elektronisk kommunikasjon) gis prioritet slik at andre viktige samfunnsfunksjoner som er avhengig av kritisk infrastruktur ikke stopper opp.

Det er etablert en arbeidsgruppe med representanter fra Sosial- og helsedirektoratet, Statens legemiddelverk og Nasjonalt folkehelseinstitutt som skal foreslå tiltak for å øke forsyningssikkerheten for legemidler. Dette er særlig rettet mot å redusere sårbarheten ved manglende tilgang til legemidler tilvirket utenfor Norge. Arbeidet ble bestemt ferdigstilt i løpet av 2005. Utvalget understreker viktigheten av å følge opp dette arbeidet, og viktigheten av at resultatet av arbeidet blir bredt forankret i alle sektorer med kritisk infrastruktur og kritiske samfunnsfunksjoner.

1.2.7.4 Politi

Utvalget har ingen særskilte vurderinger og anbefalinger knyttet til å sikre politiets kritiske samfunnsfunksjon. Det har sammenheng med at utvalget anser at funksjonsdyktigheten i første rekke kan sikres med god sikkerhet i de kritiske infrastrukturene som politiet benytter seg av. Eksempelvis vil politiets funksjonsdyktighet bli sterkt rammet av svikt i elektronisk kommunikasjonsinfrastruktur og kraftinfrastrukturen.

Utvalget ønsker likevel å peke på to forhold som er av viktighet i denne sammenheng. Dette er forhold som utvalget ikke har hatt anledning til å ta opp til grundig behandling, men som utvalget mener må utredes nærmere i sin bredde. Det første gjelder den sterke veksten i bruk av private sikkerhets- og vekterselskaper hvor selskapene faktisk utøver maktanvendelse, infiltrasjon på arbeidsplasser og etterforskning av straffbare forhold. En hovedinnvending er at private sikkerhets- og vekterfirmaer ikke er underlagt den samme strenge demokratiske kontrollen som politiet. Dette er i hovedsak oppgaver som er lagt til politiet med hjemmel i politiloven, og som er viktige funksjoner i samfunnet. Likeledes stiller utvalget spørsmål ved om oppgaver som omfatter sivil maktanvendelse, infiltrasjon på arbeidsplasser og etterforskning av straffbare forhold skal overlates til personell uten politifaglig kompetanse. Utvalget vil derfor anbefale at problemstillingen blir tatt opp i hele sin samfunnsmessige bredde med organisatorisk forankring i Justis- og politidepartementet. For det andre viser utvalget til at Politireservens størrelse og funksjon er til vurdering. I denne forbindelse mener utvalget at ansvarsdelingen mellom Heimevernet og Politireserven bør vurderes. Dette gjelder blant annet oppgaver knyttet til vakthold og sikring av kritisk infrastruktur.

1.2.7.5 Nød- og redningstjeneste

Utvalget understreker betydningen av å opprettholde og videreutvikle samvirkeprinsippet i redningstjenesten. Særlig viktig er det å ta hensyn til videreføring av samvirkeprinsippet i forbindelse med omorganisering og privatisering av offentlige virksomheter, jf. utvalgets forslag til innføring av kontrollpunkter ved omreguleringer og omorganiseringer.

DSB utarbeidet i november 2005 et forslag om å styrke samfunnets evne til å håndtere store redningsaksjoner og andre hendelser som krever ekstraordinær innsats. Forslaget bygger på en omfattende kartlegging – basert på samarbeid og bidrag fra andre myndigheter, de tre nødetatene, med flere. Forslaget innebærer en utvikling og modernisering av sivilforsvarets operative styrker. Utvalget anbefaler at DSBs forslag følges opp.

1.2.7.6 Kriseledelse

Forslag knyttet til kriseledelsesapparatet

Utvalget anbefaler:

1. Innrettingen og prioriteringen av kriseledelsesapparatet må ikke nedprioriteres som følge av at det går lang tid mellom når det inntreffer kriser av nasjonal størrelse. Prioriteringen og innrettingen av det nasjonale kriseledelsesapparatet bør derfor opprettholdes til enhver tid.
2. Kriseledelsesapparatet må være tilstrekkelig fleksibelt organisert til å kunne håndtere alle typer scenarioer som kan oppstå. Det bør ikke være slik at det sentrale kriseledelsesapparatet organiseres ulikt avhengig av situasjonen (unntatt i tilfelle krig). Dette tilsier at forholdet mellom Regjeringens kriseråd og andre organer som ev. skal tre i funksjon under kriser avklares nærmere.
3. Krisestøtteenheten bør gis meningsfylte oppgaver i det daglige som ivaretar og styrker kompetansen knyttet til nasjonal kriseledelse. Dette

kan være oppgaver knyttet til nasjonale og internasjonale nettverk for kriseledelse. Oppgaver som i dag ligger hos myndigheter og som knytter seg til nasjonal kriseledelse bør vurderes i sammenheng med konkretiseringen av oppgaveporteføljen til Regjeringens krisestøtteenhet. Utvalget ser at dette kan gjøres ved hospiteringsordninger.

4. Det må være gode og etablerte rutiner for overføring av lederansvaret mellom fagdepartementene og Justis- og politidepartementet i tilfelle kompliserte kriser. I størst mulig grad bør det på grunnlag av aktuelle krisescenarier defineres hvem som peker seg ut som lederdepartement. Dette bør kunne avklares gjennom en kombinasjon av analyser, tilsyn og øvelser og forankres i en oppdatert nasjonal beredskapsplan for ekstraordinære påkjenninger mot samfunnet.
5. Ved større kriser er det behov for en samordnet håndtering på tvers av ansvarslinjene. Dette forutsetter at også planverket er koordinert. Utvalget vil peke på at det er behov for å uniformere departementenes planverk bedre enn i dag.
6. Fylkesmannsembetenes vaktberedskap og ansvar innenfor krisehåndtering bør tydeliggjøres, blant annet når det gjelder rekvirering av ressurser og i forhold til å komme frem til gode prioriteringer mellom ulike brukere ved avbrudd i kritisk infrastruktur.
7. Prioriterte deler av forvaltningen må gis tidsmessige og funksjonelle graderte samband i sine krisehåndteringslokaler som tillater sikker kommunikasjon på nivå til og med HEMMELIG. Det må forutsettes at sambandssystemene baseres på en teknologisk plattform som tillater at de kan kommunisere med hverandre sømløst.
8. Det må gjennomføres regelmessige øvelser for å teste og videreutvikle den nasjonale kriseberedskapen i forhold til mulige infrastrukturkriser. Øvelsene må følges opp med gode evalueringer og kontinuerlige tilpasninger og forbedringer i planverk og andre tiltak. Det bør i den sammenheng tilstrebes å benytte SBS[7]/BFF[8]-planverket som en del øvelsene der det er relevant.
9. Kommunene må få en generell beredskapsplikt.

Forslag knyttet til trossamfunnenes rolle i forebygging og håndtering av kriser

Utvalget mener det bør opprettes et permanent rådgivende utvalg med bånd til Justis- og politidepartementet. Det vil bidra til å dra nytte av de ressursene som finnes i de ulike trossamfunnene, og det vil virke inkluderende. Et slikt rådgivende utvalg bør ha følgende som oppgaver:

- gi myndighetene råd om hvordan usikkerhet og mistenksomhet mot eller mellom ulike trossamfunn kan håndteres, i forbindelse med kriser der norske interesser er involvert.
- gi myndighetene råd om hvordan religiøs ekstremisme kan forebygges og håndteres.
- gi myndighetene råd om hvordan de ulike trossamfunnene kan bidra i det psykososiale arbeidet etter en krise.

Utvalget understreker betydningen av at et permanent rådgivende utvalg får tid til å utvikle en felles plattform som grunnlag for samarbeidet. Utvalget ønsker også å understreke betydningen av at et permanent rådgivende utvalg blir representativt sammensatt av ulike trosretninger i Norge. Som et første skritt foreslås etablert en arbeidsgruppe bestående av representanter for noen sentrale trossamfunn. Det foreslås at arbeidsgruppens oppgave skal være å utarbeide retningslinjene og grunnlaget for utvalget.

Forslag knyttet til varsling av befolkningen

NRK har en beredskapsmessig viktig funksjon som formidler av myndighetenes informasjon ved nasjonale kriser og katastrofer. NRK P1 er utpekt som beredskapskanal. P1 dekker hele landet, og er sammen med Sivilforsvarets tyfonanlegg den beste plattformen for å nå ut hurtig både lokalt, regionalt og nasjonalt. Utvalget merker seg at avtaler mellom ulike myndigheter og NRK ble gjort innenfor rammen av den kalde krigen. Utvalget anbefaler følgende:

1. At avtaler og innretting tilpasses dagens sikkerhets- og beredskapsmessige utfordringer. Utvalget anbefaler i den sammenheng at rollene til SMK, KKD, JD[9] og andre myndigheter ses i sammenheng og revideres.
2. Utvalget anbefaler at KKDs midler avsatt til informasjonsberedskap til mediabedrifter gjennomgås for på mest mulig effektiv måte å styrke beredskapsinnsatsen hos mediene.
3. Utvalget anbefaler at FM-sendenettet kun kan slukkes når et nytt digitalt bakkenett for radio har en like god dekning som dagens sendenett. Det må være klart at varslingsfunksjonen som er tillagt NRK P1 videreføres i DAB-nettet.

[7] SBS: Sivilt Beredskapssystem.
[8] BFF: Beredskapssystemet for Forsvaret.
[9] Statsministerens kontor, SMK. Kirke- og kulturdepartementet, KKD. Justis- og politidepartementet, JD.

1.2.8 Utvalgets anbefalinger i kapittel 13 – Forskning og utredning

Forslag knyttet til utvidelse av Forsvarets forskningsinstitutts mandat

Utvalget anbefaler at Forsvarets forskningsinstitutts mandat utvides til også å omhandle samfunnets sårbarhet i sivil sektor.

Forslag knyttet til forskningsprogrammet SAMRISK

Å tilrettelegge for et eget tverrsektorielt forskningsprogram knyttet til samfunnssikkerhet og risiko vil etter utvalgets mening bidra til å styrke og samordne komplekse og tverrsektorielle utfordringer. Det vil videre bidra til koordinert innsats mellom de ulike forskningsmiljøene. Utvalget anbefaler at forskingsprogrammet SAMRISK[10] blir iverksatt.

Forslag om å gi prioritet til sikkerhet og beredskap i forskningsprogrammer ved Norges forskningsråd

Utvalget vil understreke verdien av at forskningsprogrammer ved Norges forskningsråd som er relevante for beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner, innarbeider og gir prioritet til sikkerhets- og beredskapsmessige utfordringer. Dette kan for eksempel gjelde prosjekter innenfor Energiprogrammet og NORKLIMA.

Forslag knyttet til Konsortium for forskning på terrorisme og internasjonal kriminalitet

Utvalget vil understreke viktigheten av å opprettholde og videreutvikle kompetansen til konsortiet. Utvalget vil videre se det som relevant at Justis- og politidepartementet blir en del av brukermiljøet.

Forslag knyttet til forskning på gjensidige avhengigheter i kritisk infrastruktur

Utvalget anbefaler at det blir startet et forskningsprosjekt rettet mot mulighetene for å redusere gjensidige avhengigheter i kritisk infrastruktur. Utvalget anbefaler at forskningsprosjektet blir initiert og koordinert av Justis- og politidepartementet.

[10] SAMRISK: Samfunnssikkerhet og risikoforskning.

Kapittel 2
Oppnevning, mandat og arbeid

2.1 Oppnevning og sammensetning av utvalget

Virksomheter med ansvar for kritisk infrastruktur opprettholder samfunnets funksjonsdyktighet. Påkjenninger som truer kritisk infrastruktur truer derfor samfunnets funksjonsdyktighet. I dagens samfunn blir de kritiske infrastrukturene i økende grad gjensidig avhengige av hverandre. Dette skyldes blant annet den økte avhengigheten av IKT og utviklingen innen ordinær forretningsdrift, med avskaffing av lagerkapasitet til fordel for *just-in-time* leveranser. Sammenkoblingen mellom virksomhetene har ført til at samfunnet er blitt mer sårbart for svikt i de kritiske infrastrukturene, enten dette skyldes terrorangrep, naturkatastrofer eller uhell. Selv kortvarige bortfall av varer og tjenester kan få dominoeffekter med alvorlige konsekvenser.

En økende andel av samfunnets produksjon av varer og tjenester er i de senere år blitt overlatt til markedet, samtidig som vår avhengighet av disse varene og tjenestene har økt. Dette kan gjelde varer og tjenester som tidligere utelukkende ble levert av offentlige myndigheter eller offentlig eide virksomheter.

Kombinasjonen av økt privatisering av tidligere offentlige virksomheter, redusert offentlig eierskap og en styrket erkjennelse av at private virksomheter forvalter interesser av vital betydning for nasjonen innebærer særskilte utfordringer når det gjelder nasjonens sikkerhet. Tradisjonelt har sikkerhets- og beredskapshensyn vært ansett som viktige argumenter for et offentlig eierskap. Også kontroll med kritisk infrastruktur har vært ansett som viktig. I dag spiller disse hensynene en mindre sentral rolle, men de kan fortsatt berettige eierandeler i enkelte selskaper.

I lys av disse utfordringene ble Utvalg for sikring av landets kritiske infrastruktur (heretter kalt bare utvalget) etablert ved kongelig resolusjon 29. oktober 2004. Utvalget fikk følgende sammensetning:

- Direktør Sven Ullring, tidligere konsernsjef i Det norske Veritas, utvalgets leder (bostedskommune Oslo).
- Direktør Jon Lea, Direktoratet for samfunnssikkerhet og beredskap (bostedskommune Horten).
- Assisterende direktør Toril Hofshagen, NORVAR BA (bostedskommune Hamar).
- Administrerende direktør Grethe Høiland, Lyse AS (bostedskommune Stavanger).
- Avdelingsdirektør Bjørn Tørmo, Nærings- og handelsdepartementet (bostedskommune Vestby).
- Prorektor Gerd Bjørhovde, Universitetet i Tromsø (bostedskommune Tromsø).
- Sikkerhetssjef Anne M. Reinsnes, Telenor (bostedskommune Bærum)
- Direktør Willy Jensen, Post- og teletilsynet (bostedskommune Asker).
- Professor Kåre Petter Hagen, Norges Handelshøyskole (bostedskommune Bergen).
- Prosjektleder Einar Ellingsen, Justis- og politidepartementet (bostedskommune Bodø).

Utvalget har hatt et eget sekretariat. Hovedsekretær og leder for utvalgets sekretariat har vært rådgiver Dagfinn Buset (Justis- og politidepartementet). Øvrige utvalgssekretærer har vært rådgiver Øivind Mandt (Direktoratet for samfunnssikkerhet og beredskap) og seniorrådgiver Bjørn Nilsen (Nasjonal sikkerhetsmyndighet). Rådgiver Kjetil Sørli (Direktoratet for samfunnssikkerhet og beredskap og Nasjonal sikkerhetsmyndighet) inngikk i utvalgets sekretariat fra 7. september 2005, og erstattet Øivind Mandt som gikk ut i fødselspermisjon.

2.2 Mandat

I kgl. res. av 29 oktober 2004 fremgår følgende:

> Utvalget skal vurdere hvordan hensynet til rikets sikkerhet og vitale nasjonale interesser på best mulig vis kan ivaretas overfor virksomheter som ikke er offentlige. Eksempler på områder som utvalgets vurdering skal omfatte er kraft, tele, vannforsyningen, m.m. Utvalgets arbeid skal omfatte alle typer installasjoner og systemer som er nødvendige for at samfunnet

skal fungere tilnærmet normalt. Utvalget gis følgende mandat:

- Utvalget skal kartlegge de virkemidler som brukes for å sikre rikets sikkerhet og vitale nasjonale interesser når offentlige virksomheter privatiseres. Utvalget skal kartlegge virksomheter som antas å ha betydning for rikets sikkerhet og vitale nasjonale interesser. Utvalget skal videre kartlegge de virkemidler som i dag brukes for å sikre rikets sikkerhet og vitale nasjonale interesser i forhold til virksomheter som ikke er offentlige, eller organiserte som selvstendige rettssubjekter helt eller delvis eid av det offentlige.
- Det vises i Sem-erklæringen til at begrunnelser for direkte offentlig eierskap kan være å ivareta økonomisk virksomhet markedet ellers ikke kan løse, for eksempel særlige infrastrukturoppgaver. På denne bakgrunn skal utvalget vurdere hva slags infrastruktur Staten bør eie helt eller delvis. Denne vurderingen skal avgrenses til infrastruktur der særlig viktige hensyn ikke kan ivaretas på annen måte.
- Med utgangspunkt i den samlede oversikt som er fremskaffet gjennom mandatets punkt 1 skal utvalget vurdere hvilke virkemidler som kan være aktuelle å bruke for å ivareta rikets sikkerhet og vitale nasjonale interesser i forhold til virksomheter som privatiseres eller som er i privat eie.
- Ved vurderingen av virkemidler skal utvalget også ta i betraktning om bruk av enkelte virkemidler representerer så vidt store inngrep overfor den tiltakene retter seg mot at bruken av virkemidler må frarås, eller at særskilt lovhjemmel kreves.
- Forholdet til konkurransemessige og øvrige hensyn skal inngå som en del av utvalgets vurderinger.
- Utvalget skal vurdere de økonomiske og administrative konsekvenser av sine forslag. Minst ett forslag skal baseres på uendret ressursbruk, jf. utredningsinstruksen pkt. 3.1.
- Utvalgets rapport skal være Justis- og politidepartementet i hende innen 01.08.2005.[1]

Utvalgets tolkning av sitt mandat

Utvalget har tolket sitt mandat og sammenfattet dette på følgende måte:

- Utvalget skal kartlegge virksomheter som har betydning for rikets sikkerhet og vitale nasjonale interesser, dvs. kartlegge kritiske infrastrukturer og kritiske samfunnsfunksjoner.
- Utvalget skal kartlegge og vurdere virkemidler for sikring av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner.
- Utvalget skal vurdere alle virksomheter med ansvar for kritiske infrastrukturer og kritiske samfunnsfunksjoner, men må spesielt se på de virksomheter som ikke er eiet eller kontrollert av det offentlige.
- Utvalget skal vurdere offentlig eierskap knyttet til kritisk infrastruktur og kritiske samfunnsfunksjoner.
- Utvalget skal utrede konsekvensene av forslagene.

Utvalgets tolkning av mandatet er forankret hos justisminister Knut Storberget og tidligere justisminister Odd Einar Dørum.

Utvalget anser at en drøfting av virkemiddelbruken knyttet til omreguleringer og omorganiseringer i Forsvaret faller utenfor utvalgets mandat. Dette vil være en omfattende oppgave, som krever en egen utredning.

2.3 Arbeidsmetode

Utvalget har sett det som hensiktsmessig å ta utgangspunkt i NOU 2000:24 Et sårbart samfunn, og nyttiggjøre seg det arbeidet sårbarhetsutvalget har gjort. Sårbarhetsutvalget har kartlagt sårbarheter innenfor en rekke samfunnsområder, herunder sårbarheten i kritisk infrastruktur og kritiske samfunnsfunksjoner.

Det første møtet i utvalget ble holdt 22. november 2004, mens det 12. og siste møtet ble holdt 6. mars 2006. Det er avholdt tre to-dagers møter. Møtene det første halvåret ble benyttet til kartlegging og til å skape en felles forståelse av nåsituasjonen knyttet til sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner. Møtene høsten 2005 ble benyttet til å drøfte ønsket situasjon, samt ulike virkemidler for måloppnåelse.

Utvalget har søkt å inkludere flest mulig av sektormyndigheter og eiere av kritiske infrastrukturer. Det er sendt brev med anmodning om innspill til en lang rekke offentlige og private virksomheter. Innspillene fra virksomhetene utgjør en vesentlig del av utvalgets informasjonsgrunnlag.

Nasjonal sikkerhetsmyndighet og Direktoratet for samfunnssikkerhet og beredskap har utarbeidet en rekke notater til utvalget. Det er også innhentet bidrag fra Nærings- og handelsdepartementet, Forsvarets forskningsinstitutt, Statskonsult, ECON Analyse, SEROS – Senter for risikostyring og samfunnssikkerhet, Post- og teletilsy-

[1] Utvalget frist ble forlenget til 31. mars 2006.

net, Finn Erik Vinje og Kari Vogt. Det er for øvrig innhentet kortere bidrag og råd fra noen av de aktørene utvalget har hatt møte med, blant annet Kåre Willoch, Jan Hovden, Tore Bjørgo og Eivind Smith. Samtlige innspill er lagt til grunn i utvalgets arbeid, og de vesentligste tekstbidragene følger som egne vedlegg i del II av utvalgets rapport.

Utvalget har hatt utstrakt møteaktivitet, både nasjonalt og internasjonalt. Det er avholdt om lag 200 møter med offentlige og private virksomheter, organisasjoner og enkeltpersoner. Gjennom disse møtene har utvalget fått informasjon som har vært helt nødvendig for sitt arbeid. Utvalget har også benyttet møtene til å forankre løpende vurderinger og arbeidsmetodikk, samt skape økt bevissthet omkring sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner. En liste over de virksomheter, organisasjoner og enkeltindivider utvalget har hatt møte med følger som vedlegg til utvalgets rapport del I.

Det er foretatt en kartlegging av sektorer og virksomheter for å avdekke hvilke som faller inn under begrepet kritisk infrastruktur og kritiske samfunnsfunksjoner. Kartleggingsarbeidet har foregått i to faser. I første fase er kritisk infrastruktur og kritiske samfunnsfunksjoner sortert etter sektor, virksomhet og infrastruktur/funksjon. I andre fase er det innhentet detaljert informasjon om enkelte sentrale virksomheters virkeområder, eierstrukturer, organisering, bemanning og økonomi. Dette er informasjon som er hentet fra åpne kilder og i dialog med den enkelte virksomhet.

Utvalget arrangerte et arbeidsseminar 17. oktober 2005 for å få en grundig drøfting av forholdet mellom ivaretakelse av hensynet til borgernes frihet og borgernes sikkerhet. Carsten Smith var ordstyrer under seminaret, og Georg Apenes, Jørn Holme, Kåre Willoch og Stein Ørnhøi holdt innlegg om temaet. Formålet med arbeidsseminaret var å få belyst kompleksiteten ved ivaretakelsen av disse hensynene.

I samarbeid med Næringslivets Hovedorganisasjon arrangerte utvalget et arbeidsseminar 20. oktober 2005 for å få belyst hva en utvidelse av sikkerhetsloven i privat sektor vil innebære, og om hensynet til rikets sikkerhet mv. kan ivaretas like godt ved bruk av andre virkemidler. Jens Ulltveit-Moe var ordstyrer under dette seminaret, og Anders Bjønnes (Nasjonal sikkerhetsmyndighet), Tor-Odd Danielsen (Telenor ASA) og Håkon Mageli (Orkla Foods) holdt innlegg om temaet.

Hele utvalget reiste til Sverige for å møte *Krisberedskapsmyndigheten (KBM)*. Norges ambassadør Odd Fosseidbråten deltok på møtet. I tillegg til utfyllende informasjon om KBMs arbeid knyttet til sikring av kritisk infrastruktur, ble utvalget gitt orienteringer fra *Totalförsvarets forskningsinstitut (FOI), TeliaSonera, Säkerhetspolisen (SÄPO), 4C Strategies AB* og Saab AB.

Utvalget delte seg i små grupper og besøkte relevante myndigheter og institusjoner i USA, Canada, Storbritannia, Sveits, Tyskland, Nederland og Singapore.[2]

I USA hadde representanter fra utvalget møter med *Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), National Defense University, George Mason University* og *Heritage Foundation*.

I Canada besøkte representanter fra utvalget *Public Safety and Civil Emergency Preparedness Canada* og *Industry Canada*.

I Storbritannia hadde representanter fra utvalget møte med *National Infrastructure Security Coordination Centre (NISCC), National Security Advice Centre* og *Home Office*.

I Tyskland hadde representanter fra utvalget møte med *Bundesamt für Bevölkerungschutz und Katastrofenhilfe (BBK)* og *Bundesamt für Sicherheit in der Informationtechnik (BSI)*.

Representanter fra utvalget hadde møte med Innenriksministeriet i Nederland.

I Sveits fikk representanter fra utvalget møte med *Federal Office for National Economic Supply, Federal Office of Communication* og *Melde- und Analysestelle Informationssicherung*.

I Singapore hadde utvalgets leder og Norges ambassadør Enok Nygaard møter med *Ministry of Home Affairs*.

[2] Utvalgets leder besøkte sikkerhetsmyndighetene i Singapore i forbindelse med et annet besøk til Singapore. Dette besøket fant sted uten kostnader for staten.

Kapittel 3
Sentrale begreper

3.1 Kritisk infrastruktur og kritiske samfunnsfunksjoner[1]

Samfunnets funksjonsdyktighet er svært avhengig av en rekke fysiske og tekniske infrastrukturer. Ved alvorlig svikt i disse infrastrukturene er samfunnet ikke i stand til å opprettholde de leveranser av varer og tjenester som befolkningen er avhengig av. Disse infrastrukturene kan omtales som kritiske for samfunnet.

Felles er at det ved alvorlig svikt i disse raskt vil kunne oppstå massive forstyrrelser i samfunnet. De har dermed et stort sårbarhetspotensial. Felles er også at de i større eller mindre grad er gjensidig avhengige av hverandre, og virkningene av svikt har dermed en sektorovergripende karakter.

Utvalget har utarbeidet en definisjon for å tydeliggjøre begrepet:

> 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.

Til sammen er dette med på å understøtte rikets sikkerhet og landets vitale nasjonale interesser.

For begrepsmessig å konkretisere kritisk infrastruktur, skiller utvalget mellom kritisk infrastruktur og kritiske samfunnsfunksjoner. En presis tilnærming til hva kritisk infrastruktur er, innebærer å identifisere både kritisk infrastruktur og kritiske samfunnsfunksjoner.

Hvordan identifisere kritisk infrastruktur og kritiske samfunnsfunksjoner?

Utvalgets definisjon angir en retning for hva kritisk infrastruktur er. For å operasjonalisere begrepet kritisk infrastruktur bruker utvalget et sett med skjønnsmessige retningslinjer. Retningslinjene tar utgangspunkt i samfunnets grunnleggende behov – både i forhold til storsamfunnets og enkeltindividets behov. Dette kan være trygghet for den enkelte og basale fysiske behov som vann, mat, varme og lignende. Ut fra samfunnets grunnleggende behov utledes hvilke samfunnsfunksjoner som må til for å dekke de grunnleggende behovene.[2] Disse omtales som kritiske samfunnsfunksjoner.[3] Når forståelsen for hvilke funksjoner som er mest kritiske er etablert, har man et utgangspunkt for å se hvilken infrastruktur som må være på plass for at disse skal fungere.

Eksempelvis kan ett av de mest grunnleggende behovene være å få hjelp ved sykdom og skade. Problemstillingene blir da som følger: Befolkningen har behov for hjelp ved sykdom og skade; samfunnsfunksjonen som dekker behovet er et helsevesen. Hvilke infrastrukturer er nødvendige for å opprettholde funksjonen helsevesen? Det kan eksempelvis være vann- og strøminfrastruktur, farmasøytisk industri osv. Et annet eksempel kan ta utgangspunkt i myndighetenes behov for effektivt å styre og administrere landet. En grunnleggende funksjon som dekker dette behovet er samfunnets ledelsesapparat. Hvilken infrastruktur er funksjonen avhengig av? Det kan eksempelvis være telenettet og strømnettet.

Fremgangsmåten er deduktiv og gir en tilnærming for å vurdere hva slags infrastruktur som må til for å opprettholde driften til en funksjon. På den

[1] Hagen, Janne og Fridheim, Håvard 2005. *Hva er kritisk infrastruktur?* Forsvarets forskningssinstitutt. FFI/Notat 2005/00363 – i del 2, vedlegg 1; Sørli, Kjetil 2005. *Notat – om definisjonen av kritisk infrastruktur.* Direktoratet for samfunnssikkerhet og beredskap – i del 2, vedlegg 2; Sørli, Kjetil 2005. *Sårbarhet i kritisk infrastruktur – utfordringer. Innledende utredning om kritisk infrastruktur til Utvalg for sikring av landets kritiske infrastruktur.* Direktoratet for samfunnssikkerhet og beredskap – i del 2, vedlegg 3.

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

[3] Begrepet kritiske samfunnsfunksjoner kan også omtales som samfunnskritiske funksjoner eller samfunnets kritiske funksjoner.

annen side gir den ingen svar på hvilke av infrastrukturene som er mest sårbare og utsatte for bortfall. Den gir heller ingen svar på hvilke av infrastrukturene som har det største skadepotensial for samfunnets funksjonsdyktighet ved bortfall, og som dermed utgjør kritisk infrastruktur.

På et overordnet nivå kan det angis særlig tre kriterier for å identifisere kritisk infrastruktur. Fremgangsmåten og kriteriene legger til sammen til rette for å systematisere en skjønnsmessig vurdering. For det første kan kritisk infrastruktur avgrenses ut fra kriteriet avhengighet, for det andre ut fra kriteriet alternativer og for det tredje ut fra kriteriet tett kobling.

Avhengighet

Første trinn innebærer å finne avhengighet av den aktuelle infrastrukturen. Bortfall av infrastruktur som et stort antall er avhengig av har alvorlige konsekvenser, og dette kriteriet veier tyngst når kritisk infrastruktur skal identifiseres. Et stort antall av eksterne avhengige tilsier altså kritikalitet.

Eksempelvis er hele samfunnet avhengig av en veginfrastruktur for å fungere. På samme måte er praktisk talt alle samfunnsfunksjoner avhengig av strøm gjennom kraftinfrastrukturen og vann gjennom vannforsyningsinfrastrukturen.

Alternativer

Andre trinn innebærer å vurdere alternativer. Manglende alternativer tilsier kritikalitet.

Eksempelvis har Norge et stort antall kraftverk spredt ut over hele landet. Dette medfører at bortfall av ett kraftproduserende anlegg ikke får store konsekvenser for kraftleveransen sett under ett. Dette står i motsetning til land med noen få, men store kraftproduserende enheter. Bortfall av ett kraftproduserende anlegg vil i slike tilfeller få store konsekvenser på grunn av manglende alternativer av kraftproduserende enheter.

Tett kobling

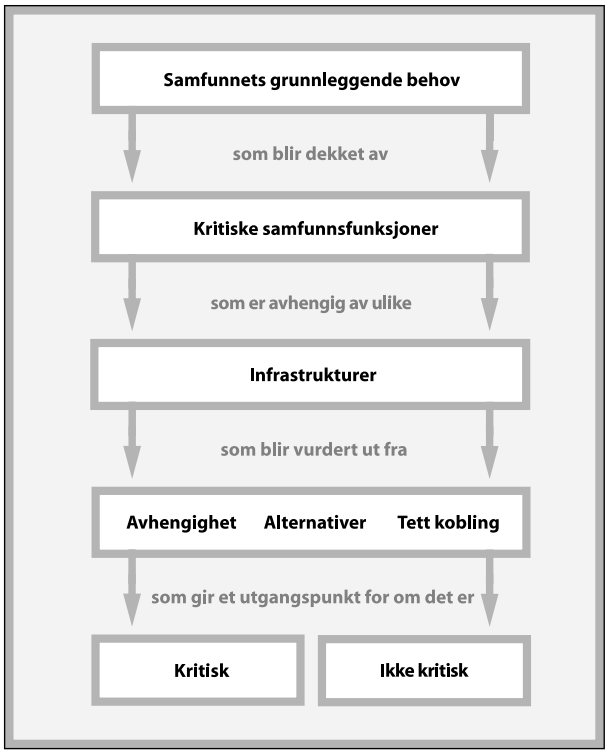
Tredje trinn innebærer å vurdere i hvilken grad infrastrukturen er tett koblet. Et tett koblet system innebærer at forstyrrelser ett sted i systemet får umiddelbare konsekvenser for systemet som helhet. Mestring av et tett koblet system krever sentralisert styring.[4] Høy grad av tett kobling tilsier kritikalitet.

Eksempler kan hentes fra offentlig transport. Jernbane og lufttrafikk i Norge er avhengig av sentralisert styring i sanntid for effektiv og sikker drift. Busstrafikk kan derimot operere uten en sentralisert styring, eller i hvert fall med langt lavere grad av sentralisert kontroll og styring i sanntid. Bortfall av knutepunkter i tett koblede systemer vil få store konsekvenser for funksjonsdyktigheten til infrastrukturen. El-nettet, særlig sentralnettet, er et ytterligere eksempel.

Skjematisk kan retningslinjene fremstilles som vist i figur 3.1.

Ved å ta en overordnet gjennomgang av de ulike sektorenes infrastruktur med bakgrunn i retningslinjene, vil det avtegne seg et bilde av at det er noen felles infrastrukturer som går igjen hos de aller fleste og som mange er svært avhengige av. Det fremkommer også at det er noen deler av infrastrukturen som er mer utsatte enn andre.

På bakgrunn av retningslinjene mener utvalget at *kritisk infrastruktur* per i dag skal avgrenses til å gjelde de anlegg og systemer som understøtter elektrisk kraft, elektronisk kommunikasjon, transport, olje og gass, vann og avløp og satellittbasert infrastruktur: Nærmere vurderinger av de ulike infrastrukturene er omtalt i kapittel 10.



Figur 3.1 Retningslinjer for å identifisere kritisk infrastruktur og kritiske samfunnsfunksjoner ut fra samfunnets grunnleggende behov.

[4] Teorien om tett koblede systemer er hentet fra Charles Perrows teorier om systemulykker. En av Perrows hovedteser er at et tett koblet system bare kan kontrolleres effektivt gjennom sentralisert styring. Perrow viser til jernbanesystemer og fly som tett koblede systemer. Perrow, Charles 1999. *Normal Accidents. Living with High Risk Technologies.* Princeton University Press.

Tabell 3.1 Kritisk infrastruktur og kritiske samfunnsfunksjoner. Utvalget har ikke eksplisitt vurdert de kritiske samfunnsfunksjonene som står i kursiv

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

Utvalget har også identifisert hvilke samfunnsfunksjoner som er mest kritiske for samfunnet med utgangspunkt i de overnevnte retningslinjene. Utvalget har avgrenset disse til å være bank og finans, matforsyning, helse, sosial og trygdetjenester, politi, nød- og redningstjeneste, kriseledelse, Regjering, Storting, forsvar, domstolene, miljøovervåkning og renovasjon, som vist i tabell 3.1.

Nærmere vurderinger av de ulike samfunnsfunksjonene er omtalt i kapittel 11 med unntak av Storting, Regjering, domstolene, forsvar, miljøovervåkning og renovasjon.[5]

Utvalget understreker at retningslinjene ikke gir en endelig og objektiv oversikt over hva som er kritiske og hva som ikke er kritiske infrastrukturer og samfunnsfunksjoner. Høy grad av kompleksitet, stor dynamikk og gjensidige avhengigheter i infrastrukturer og samfunnsfunksjoner tillater ikke absolutte avgrensinger, men tilsier tvert i mot bruk av skjønn. Forståelsen av hva som er kritisk vil også endre seg over tid, noe som skyldes endringer i den generelle samfunnsutviklingen, utviklingen og anvendelsen av ny teknologi, og endringer i økonomiske og sosiale forhold. Selv om retningslinjene ikke gir eksakte svar, så tilrettelegger de for en skjønnsmessig vurdering. Utvalget har derfor funnet de formålstjenlige som et utgangspunkt for å skjønnsmessig vurdere overordnede virkemidler knyttet til kritisk infrastruktur og kritiske samfunnsfunksjoner.

På bakgrunn av en skjønnsmessig vurdering har utvalget laget en liste over kritiske infrastrukturer og kritiske samfunnsfunksjoner. Denne listen er sikkerhetsgradert.

3.2 Rikets sikkerhet og vitale nasjonale interesser

Utvalget har valgt å ta utgangspunkt i NOU 2003:18 Rikets sikkerhet (straffelovskommisjonens delutredning VIII) for å tolke begrepene «rikets sikkerhet» og «vitale nasjonale interesser».

Tradisjonelt omfatter begrepet «rikets sikkerhet» forhold av sikkerhetspolitisk betydning for vår nasjonale handlefrihet og vår territorielle integritet. Begrepet er i stor grad knyttet til sikkerhetspolitiske scenarier som krig, sikkerhetspolitisk krise og internasjonal terrorisme.

Det er lagt til grunn at innholdet i begrepet «rikets sikkerhet» vil kunne forandre seg med samfunnsutviklingen. Det er blant annet blitt tydeligere at begrepet ikke bare omfatter «ytre sikkerhet» (vårt sikkerhetspolitiske forhold til andre stater), men at begrepet også omfatter «indre sikkerhet».

I drøftingen av begrepet «rikets sikkerhet» i forhold til spørsmålet om hva som skal vernes av straffeloven (NOU 2003:18), bringes begrepet grunnleggende nasjonale interesser inn (side 72):

> Under enhver omstendighet finner utvalget at vernet mot innhenting og avsløring av hemmelige opplysninger, ikke bør begrenses til interesser som gjelder rikets sikkerhet i tradisjonell forstand, men at også grunnleggende nasjonale interesser ellers bør omfattes. Ved siden av forholdet til andre stater, herunder forhandlingsposisjoner, er det nærliggende å fremheve de interesser som er knyttet til infrastrukturen, energi-, mat- og vannforsyning, samferdsel og telekommunikasjon, helseberedskap, bank- og pengevesen og andre samfunnsøkonomiske forhold, [...]

Sikringen av landets kritiske infrastruktur og kritiske samfunnsfunksjoner, omfattes således av begrepet «*grunnleggende* nasjonale interesser». Etter utvalgets mening er det ingen grunn til å

[5] Utvalget mener at en vurdering av Forsvaret som kritisk samfunnsfunksjon vil kreve en egen utredning. Det har ikke vært mulig innenfor utvalgets tids- og ressursrammer å vurdere Storting, Regjering, domstolene, forsvar, miljøovervåkning og renovasjon, men utvalget påpeker at disse er kritiske samfunnsfunksjoner.

skille mellom meningsinnholdet i de mange variantene som finnes av dette begrepet[6].

Det følger av ovennevnte at begrepene «rikets sikkerhet» og «vitale nasjonale interesser» til sammen skal dekke samfunnets totale sikkerhetsinteresser, slik de defineres på bakgrunn av de sikkerhetsutfordringene Norge til enhver tid står overfor. Samtidig er det viktig at terskelen for å anse noe for å true «rikets sikkerhet» og «vitale nasjonale interesser» skal være høy.

En konsekvens av å opprettholde en viss dynamikk i meningsinnholdet til begrepene «rikets sikkerhet» og «vitale nasjonale interesser», er at begrepene først vil finne sin nærmere avgrensning gjennom forvaltningspraksis, fagteori, domstolspraksis, m.m. I denne utredningen favner begrepene «rikets sikkerhet» og «vitale nasjonale interesser» sikringen av landets kritiske infrastruktur og kritiske samfunnsfunksjoner.

3.3 Risiko

En vanlig definisjon er å se på risiko som en kombinasjon av mulige konsekvenser og tilhørende sannsynligheter.[7] Mer generelt kan risiko defineres som kombinasjonen av mulige konsekvenser og tilhørende usikkerhet. Sannsynlighetsbegrepet brukes til å uttrykke denne usikkerheten og definisjonene faller således sammen hvis vi begrenser oss til en kvantitativ beskrivelse. Ulike risikoindekser brukes, som for eksempel forventet tap fremkommet ved å multiplisere mulige tap med tilhørende sannsynlighet. Forventningsverdien gir begrenset informasjon i forhold til kombinasjonen av mulige konsekvenser og sannsynlighet (usikkerhet).

Risikoen avhenger av den foreliggende informasjon og kunnskap, og er således ikke en objektiv størrelse. Når usikkerhetene er små vil en imidlertid kunne gi gode prediksjoner av de mulige konsekvenser. Det kan bety at sannsynlighetsfordelingen over mulige konsekvenser er mer konsentrert, noe som utelukker ekstreme konsekvenser.

Det er også mulig å tilnærme seg risiko ved å legge vekt på en samfunnsmessig verdivurdering. Fokus vil da være på konsekvens, og ikke på sannsynlighet. For eksempel vil risikovurderinger knyttet til rikets sikkerhet og vitale nasjonale interesser legge stor vekt på konsekvenser, og mindre på sannsynlighet. I slike tilfeller vil det iverksettes defensive sikkerhetstiltak på grunnlag av den samfunnsmessige verdien, ikke på grunnlag av sannsynligheten for at en hendelse skal skje.

Risikoen kan også uttrykkes med et spredningsmål for mulige konsekvenser, som standardavvik eller statistisk varians. Liten spredning indikerer stor grad av forutsigbarhet mht. konsekvenser og i den forstand mindre risiko.

En annen tilnærming er å vurdere to ulike innfallsvinkler når risiko for terrorhandlinger skal vurderes.[8] For det første ved et sårbarhetsperspektiv. Utgangspunktet for analysen er da å undersøke hvor lett eller vanskelig det er å forårsake skade, og hvor store konsekvenser det eventuelt vil kunne få. For det andre ved å ha et trusselperspektiv. Utgangspunktet for analysen er da å identifisere mulige aktører som kan ha interesse av å utføre skade, og eventuelt hvilken kapasitet de har til å gjennomføre en skadelig handling.

Tilnærmingen til risikobegrepet er som vist ikke ensidig, og avhenger i stor grad av hvilket fagmiljø man kommer fra, og hva formålet med risikovurderingen er.

3.4 Sårbarhet

Sårbarhetsutvalget (NOU 2000:24) definerte sårbarhet på følgende måte:

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

Sårbarhet er beskrevet på følgende måte i Innst. S. nr. 9 (2002-2003) fra forsvarskomiteen og justiskomiteen:

> Sårbarhet betegner en begrenset evne til å tåle påkjenninger eller påvirkninger som kan resultere i betydelige negative avvik fra normal funk-

[6] I tillegg til at Straffelovkommisjonen benytter begrepet «grunnleggende nasjonale sikkerhetsinteresser», benyttes begrepet «vitale nasjonale interesser» i utvalgets mandat, begrepet «vitale nasjonale sikkerhetsinteresser» brukes i sikkerhetsloven, mens begrepet «viktige nasjonale interesser» brukes i etterretningsloven.

[7] Denne tilnærmingen sammenfaller med ISO-standardens definisjon av risiko.

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

sjon for det system som den sårbare komponent inngår i. Graden av sårbarhet beskriver hvor lett det er å påføre slik skade.[9]

En annen måte å tilnærme seg sårbarhetsbegrepet på, er å se på avhengighet. Fokuset dreies da fra de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, til å se på hvor avhengig systemet er av eksterne leverandører for normal drift. Tilnærmingsmåten er komplementær og utelukker ikke den første. Følgende eksempler kan illustrere tilnærmingsmåten: De brukere som ønsker å gå fra fasttelefoni til IP-telefoni gjør seg avhengig av strøm og Internettilgang lokalt for å få summetone. Tilgang til telefoni blir da sårbar overfor strømbrudd og bortfall av Internett. Et annet eksempel er pasienter som bruker elektromedisinsk utstyr og som ønsker å flytte hjem fra sykehus. Hvis pålegg om nødstrøm også hjemme ikke blir fulgt, gjør brukeren seg avhengig av strømforsyningen, og sårbarheten øker. Tilnærmingen er nyttig for å vise til samfunnets sårbarhet som resultat av avhengighet til eksempelvis strøm, tele og vann.

3.5 Trussel

Trusselbegrepet omhandler kapasitet og intensjon til å gjennomføre skadelige handlinger. Siden intensjoner kan endre seg raskt, kan trusselsituasjonen, i motsetning til sårbarheter, være svært dynamisk over et kort tidsrom. [10]

Begrepet trussel brukes også til å beskrive faren ved konsekvensene av utilsiktede hendelser. En trussel vil i denne sammenhengen ikke bestå av aktører med kapasitet og intensjon til å gjennomføre skade, men bestå av at hendelsen i seg selv vil kunne utgjøre en trussel mot noe eller noen. Eksempelvis vil en brann i en høyblokk utgjøre en trussel mot sikkerheten til de som oppholder seg der.

3.6 Samfunnssikkerhet

Begrepet samfunnssikkerhet er ikke entydig.[11] Det er ikke knyttet til noe bestemt scenario av typen krig eller terror, men omfatter alle typer påkjenninger samfunnet kan utsettes for. Det er samtidig klart at begrepet omfatter påkjenninger som påvirker nasjonens indre sikkerhet og vitale nasjonale interesser. Tiltak for å ivareta befolkningens trygghetsfølelse og tiltak for å sikre kritisk infrastruktur og kritiske samfunnsfunksjoner omfattes av begrepet samfunnssikkerhet.

Det kan identifiseres tre ulike tilnærminger til begrepet: En bred, en snever og en politisk. Den sistnevnte beveger seg mellom de to andre, avhengig av det politiske sakskartet.

I den brede tilnærmingen er samfunnssikkerhet for det første å kunne forebygge og håndtere ekstraordinære hendelser. For det andre er samfunnssikkerhet å ha ressurser til å forebygge og håndtere dagligdagse hendelser. For eksempel truer ikke én enkelt brann samfunnets sikkerhet, men hvis samfunnet ikke har ressurser til å forebygge og håndtere branner vil samfunnets sikkerhet være truet. For det tredje innebærer samfunnssikkerhet å forhindre at mindre hendelser blir så mange at det går ut over samfunnet. For eksempel fører dødsulykker i trafikken til store personlige og samfunnsmessige omkostninger, men de truer ikke samfunnets sikkerhet i seg selv.

Fellesnevneren i forhold til en bred definisjon som omfatter de tre aspektene, er at det på en eller annen måte har å gjøre med samfunnets mulighet til å minimalisere alle tenkelige risikoer. Det kan argumenteres for at en bred definisjon av begrepet gjør det upresist og vanskelig å bruke, og da særlig i forhold til en politisk virkelighet hvor det alltid vil være et spørsmål om å prioritere.

Den andre og mer snevre tilnærmingsmåten har fokus på at samfunnssikkerhet handler om å forebygge og håndtere ekstraordinære hendelser som krever ressurser ut over det vanlige. Her er de dagligdagse hendelsene holdt utenfor. Hensikten med å spisse begrepet er å forhindre at de dagligdagse hendelsene tar all fokus fra de ekstraordinære, slik at samfunnet dermed står i fare for glemme disse. Innenfor en slik definisjon har ekstraordinære hendelser fokus fordi de har et meget stort skadepotensial.

Den tredje definisjonen av samfunnssikkerhet er den politiske. I St. meld. nr. 17 (2001-2002) Samfunnssikkerhet, står det følgende:

> Samfunnssikkerhet brukes i denne meldingen for å beskrive den evne samfunnet som sådan har til å opprettholde viktige samfunnsfunksjo-

[9] Innst. S. nr. 9 (2002–2003) *Innstilling fra forsvarskomiteen og justiskomiteen om samfunnssikkerhet - Veien til et mindre sårbart samfunn,* kapittel 5.

[10] Henriksen, Stein 2004. Ikke utgitt utvidet manus *NSBR04.* Direktoratet for samfunnssikkerhet og beredskap; Mærli, Morten Bremer 2004. *Crude Nukes on the Loose?* Unipub AS 2004.

[11] Sørli, Kjetil 2005. Notat – *Et blikk på begrepet samfunnssikkerhet for å operasjonalisere «nasjonal trygghetsfølelse».* Direktoratet for samfunnssikkerhet og beredskap – i del 2, vedlegg 4.

ner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for påkjenninger.

[...]

Arbeidet med samfunnssikkerhet tar utgangspunkt i at kriser skal forhindres og at kriser som har oppstått håndteres på en så god måte som mulig. De mest sentrale målsettinger for arbeidet med samfunnssikkerhet er at avbrudd i viktige samfunnsfunksjoner og større ulykker ikke skal medføre alvorlige samfunnsmessige tap.[12]

Samfunnssikkerhetsbegrepet brukes bredt og dekker sikkerhet mot hele spekteret av utfordringer, fra begrensede, naturskapte hendelser, via større krisesituasjoner som representerer omfattende fare for liv, helse, miljø og materielle verdier, til sikkerhetsutfordringer som truer nasjonens selvstendighet eller eksistens.

I St. meld. nr. 39 (2003-2004) Samfunnssikkerhet og sivilt-militært samarbeid, står det følgende:

> Regjeringen vil understreke at det grunnleggende mål for alt samfunnssikkerhetsarbeid er å forebygge at uønskede hendelser inntreffer og minimalisere konsekvensene når slike situasjoner skulle oppstå. [...] Arbeidet med forebyggende brannvern er en viktig del av samfunnssikkerhetsarbeidet. [...] I samfunnssikkerhetsarbeidet er det nødvendig å vie oppmerksomhet til mulige negative konsekvensene av et endret klima.[13]

Her er det ikke lenger ekstraordinære hendelser, men forebygging av uønskede hendelser som ligger til grunn. Forklaringer på endringen i bruken av begrepet er flere. De kan være både organisatoriske og trusselmessige, men viser primært at begrepet er under endring, og at det lar seg påvirke av den politiske virkeligheten.

St.meld. nr. 37 (2004–2005) Flodbølgekatastrofen i Sør-Asia og sentral krisehåndtering, omtaler samfunnssikkerhet på følgende måte:

> Samfunnssikkerhet dreier seg om å ivareta sivilbefolkningens trygghet og sikre sentrale samfunnsfunksjoner og viktig infrastruktur mot angrep og annen skade i situasjoner der statens grunnleggende interesser ikke er truet. Samtidig har utviklingen medført et økt fokus på menneskelig sikkerhet der menneskerettighetene og ikke minst retten til liv og personlig trygghet står i sentrum.
>
> [...]
>
> Sentralt i dagens samfunnssikkerhetsarbeid er beskyttelse av sivilbefolkningen og vitale samfunnsinteresser i situasjoner hvor det ikke foreligger en tradisjonell militær trussel.
>
> [...]
>
> De sikkerhetspolitiske rammene, og da særlig utviklingen i internasjonal terrorisme, har fått økt betydning for samfunnssikkerheten. En rekke risikofaktorer, som faren for smittsomme sykdommer, naturhendelser og store ulykker har også fått økt betydning for sikkerhets- og beredskapsarbeidet nasjonalt.
>
> [...]
>
> Brannvesenet er en vesentlig ressurs på samfunnssikkerhetsområdet. Et velfungerende brannvesen er av grunnleggende betydning for samfunnets evne til å kunne håndtere også ekstraordinære hendelser.[14]

Her er det sikring av sentrale samfunnsfunksjoner og viktig infrastruktur som blir vektlagt. Også den nye sikkerhetspolitiske situasjonen blir trukket frem. Samtidig blir det vist til retten til liv og personlig trygghet. Omtalen av begrepet, slik det fremstår her, kan derfor hevdes å ha en tyngde mot å trygge samfunnet og i mindre grad mot individet. Både tilsiktede og utilsiktede hendelser er trukket frem.

3.7 Totalforsvar og sivilt-militært samarbeid

I Norge har sivile og militære tiltak som er relevante for nasjonal sikkerhet og forsvar blitt gruppert under begrepet totalforsvar. Begrepet har antakelig sin opprinnelse fra Forsvarskommisjonen av 1946, og ble etter hvert også benyttet i andre nordiske land. Det faktiske begrepsinnholdet er imidlertid basert på de erfaringer flere nasjoner, både krigførende og nøytrale, fikk i løpet av de to verdenskrigene.

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

Hovedformålet med totalforsvarskonseptet var å kanalisere så mange ressurser som mulig inn i militært forsvar av landet, og å sikre fysisk overlevelse for (så mange som mulig av) befolkningen, sivile eller militære. Trusselen om den totale krig

[12] St.meld. nr. 17 (2001-2002) *Samfunnssikkerhet.*

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

[14] St.meld. nr. 37 (2004-2005) *Flodbølgekatastrofen i Sør-Asia og sentral krisehåndtering.*

rammet inn begrepet. I prinsippet gjaldt målsetningen gjennom hele den kalde krigen og fremstår som en restoppgave den dag i dag, men nå som en del av samfunnssikkerheten.

Med dagens sikkerhetspolitiske utfordringer for fastlands-Norge og tilliggende sjøområder, ligger vekten mer på hva Forsvaret kan gjøre for det sivile samfunnet, enn på hva det sivile samfunnet kan gjøre for å støtte Forsvaret. Samarbeidet mellom sivile og militære myndigheter for å støtte opp under samfunnssikkerhet omtales ofte som «sivilt-militært samarbeid».

Utvalget velger å bruke betegnelsen sivilt-militært samarbeid.

3.8 Beredskap og forebygging

Beredskap er planlegging og forberedelse av tiltak for å håndtere uønskede hendelser på best mulig måte etter at de har skjedd. Forebygging er tiltak som søker å redusere sannsynlighet for at uønskede hendelser oppstår, og tiltak som skal redusere konsekvensene av en uønsket hendelse.

I kjernen av begrepet beredskap ligger erkjennelsen om at det alltid vil oppstå uønskede hendelser selv om forebyggende tiltak er iverksatt på forhånd. Det vil likevel være et mål å redusere sannsynligheten for uønskede hendelser ved å forebygge. Det fremstår derfor som en utfordring å balansere forebyggende tiltak og beredskapstiltak.

Forholdet mellom prioritering av beredskap og forebyggende tiltak er berørt i kapittel 14, økonomiske og administrative konsekvenser.

3.9 Befolkningens trygghetsfølelse

Begrepet befolkningens trygghetsfølelse er en subjektiv størrelse. Det handler om en opplevd trygghet for at samfunnet fungerer normalt og at risikoer er kjente og under kontroll. Bortfall av befolkningens trygghetsfølelse beskriver en situasjon der den opplevde følelsen av trygghet erstattes av frykt, usikkerhet og tvil i store deler av befolkningen. Dette kan igjen ha store samfunnsmessige konsekvenser.

Det er ingen direkte sammenheng mellom den reelle sikkerhetssituasjonen i samfunnet og trygghetsfølelsen i befolkningen. Dette misforholdet kan skape forventninger om tiltak i sikkerhets- og beredskapsarbeidet som objektivt sett kan være uhensiktsmessige. Uhensiktsmessige, situasjonsavhengige forventninger kan legge press på grunnleggende rettigheter som eksempelvis personvern, rettssikkerhet, eiendomsrett, ytringsfrihet og bevegelsesfrihet. Det kan dessuten foranledige tiltak som objektivt sett ikke tjener noe annet formål enn å synliggjøre at myndighetene responderer på befolkningens opplevde sikkerhetsbehov.

3.10 *Safety* og *Security* – på norsk

De engelske ordene *safety* og *security* brukes som hjelpeord på norsk for å beskrive to aspekter ved sikkerhet. *Safety* brukes for å beskrive sikkerhet mot uønskede hendelser som resultat av tilfeldigheter. *Security* brukes for å beskrive sikkerhet mot uønskede hendelser som resultat av overlegg.[15] Bruken av engelske ord gjenspeiler at det ikke eksisterer noen leksikal distinksjon mellom de to typene av uønskede hendelser på norsk.[16] Det kan også stilles spørsmål ved hvorvidt det er fullt ut sammenfall mellom hvordan de norske fagmiljøer bruker de engelske ordene og engelsk dagligtale.

Bruk av tilsvarende ord på norsk kan gjøres etter skjønn – de kan såkalt stipuleres, noe som er legitimt når det som i vårt tilfelle springer ut fra et faglig behov. Likevel ligger det ingen automatikk i at stipulerte ord blir tatt i bruk. Enkelte store norske konserner har stipulert norske ord for *safety* og *security* til eget bruk. *Safety* er satt til «sikkerhet», mens *security* er satt til «sikring».

Ut fra et ønske om å finne tilfredsstillende norske ord har utvalget bedt professor Finn-Erik Vinje vurdere norske ord for *safety* og *security*.[17] I sitt tilsvar til utvalget har professor Vinje kommet frem til at en *mulig* tilnærming kan være en tredeling av begrepet. Begrepet «sikkerhet» kan brukes til å dekke alle uønskede hendelser, uavhengig av om de er utilsiktede eller tilsiktede. «Sikkerhet» fremstår på denne måten som et overbegrep, et såkalt hypernym. Sikkerhet mot uønskede utilsiktede hendelser kan settes til «trygghet», mens sikkerhet mot uønskede tilsiktede hendelser kan settes til «sikring».

Utvalget er på linje med professor Finn-Erik Vinje når han skriver at dette «[...]vil være en vilkårlig konstruksjon – i den forstand at den ikke er oppstått spontant i allmennspråket og neppe imøtekommer noe presserende behov der».

Både «trygghet» og «sikring» blir i dagligtalen brukt om hverandre for å beskrive sikkerhet mot både uønskede utilsiktede og tilsiktede hendelser.

---

15 NOU 2000:24 *Et sårbart samfunn*.

16 Den kan i denne sammenheng nevnes at de to ordene heller ikke er entydige i engelsk dagligtale.

17 Vinje, Finn-Erik 2005. *Sikkerhet – Safety/Security. En begrepsutredning* – i del 2, vedlegg 5.

Utvalget ønsker likevel å understreke betydningen av at ordet «sikkerhet» blir benyttet som et hypernym. Etter utvalgets mening burde alt sikkerhetsarbeid omhandle både *safety* og *security*. Ved å bruke sikkerhet som et hypernym blir dette understreket. For å beskrive *safety* på norsk, bruker utvalget «sikkerhet mot uønskede utilsiktede hendelser». For å beskrive *security* på norsk, bruker utvalget «sikkerhet mot uønskede tilsiktede hendelser». Ved å benytte seg av en slik tredeling, oppnås ønsket presisjon, samtidig som man unngår å stipulere ord som ikke faller naturlig i norsk dagligtale.

Kapittel 4
Sikkerhetsutfordringer

Informasjon om ulike sikkerhetsutfordringer er et fundament for innretting og prioritering av tiltak for sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner. I dette kapittelet gis det først en kort oversikt over den sikkerhetspolitiske ramme slik den fremstår i dag. Deretter presenteres i korte trekk sikkerhetsutfordringer for kritisk infrastruktur og kritiske samfunnsfunksjoner. Med det menes ulike trusler, sårbarheter og risikoer som kan medføre svikt eller ødeleggelse av kritisk infrastruktur og kritiske samfunnsfunksjoner.[1] Videre redegjøres det for rollene til Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet, Etterretningstjenesten og Direktoratet for samfunnssikkerhet og beredskap i forhold til å rapportere trussel-, risiko- og sårbarhetsinformasjon.

4.1 Nye sikkerhetspolitiske utfordringer

Norsk sikkerhetspolitikk er under endring. For det første har forutsetningene for den tradisjonelle sikkerhetspolitikken endret seg. For det andre favner begrepet bredere nå enn tidligere.

En tradisjonell tilnærming til sikkerhetspolitikk tar utgangspunkt i forsvars- og utenrikspolitiske virkemidler for å ivareta og fremme grunnleggende nasjonale sikkerhetsinteresser.[2] Deltagelse i kollektive sikkerhetsorganisasjoner som FN og NATO, opprettholdelsen av et relevant nasjonalt forsvar og en aktiv utenrikspolitikk for å nå nasjonale mål, er eksempler på det.

Avslutningen av den kalde krigen, oppblomstring av regionale konflikter på 1990-tallet og fremveksten av internasjonal terrorisme har endret forutsetningene for den tradisjonelle sikkerhetspolitikken. Også økende forpliktende samarbeid og gjensidig avhengighet mellom land og regioner er med på å understreke endringene. Videre påvirker globaliseringen utformingen av sikkerhetspolitikken med blant annet forhold som økt bevegelse av tjenester, varer, mennesker, kulturimpulser, ideologier og religioner over landegrensene.

Endrede forutsetninger for den tradisjonelle sikkerhetspolitikken har blant annet ført til at territorialforsvaret ikke lenger er førende for utforming og innretting. Dagens forsvarspolitiske konsept er i større grad innrettet mot å sikre nasjonale interesser ved å delta i militære operasjoner utenlands. På det utenrikspolitiske området medfører det økende antall berøringspunkter mellom nasjoner at en større andel av den utenrikspolitiske samhandlingen blir håndtert av andre enn Utenriksdepartementet. Endringer i forutsetningene for det som kan omtales som en tradisjonell sikkerhetspolitikk faller sammen med fremveksten av det som er omtalt som sårbarhetssamfunnet, hvor det moderne samfunn i økende grad er sårbart for bortfall av kritiske tjenester og ressurser.[3]

Den økte bevisstheten om samfunnets sårbarhet har skapt grunnlaget for å se sikkerhetspolitiske utfordringer på en ny måte: Den tradisjonelle sikkerhetspolitiske tilnærmingen som er fundert i de to pilarene utenriks- og forsvarspolitikk, er i større grad enn tidligere supplert med en tredje pilar, nemlig samfunnssikkerhet. Der den tradisjonelle utenriks- og forsvarspolitikken bidrar til å gi nasjonen handlingsrom i forhold til andre nasjoner og eksterne trusler, handler samfunnssikkerhet om å gi nasjonens innbyggere trygghet for at samfunnet fungerer normalt. Beskyttelse av landets kritiske infrastruktur og kritiske samfunnsfunksjoner er en viktig komponent i dette.[4]

Avhengighet av sivil infrastruktur er ikke noe nytt. I etterkrigstiden førte erkjennelser om avhengighet til at det ble bygget opp et apparat for å sikre

[1] Se for øvrig Davidsen, Bjørnar og Nilsen, Bjørn 2005. *Risikobildet. Notat til infrastrukturutvalget.* Nasjonal sikkerhetsmyndighet – i del 2, vedlegg 6.

[2] Forsvarsdepartementet omtaler dette som statssikkerhet. St.prp. nr. 42 (2003-2004) *Den videre moderniseringen av Forsvaret i perioden 2005-2008.*

[3] Den første BAS-studien til Forsvarets forskningsinstitutt fra 1997 og sårbarhetsutvalgets utredning fra 2000 var blant de første i Norge som viste til det. NOU 2000:24 *Et sårbart samfunn;* Hæsken, Ole Morten. Olsen, Thor Gunnar. Fridheim, Håvard. *Beskyttelse av samfunnet (BAS) – Sluttrapport.* Forsvarets forskningsinstitutt. FFI/Rapport-97/01459.

[4] En fjerde pilar i det sikkerhetspolitiske begrepet handler om grunnleggende verdier som menneskerettigheter, demokrati, rettstatens prinsipper og lignende.

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

Endringer i både samfunnets struktur og trusselbildet har medført at det i større grad enn tidligere er sivile og ikke militære utfordringer som er rammen for dagens sikkerhetspolitiske utfordringer. Med dagens sikkerhetspolitiske forståelse ligger vekten mer på hva Forsvaret kan gjøre for å bistå det sivile samfunnet enn hva det sivile samfunnet kan gjøre for å forsvare landet mot en ekstern fiende. Tiltak for å trygge eksempelvis kraftforsyning og telenettet er i dag ikke begrunnet ut fra en totalforsvarstankegang, men ut fra det sivile samfunns avhengighet av kraft og tele.

4.2 Sikkerhetsutfordringer – kritisk infrastruktur og kritiske samfunnsfunksjoner

Under den kalde krigen var trusselen klart definert, og den var i hovedsak av militær art. Dagens trusselbilde fremstår derimot som diffust. Det er i mange sammenhenger mer naturlig å snakke om potensielle trusler, enn konkrete trusler. Usikkerhet og trusler knyttet til forhold som klimaendringer, internasjonal terrorisme og naturkatastrofer er eksempler på det. Ingen av disse potensielle truslene er nødvendigvis nye. Det nye er at truslene har endret karakter, og har et potensial for å true samfunnets sikkerhet ved at samfunnets sårbarhet er endret. I sum er de potensielle truslene blitt flere og mer uoversiktlige. De har også potensial for å ramme kritisk infrastruktur og kritiske samfunnsfunksjoner. Sårbarheten har også endret seg. Det skyldes økende avhengighet av teknologiske løsninger, introduksjon av ny teknologi, nye måter å organisere virksomheter på (omregulering/bortsetting) og trekk ved globalisering. En rekke av disse utfordringene vil i det følgende bli omtalt.

4.2.1 Klimaendringer/naturkatastrofer

Klimaet er i endring, og global oppvarming vil gi effekter i store deler av verden. I forskningsprogrammet RegClim[5] arbeides det med å utarbeide regionale scenarioer for klimaets utvikling. Et av disse områdene er Norden. I følge RegClim forventes det et våtere høst- og vinterklima på Vestlandet. Videre forventes det en generell vindøkning som særlig vil slå ut fra Vestlandskysten til Trøndelag, samt i Barentshavet øst for Finnmark. Det kan forventes at deler av det norske samfunnet må tilpasse seg økt nedbørsmengde, økt frekvens av storm og stormflo samt økt fare for flom, skred og ras. Slike endringer kan gi utfordringer med hensyn til kritiske samfunnsfunksjoner og kritisk infrastruktur.

Samferdsel, bygningsmasse, kraftforsyningsanlegg og anlegg for vannforsyning og avløpshåndtering vil stå overfor klimarelaterte utfordringer i årene fremover. Både veger, bygninger og tekniske anlegg er viktige fysiske strukturer for samfunnet. Dimensjonering av hva slike konstruksjoner skal tåle vil være en viktig faktor for tilpasning til endrede klimabetingelser.[6]

Med store mengder nedbør over kort tid er det fare for at dagens damanlegg må dimensjoneres opp i forhold til hva konstruksjonene er beregnet for. Demninger og oppdemmingsanlegg kan særlig skades i flomsituasjoner. Det er også forventet en større fare for skade på tekniske installasjoner på grunn av periodevis overbelastning. Ved ekstremnedbør kan det oppstå forurensningssituasjoner for vannforsyningen. Avløpssystemet er mange steder ikke dimensjonert til å ta unna de kraftige regnskyllene vi har opplevd de senere årene, med den konsekvens at avløpsvannet strømmer tilbake inn i bygninger og forårsaker skader. Langvarig kulde med dyptgående tele i bakken kan føre til frost i vann- og avløpsledninger i områder der vannet periodisk blir stående stille i ledningene.

---

[5] RegClim er kortnavnet på et koordinert forskningsprosjekt for utvikling av scenarier for klimautviklingen i Norden.

[6] Rapport fra en tverretatlig arbeidsgruppe 2002. *NTP 2006-2015. Strategiske analyser. Virkninger av klimaendringer for transportsektoren - forstudie.* Jernbaneverket, Kystverket, Luftfartsverket, Statens vegvesen.

Økt lavtrykksaktivitet kan føre til mer og kraftigere tordenvær som også kan føre til strømutfall og derved stoppe strømforsyningen og/eller ødelegge elektroniske komponenter.

Videre ventes det utfordringer på grunn av raske temperaturvekslinger vinterstid. Strømledninger har blitt islagt og har medført ledningsbrudd og brudd i stømforsyningen. Nedfrysing og istapper om vinteren medfører også mer krevende vedlikehold.

Når det gjelder klimasårbarhet i forhold til bebyggelse og tekniske anlegg, er det to viktige forhold som spiller inn. Det ene er lokaliseringen av bebyggelsen i områder utsatt for virkninger av klimaendringer, og det andre er selve utformingen av bebyggelsen.

Samferdselssektoren vurderes som spesielt sårbar i forhold til de klimaendringer som ventes i årene fremover i forhold til forekomsten og styrken i ekstremværet. Dette vil vedrøre den løpende driften samt vedlikehold og beredskap i forhold til eksisterende infrastruktur. Høsten og vinteren 2004 samt høsten 2005 var store deler av Vestlandskysten utsatt for utfordringer med ekstreme nedbørsmengder, flomhendelser og ras som satte både beredskap og samferdsel på prøve. Samfunnet er avhengig av at infrastruktur som veger, baner og kaianlegg er tilgjengelige og uten fare for liv og helse.

Valg som gjøres i dag for investering i veger, bygninger og tekniske anlegg, vil påvirke hvilke effekter klimaendringer kan få for vår infrastruktur i lang tid fremover. Planlegger vi for fremtidige endringer i klimaet, kan vi tilpasse oss de ekstreme værsituasjonene som følger av endringene.

4.2.2 Aldring i kritisk infrastruktur

Vedlikehold og utskifting av materiell er en særlig utfordring ved kapitalintensive og til dels vanskelig tilgjengelige infrastrukturer. Utfordringene øker ved forhold som nye eierskaps- og organisasjonsformer, nye brukerforventninger og teknologiske og kompetansemessige generasjonsskifter. Utfordringene er tydelige i to infrastrukturer, nemlig transportnettverk i kraft- og vannforsyning.

Kraft

Det er blitt hevdet at kraftnettets evne til å motstå store påkjenninger er i ferd med å svekkes. [7] Svekkelser vil kunne skyldes effektivisering og økende belastning uten at nettet bygges ut. Forhold som endret drift og reduksjon i vedlikehold spiller også inn. Direktoratet for samfunnssikkerhet og beredskap stiller spørsmål om det er kommet til et skjæringspunkt mellom effektiv bruk av infrastrukturen og driftssikkerheten. På bakgrunn av direktoratets egne tilsynserfaringer synes dette punktet å ha blitt passert i enkelte tilfeller.

Det har vært en betydelig nedbemanning og omstrukturering i nettvirksomhet de siste 10-15 årene. Aldring av kompetansen er fra bransjehold beskrevet som betydelig, og antall personer med lokalkunnskap har gått ned. Storskala nettforvaltning har medført at tjenester i større grad er satt ut, og det er blitt mindre nærhet til egen infrastruktur. Utviklingen har ført til en svekket kompetanse, noe som kan utgjøre en utfordring ved kriser hvor manglende kompetanse og lokalkunnskap kan utgjøre hindre for en raskest mulig reetablering.

Vann og avløp

Det er en utfordring for vann- og avløpssektoren at økende alder på ledningsnettet fører til tæring/korrosjon, begroing og mekaniske belastninger som gir forvitring og økte driftsproblemer i form av blant annet lekkasjer, ledningsbrudd og risiko for redusert vannkvalitet. Beregninger utført av SSB viser at gjennomsnittlig årlig fornyelsestakt for det kommunale ledningsnettet var på 0,48 % og 0,56 % for henholdsvis vannledningsnettet og avløpsledningsnettet i perioden 2002-2004. Det tilsvarer en nødvendig levetid for ledningsnettet på henholdsvis 210 og 180 år, forutsatt samme utskiftningstakt fremover.[8] Erfaringer med eksisterende ledningsnett tilsier at det vil ha atskillig kortere levetid enn 200 år. En god del av ledningsnettet vil dessuten måtte skiftes ut etter bare få tiår, blant annet som følge av for dårlige materialkvaliteter og for dårlig arbeidsutførelse en del steder.

En annen utfordring er at bransjen generelt, og spesielt de mindre kommunene, sliter med rekrutteringen. Med store pensjonskull i vente de neste 5-15 årene, står man om kort tid overfor store utfordringer, da det samtidig har vært en markert nedgang i antall nyutdannede med VA-kompetanse.[9] Ved mindre vann- og avløpsverk vil det ofte være et problem å ha fagmiljøer med tilstrekkelig kompetanse for å oppfylle de stadig skjerpede krav

---

[7] Direktoratet for samfunnssikkerhet og beredskap tar opp aldring i kritisk infrastruktur i DSB-rapport 2006. *Nasjonal sårbarhets- og beredskapsrapport 2005. NSBR-05. Håndtering av store hendelser og potensiell aldring i kritiske infrastrukturer.* Direktoratet for samfunnssikkerhet og beredskap (DSB). Internettutgaven.

[8] Statistisk sentralbyrå 2005. *KOSTRA: Kommunal avløpsstatistikk 2004;* Statistisk sentralbyrå 2005. *KOSTRA: Kommunal vannforsyning 2004.*

[9] NORVAR-notat 2001. *Undersøkelse om rekruttering til VA-bransjen.*

til tjenestekvalitet som stilles i regelverket. Samtidig er FoU-nivået innen VA-sektoren på et svært lavt nivå, sammenliknet med de fleste andre infrastruktursektorer.

4.2.3 Terrorisme og organisert kriminalitet

Terrorisme

Terrorangrepene i Madrid 2004 og London 2005 viste at europeiske land er mål for islamistisk terrorisme. Også flere planlagte terroraksjoner er avverget de siste årene i Europa. Norske interesser er berørt på ulike måter. Trusler fra al-Qaidas nestleder Ayman al-Zawahiri i mai 2003 og oktober 2004 rettet seg blant annet mot norske interesser, og flere norske ambassader har vært midlertidig stengt etter terrortrusler de to siste årene. Likeledes oppholder personer med tilknytning til islamistiske terrornettverk i utlandet seg i Norge. Slike og lignende forhold gjør at terrortrusselen mot Norge vurderes som moderat av PST.

Fremveksten av internasjonal terrorisme reiser spørsmålet om kritisk infrastruktur og kritiske samfunnsfunksjoner er mål for terroraksjoner. Hvis et sårbarhetsperspektiv legges til grunn, er potensialet for alvorlige konsekvenser stort. I følge NUPI kan de viktigste potensielle og sårbare mål for terrorisme og sabotasje deles inn i:[10]

- Energiproduksjon, herunder olje- og gassutvinning og elektrisk kraft.
- Samferdsel
- Informasjons- og kommunikasjonsteknologi
- Kontroversielle næringer og aktiviteter
- Symbolobjekter og -personer
- Utenlandske mål i Norge

Kritisk infrastruktur og kritiske samfunnsfunksjoner er hovedsakelig interessante mål for internasjonale terrorgrupper i den grad aksjoner mot denne type mål kan føre til massedrap. Kjemisk industri, transport av farlig gods og lignende er teoretisk sett potensielle massedrapsarenaer, men tog, buss, undergrunnsstasjoner, tunneler og lignende er enklere og langt mer tilgjengelige arenaer for massedrapsterror.

På bakgrunn av erfaringer med terrorhendelser i utlandet de senere år, skiller nettopp offentlig transport seg ut som terrormål.[11] Ved å ramme steder med mange mennesker oppnår terrorister medieoppmerksomhet. Knutepunkter for offentlig transport er slike steder.

Det norske samfunnet er sårbart for bortfall av kritisk infrastruktur og kritiske samfunnsfunksjoner. Med riktig kompetanse kan det også være lett å ramme kritisk infrastruktur og kritiske samfunnsfunksjoner. Konsekvensene ved bortfall er så store at ulike forebyggings- og beredskapstiltak fremstår som viktige, også i forhold til terrorhandlinger mot alle typer av kritisk infrastruktur og kritiske samfunnsfunksjoner.

Organisert kriminalitet

Organisert kriminalitet fremstår ikke som noen spesiell utfordring for funksjonsdyktigheten til kritisk infrastruktur og kritiske samfunnsfunksjoner. Det er likevel enkelte hendelser som kan gi utilsiktede effekter på enkelte kritiske samfunnsfunksjoner. Eksempelvis kan store mengder med kredittkortnumre på avveie svekke tilliten til bruk av korttjenester. Det kan igjen føre til større bruk av kontanter og en mindre fleksibel finansiell infrastruktur. Ransbølgen i Sverige i 2005, hvor et større antall pengetransporter ble rammet, så en periode ut til å stoppe vaktselskapers villighet til å transportere sedler og mynter. Det kunne få som konsekvens at flyten av sedler og mynter stoppet opp.

Selv om organisert kriminalitet ikke fremstår som noen spesiell utfordring for funksjonsdyktigheten, representerer organiserte kriminelles økende bruk av elektronisk kommunikasjon en ny og spesiell sikkerhetsutfordring. Det er registrert et økende antall økonomisk motiverte angrep på datanettverk og systemer, og i flere tilfeller har etterforskning avdekket at organiserte kriminelle miljøer står bak. Utpressingsscenarier, der organiserte kriminelle grupperinger truer med angrep på samfunnskritiske funksjoner for å få utbetalt større pengesummer, kan heller ikke avvises.

4.2.4 Omorganisering, omregulering og bortsetting

Virksomheter med sikkerhets- og beredskapsoppgaver omorganiseres og omreguleres. Det gjelder

[10] Arnesen, Signe Astrup. Bjørgo, Tore. Mærli, Morten Bremer 2004 *Hva gjør Norge utsatt for terrorisme? Trusselscenarier og norsk sårbarhetsforvaltning.* Underlag til Nasjonal sårbarhets- og beredskapsrapport, Direktoratet for samfunnssikkerhet og beredskap (DSB). NUPI.

[11] Forsvarets forskningsinstitutt har utgitt en rekke rapporter om kritisk infrastruktur som terrormål. Se for eksempel Lia, Brynjar 2004. *Nye aksjonsformar i internasjonal terrorisme: Konsekvensar for norsk samfunnstryggleik.* Innspel til Nasjonal sårbarhets- og beredskapsrapport, Direktoratet for samfunnssikkerhet og beredskap (DSB) 2004. Forsvarets forskningssinstitutt; Lia, Brynjar og Nesser, Petter 2005. *Terror mot jarnvegar: Eit oversyn over typiske terroraksjonar mot togpassasjertransport.* Forsvarets forskningsinstitutt. FFI Rapport-2005/01451.

også virksomheter som på grunn av deres kritiske funksjon kan sies å ha betydning for rikets sikkerhet og vitale nasjonale interesser. Det må sies å være en sikkerhetsutfordring at hensynet til forretningsmessig drift kan komme i konflikt med hensynet til sikkerhet og beredskap. Overfor disse virksomhetene er det behov for å sikre at sikkerhets- og beredskapsoppgavene ivaretas på en hensiktsmessig måte. Det kan gjøres gjennom ulike virkemidler. Likevel er det usikkerhet knyttet til hvorvidt bruk av disse virkemidlene er tilstrekkelig for å oppnå ønsket målsetning. Eksempelvis kan det hevdes at det kun er eier som har tilstrekkelig nærhet til å avdekke skjulte svakheter, ikke et eksternt tilsynsorgan. På den annen side kan det hevdes at en omreguleringsprosess vil tydeliggjøre myndighetenes krav om sikkerhet og beredskap. En slik tydeliggjøring sammen med gode tilsynsrutiner kan legge grunnlaget for at hensynet til sikkerhet og beredskap blir godt ivaretatt. Det er også en utfordring at utviklingen går så hurtig at myndighetsorganer blir hengende etter både organisatorisk og i forhold til lovgivningen. Ved slike anledninger handler det ofte om manglende evne til å kommunisere et samfunnsansvar overfor virksomheter hvis fremste prioritet er å sikre avkastning.

Inn i dette bildet kommer også utfordringene knyttet til bortsetting. Hensikten med bortsetting er å fokusere på egne kjerneområder i en virksomhet ved å sette ut aktiviteter som er definert som perifere. Det kan være drifting av IKT-systemer, vedlikehold, regnskap osv. Som resultat kan driften bli mer kostnadseffektiv, men samtidig gjør virksomheten seg avhengig av andre tjenesteleverandører som er sentrale for opprettholdelse av egen drift. Manglende forståelse og nærhet til driftskritiske løsninger i egen virksomhet kan derfor skape en sårbarhet overfor uforutsette hendelser. I slike tilfeller kan det tenkes at det kun er eksterne tilsynsorganer som evner å avdekke sikkerhetsutfordringer. Bildet kompliseres ytterligere ved at sentrale tjenester bortsettes uavhengig av geografi, og det kan derfor oppstå situasjoner hvor nasjonal kontroll med kritisk infrastruktur og kritiske samfunnsfunksjoner begrenses av andre lands prioriteringer.

Et annet trekk i denne sammenheng er at eierstrukturen i selskaper kan fremstå med uklar nasjonalitet og at eierkonstellasjoner i prinsippet kan endres raskt. Det kan reises spørsmål om utenlandsk eierskap vil ivareta norske interesser ved store uforutsette hendelser. Sikkerhet og beredskap er i stor grad regulert ved nasjonal lovgivning.[12] Plassering av driftsentraler og hovedkontorer utenlands vil i sterk grad redusere norske myndigheters muligheter til å prioritere norske interesser. Funksjonsdyktigheten til virksomheten vil være prisgitt andre lands innretting og prioritering av sikkerhets- og beredskapsarbeidet. Utenlandsk eierskap kan også medføre at teknisk kompetanse flyttes utenlands av hensyn til lønnsomhet. Evnen til nasjonal skadeoppretting og prioritering vil da reduseres.

4.2.5 Globalisering

Felles for det som er tatt opp i det foregående er at det har trekk koblet til globalisering. Globaliseringen kan sies å gi en rekke fordeler som blant annet økt velferd og et større kulturelt mangfold, men det åpner samtidig opp for økt sårbarhet. Norsk produksjon og tjenesteyting blir i økende grad vevd sammen med og avhengig av resten av verden. Avhengigheter går også den andre veien, særlig i form av til andre lands avhengighet av vår olje- og gassproduksjon. Produksjonsstopp i Norge betyr stopp i leveransene til mottagerland. Globalisering gjør oss dermed ikke bare potensielt mer sårbar, den bidrar også til andres sårbarhet. Et nytt trekk de senere år finner vi i koblingen mellom globalisering og avanserte IKT-løsninger. Kritiske samfunnsfunksjoner kan nå i økende grad bli kontrollert av driftssentraler utenfor landets grenser. Dette gjelder særlig på finans, tele- og energisektoren, men også til en viss grad transportsektoren.

4.2.6 Elektronisk kommunikasjon

Teknologiutvikling innenfor elektronisk kommunikasjon er en sentral del av samfunns- og velstandsutviklingen. Samtidig stiller den samfunnet overfor et sett med nye sikkerhetsutfordringer. Det skyldes at befolkningens velferd i økende grad er avhengig av elektroniske kommunikasjonsløsninger som er koblet sammen i nettverk. På de fleste sektorer bryter kritiske samfunnsfunksjoner sammen uten tilgjengelighet til elektronisk kommunikasjon. Skadepotensialet er derfor særdeles høyt.

Ny bruk av elektronisk kommunikasjon legger blant annet til rette for å effektivisere drift ved å sentralisere tjenester. Dette gir samtidig enkeltpersoner store muligheter til å forårsake skade, enten den er tilsiktet eller utilsiktet. Teknologien muliggjør på mange måter at «liten tue kan velte stort lass», også innenfor kritisk infrastruktur og kri-

[12] Det finnes eksempler på områder som reguleres gjennom internasjonalt regelverk, eksempelvis skips- havne- og flysikkerhet.

tiske samfunnsfunksjoner. Det er dermed en utfordring at mulighet til å forårsake sårbarhet utvikler seg bort fra systemnivå ned til individnivå. Det setter ekstra krav til opplæring, kontroll med tilgang og håndtering av innsideproblematikk.

Innenfor kritiske samfunnsfunksjoner vokser også utfordringene etter hvert som prosesser som tidligere ble kontrollert innenfor lukkede systemer, i økende grad kobles til Internett. Et eksempel er styrings- og prosessystemer som blir koblet opp mot administrative systemer, som igjen blir koblet opp mot Internett for å imøtekomme publikums behov for informasjon. Det er også økende bruk av teknologiske løsninger hvor eksempelvis driftspersonale plassert utenfor eget nettverk har behov for å knytte seg direkte opp mot egne prosessystemer, og hvor Internett er koblingen mellom bruker og det interne nettverket. Denne utviklingen kommer hovedsakelig som et resultat av krav til økt effektivitet og fleksibilitet.

4.2.6.1 Angrep på datanettverk

Det har hittil ikke vært påvist noe koordinert eller vidtrekkende nettverksangrep som har truet samfunnets funksjonsdyktighet. Likevel kan det ikke avvises at det økende antall av tilsynelatende tilfeldige nettverksangrep i noen tilfeller er initiert av terrorgrupper.

Det er ulike synspunkter på hvilken effekt nettverksangrep vil ha på kritisk infrastruktur og kritiske samfunnsfunksjoner. Noen mener at koordinerte nettverksangrep kan bli benyttet for å forsterke effekten av konvensjonelle angrep. Andre er mer usikre på hvor ødeleggende effekten vil kunne bli av direkte angrep. Mens enkelte mener at virkningene kan slå alvorlig ut i økonomien, mener andre at de forskjellige systemene allerede er svært robuste og at gjenoppretting etter et angrep vil kunne gå relativt raskt slik at katastrofale effekter unngås.

Uoppdagede sårbarheter vil til enhver tid utgjøre en trussel, avhengig av hvem som oppdager sårbarhetene og dermed muligheten til å utnytte dem. Man kan tenke seg en meget alvorlig situasjon dersom noen finner en alvorlig sårbarhet og i tillegg gjør en grundig planlegging av hvordan den skal utnyttes før den oppdages og korrigeres. (Et såkalt *Zero-Day Attack*.)

Hvor reell er trusselen om nettverksterrorisme?

I utgangspunktet er det viktig å skille mellom «nettverksangrep» og «nettverksterrorisme». Det første begrepet omhandler alle logiske angrep, så vel store som små, som kan rette seg mot enkeltmaskiner hos privatpersoner eller bedrifters informasjonssystemer. Nettverksterrorisme defineres som omfattende logiske angrep som fører til omfattende skadevirkninger. Selv om hackeres aktiviteter på nettet kan føre til omfattende skadevirkninger, ville det ikke være riktig å sette alle hackere i samme kategori som terrorister.

Det har så langt vært vanskelig å forestille seg at kritiske samfunnsfunksjoner som vannforsyning, strømforsyning, kraftforsyning og lignende kan rammes katastrofalt på grunn av terror i form av logisk angrep fra utsiden alene, uten at det også er etablert noen form for støttespillere på innsiden. På grunn av den allerede innebygde sikkerheten, er et fullstendig fjernstyrt terrorangrep med katastrofale konsekvenser mindre sannsynlig. Ikke desto mindre skal man være oppmerksom på de stadig sterkere koblingene som skjer mellom prosessystemer og Internett.

Det er i prinsippet mulig å trenge seg ulovlig inn i IT-systemer som fjernstyrer kritisk infrastruktur og kritiske samfunnsfunksjoner, men det er ikke uten videre enkelt å skulle overta styringen uten at dette oppdages av det ordinære driftspersonellet. Det er en utbredt oppfatning at det er enklere å bruke eksplosiver for å skade kritisk infrastruktur og kritiske samfunnsfunksjoner, enn å ta kontrollen over et datastyringssystem.

Den største trusselen ved nettverksangrep oppstår når det logiske angrepet kombineres med fysiske midler. Logisk angrep som forhindrer planlagt respons og andre nødtiltak, saboterer transportstyringssystemer eller telekommunikasjon med hjelp av innsidere kan mangedoble effekten av et vel planlagt angrep.

Kanskje er det i særdeleshet små og mellomstore bedrifter (i tillegg til privatpersoner) som er mest utsatt ved at de ikke har tilstrekkelig kompetanse og økonomiske midler til å skaffe seg tilfredsstillende beskyttelse. Selv om de ikke er utpekte mål for spesielle angrep, vil mange av dem før eller senere kunne bli offer for ett av de utallige angrepene som settes ut i livet uten noen bestemt adresse. Likevel kan målrettede angrep mot større aktører – der angriperen har et klart definert mål, er tålmodig og gjennom systematisk og grundig arbeid angriper systemene uten å bli oppdaget for det er for sent – utgjøre den største trusselen.

Per i dag viser islamistiske terrorgrupperinger stor oppfinnsomhet med å bruke IKT-systemer som en informasjonsplattform, mens de så langt ikke har vist samme oppfinnsomhet med å bruke IKT-systemer som en våpenplattform. Selv om terrorgrupperinger i dag trolig mangler kompetanse til å utføre nettverksterrorisme, må det tas høyde

for at disse miljøene raskt kan opparbeide nødvendig kompetanse. En mer inngående vurdering av trusselen fra terrorgrupper må innbefatte konkrete vurderinger av intensjon og kapasitet hos bestemte, identifiserte grupperinger. Dette forutsetter etterretningsinformasjon som er sikkerhetsgradert.

Den raske utviklingen i nettverksangrep fra så vel organiserte kriminelle som andre grupper, gjør at myndigheter må ta på alvor behovet for å beskytte kritisk infrastruktur og kritiske samfunnsfunksjoner på døgnkontinuerlig basis. Et tiltak som allerede er iverksatt er opprettelsen av NorCERT[13].

4.2.7 Etterretningsvirksomhet

Flere stater utfører etterretningsvirksomhet i og mot Norge. Målet for den ulovlige etterretningsvirksomheten er innhenting av informasjon som ikke er åpent tilgjengelig eller som på en eller annen måte er beskyttet.[14] Mens kompromittering av skjermingsverdig informasjon kan være straffbar i henhold til norsk lov, er det nyttiggjøringen av denne informasjonen som vil være utslagsgivende med tanke på skadevirkninger for Norge og norske interesser.

I tillegg til etterretning mot og påvirkning av det politiske miljøet, foregår det også etterretning mot deler av næringslivet. For norske bedrifter vil slik etterretningsvirksomhet kunne føre til svekket konkurranseevne, reduserte markedsandeler og dermed tap av inntekter og arbeidsplasser. Etterretningsvirksomhet kan også føre til kompromittering av militær og annen sensitiv informasjon.

Skadevirkninger av spionasje rettet mot for eksempel sikkerhetspolitiske vurderinger og forsvarshemmeligheter, kan innebære en svekkelse av norsk strategisk evne til å møte endringer i risikobildet. Samfunnssikkerheten i Norge kan også trues dersom detaljert informasjon om beredskapsplaner og sårbarhet i kritisk infrastruktur kommer på avveie.

Den utstrakte bruken av IKT-systemer som er koblet til Internett fremstår som en ny utfordring i etterretningssammenheng. Informasjon som tidligere var lagret på papir og på enkeltstående datamaskiner, har med fremveksten av Internett et større potensial for å bli kompromittert.

[13] CERT: *Computer Emergency Response Team*

[14] Politiets sikkerhetstjeneste peker på at flere stater utfører etterretningsvirksomhet med fordekte midler i og mot Norge. Politiets sikkerhetstjeneste (PST) 2005. *Politiets sikkerhetstjenestes ugraderte trusselvurdering 2005*.

4.2.8 Gjensidige avhengigheter

En viktig del av sikkerhetsutfordringene utgjøres av den til dels uforutsigbare gjensidige avhengigheten på tvers av ulike infrastrukturer. Moderne samfunnsdrift støtter seg i stadig større grad på noen sentrale funksjoner som blir stadig mer avhengige av hverandre. Ved at kritiske tjenester settes ut til underleverandører, vokser dette frem som en stadig viktigere del av kritisk infrastruktur. Dette gjelder særlig innen elektronisk kommunikasjon, men også på andre områder som for eksempel strømforsyning. Alvorlige forstyrrelser i én funksjon kan derfor gi omfattende ringvirkninger gjennom forstyrrelser i mange andre tilknyttede funksjoner.

Det foreligger en del forsknings- og utredningsmateriale på gjensidige avhengigheter mellom kritisk infrastruktur og kritiske samfunnsfunksjoner, men nøyaktig hvordan de gjensidige avhengighetene påvirker utfallet av større sammenbrudd er vanskelig å forutsi.[15] Høy grad av kompleksitet tilsier at nytteeffekten av slike analyser er størst når de utføres på mindre og avgrensede objekter og systemer. For eksempel vil analyser av punkter i elektroniske overføringsnett og punkter i strømnettet kunne avdekke behov for tiltak som reduserer sårbarhet som følge av gjensidige avhengigheter dem i mellom.

4.3 Sentrale aktører og deres rapportering om sikkerhetsutfordringene

Politiets sikkerhetstjenestes ansvarsområde

De gjøremål som utføres av Politiets sikkerhetstjeneste (PST) reguleres av lov av 4. august 1995 nr. 53 om politiet (politiloven) § 17 a-c. PSTs ansvar for å utarbeide trusselvurderinger fremgår av § 17 c, nr. 1.

PSTs trusselvurderinger omhandler informasjon som tar sikte på å forebygge og avverge alvorlige kriminelle handlinger, herunder terrorisme, sabotasje, ulovlig etterretningsvirksomhet, brudd på reglene om spredning av masseødeleggelsesvåpen, mv. PST utarbeider både faste årlige trusselvurderinger og hendelsesstyrte trusselvurderinger, blant annet knyttet til alvorlige situasjoner som inntreffer i utlandet.

[15] For FFIs tilnærming, se Hæsken, Ole Morten. Olsen, Thor Gunnar. Fridheim, Håvard. *Beskyttelse av samfunnet (BAS) – Sluttrapport.* Forsvarets forskningsinstitutt. FFI/Rapport-97/01459; For en illustrasjon på den nederlandske fremgangsmåten, se Ministry of the Interior and Kingdom Relations 2003. *Critical Infrastructure Protection in The Netherlands. The Netherlands,* side 15-17.

Trusselvurderingene beskriver gjeldende trusselsituasjon ved blant annet å redegjøre for hvem eller hva som utgjør en trussel, bakgrunnen for trusselen, sannsynligheten for at den skal materialisere seg, mv. Trusselvurderingene kan også inneholde PSTs anbefalinger om tiltak for å ivareta sikkerheten til Norge og norske interesser. PST har ikke myndighet til å instruere virksomheter om hvilke sikkerhetstiltak som skal gjennomføres. Det er således den enkelte virksomhet som har et selvstendig ansvar for å følge opp eventuelle anbefalinger om tiltak. Trusselvurderingene er et helt sentralt grunnlag for virksomheters vurderinger av hvilke sikkerhetstiltak som skal iverksettes for å hindre at en trussel materialiserer seg.

Det påpekes at PSTs trusselvurderinger ikke bare er til bruk for politiske myndigheter. Vurderingene vil også kunne omhandle anbefalinger om sikkerhetstiltak i private virksomheter, og således være et sentralt grunnlag for sikkerhetsarbeidet i privat sektor.

Nasjonal sikkerhetsmyndighets ansvarsområde

Nasjonal sikkerhetsmyndighets (NSMs) hovedansvar og oppgaver reguleres av lov av 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven) med tilhørende forskrifter. Forebyggende sikkerhetstjeneste og NSMs ansvarsområde omfatter alle tiltak for å sikre skjermingsverdig informasjon og skjermingsverdige objekter[16] mot sikkerhetstruende virksomhet som spionasje, sabotasje og terrorhandlinger.

NSM skal i henhold til sikkerhetslovens § 8 koordinere de forebyggende sikkerhetstiltak og kontrollere sikkerhetstilstanden. Videre skal NSM i henhold til sikkerhetslovens § 9 innhente og vurdere informasjon av betydning for gjennomføringen av forebyggende sikkerhetstjeneste og gi informasjon, råd og veiledning til virksomheter. Som en oppfølging av oppgavene gitt i medhold av sikkerhetsloven, gir NSM ut en årlig risikovurdering og periodevise sikkerhetsvurderinger til virksomheter som er omfattet av loven. I NSMs vurderinger gis det sikkerhetsfaglige anbefalinger til ansvarlige virksomheter.

NSMs sikkerhetsfaglige anbefalinger tar utgangspunkt i risikoen knyttet til at sikkerhetstruende virksomhet inntreffer (terror, sabotasje og spionasje). NSM kan gi anbefalinger selv om det er lav sannsynlighet for at slike hendelser inntreffer. Anbefalingene gis med bakgrunn i at skadepotensialet ved sikkerhetstruende virksomhet vil være uakseptabelt høyt. NSM baserer dessuten anbefalingene på en vurdering av sikkerhetstilstanden i et lengre tidsperspektiv. NSM har også mulighet til å gi pålegg om sikkerhetstiltak innenfor sikkerhetslovens rammer.

Etterretningstjenestens ansvarsområde

Etterretningstjenesten skal innhente, bearbeide og analysere informasjon på de saksfelt som til enhver tid prioriteres av overordnet politisk og militær myndighet innenfor rammen av Lov av 20 mars 1998 nr. 11 om Etterretningstjenesten. Etterretningstjenestens ansvar og oppgaver er regulert i Instruks om etterretningstjeneste, fastsatt ved kgl. res. av 31. august 2001. I lovens § 3, 1. ledd fremgår det at Etterretningstjenesten skal innhente, bearbeide og analysere informasjon som angår norske interesser sett i forhold til fremmede stater, organisasjoner eller individer, og på denne bakgrunn utarbeide trusselanalyser og etterretningsvurderinger, i den utstrekning det kan bidra til å sikre viktige nasjonale interesser. Oppgavelisten i lovens § 3 er ikke uttømmende. Hva andre viktige nasjonale interesser omfatter, vil avhenge av hvilke sikkerhetsutfordringer Norge til enhver tid stilles overfor. Informasjons fra Etterretningstjenesten er et grunnlag for nasjonale myndigheters avgjørelser knyttet til forebygging og håndtering av sikkerhetspolitiske episoder, kriser og krig.

Koordineringen av etterretnings- og sikkerhetstjenestene

Koordinerings- og rådgivningsutvalget for etterretnings- og sikkerhetstjenestene (KRU) er et samarbeidsorgan for spørsmål som gjelder etterretnings- og sikkerhetstjenestene, og et rådgivningsutvalg for de berørte statsråder. Utvalgets oppgaver er å ivareta overordnet koordinering av Politiets sikkerhetstjenestes, Nasjonal sikkerhetsmyndighets og Etterretningstjenestens arbeidsoppgaver, prioriteringer og mål, samt analysere og utrede felles problemstillinger knyttet til trusselbildet, jf. Instruks for Koordinerings- og rådgivningsutvalget for etterretnings- og sikkerhetstjenestene, fastsatt ved kgl. res. av 20. desember 2002. Utvalget består av 6 faste medlemmer fra hhv. Forsvarsdepartementet, Justis- og politidepartementet, Utenriksdepartementet, sjefen for Etterretningstjenesten, direktøren for Nasjonal sikkerhetsmyndighet og sjefen for Politiets sikkerhetstjeneste. Ledelsen

[16] Skjermingsverdige objekter er definert som «eiendom som må beskyttes mot sikkerhetstruende virksomhet av hensyn til rikets sikkerhet eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser». Dette kan være områder, bygninger, anlegg, eller deler av slik eiendom.

av utvalget alternerer mellom representantene fra Justis- og politidepartementet, Forsvarsdepartementet og Utenriksdepartementet. Det er etablert et fast sekretariat for utvalget med representanter for de tre departementer som skal tilrettelegge for og følge opp saker som behandles i utvalget. Sekretariatsledelsen ivaretas av det departement som til enhver tid innehar ledelsen av utvalget. KRUs ansvar og oppgaver skal ivareta samfunnets evne til å fange opp endringer i trussel- og risikobildet og evne til å iverksette tiltak for å møte nye utfordringer, særlig innenfor samfunnskritiske funksjoner.[17]

Direktoratet for samfunnssikkerhet og beredskaps ansvarsområde

DSB skal være pådriver i arbeidet med å forebygge ulykker, kriser og andre uønskede hendelser. Videre skal DSB sørge for god beredskap og effektiv ulykkes- og krisehåndtering. DSB leder Sivilforsvaret, setter prioriteringer for fylkesmennenes beredskapsarbeid i fylker og kommuner og tilrettelegger planer og øvelser for den nasjonale kriseberedskapen. Direktoratet har det faglige og administrative ansvaret for Nasjonalt utdanningssenter for samfunnssikkerhet og beredskap, Sivilforsvarets beredskaps- og kompetansesentre på Starum, Trondheim, Jæren og Norges Brannskole. DSB er nasjonal fagmyndighet innen brann- og eksplosjonsvern og elsikkerhet, og fører blant annet tilsyn med det kommunale brannvesen, høyspenningsanlegg, elektromedisinsk utstyr, m.m.

Direktoratet for samfunnssikkerhet og beredskap er i instruks (fastsatt ved kgl.res. av 24. juni 2005) blant annet gitt i oppgave å ha oversikt over sårbarhets- og beredskapsutviklingen i samfunnet og ta initiativ for å forebygge hendelser med sikte på å hindre tap av liv, helse, miljø, viktige samfunnsfunksjoner og store materielle verdier, samt å ha et sektorovergripende perspektiv med vekt på store ulykker og ekstraordinære situasjoner.

Som en del av instruksen er DSB gitt i oppdrag å utarbeide en nasjonal sårbarhets- og beredskapsrapport som grunnlag for videre oppfølging av sikkerhets- og beredskapsarbeidet på tvers av sektorer og etatsgrenser. Direktoratet avga sin første rapport i september 2005 til Justis- og politidepartementet, mens den andre kom vinteren 2006. Rapportene inneholder trendanalyser, vurderinger av status innen særskilte områder, og anbefalinger om fremtidige tiltak, herunder planer, forebyggende tiltak, analyser, forskning, mv. Formålet er å dokumentere status for samfunnssikkerhet og beredskap innen særlige områder, og peke på nye sårbarheter som grunnlag for strategiutforming og prioritering av tiltak.

[17] Jf. St.prp. nr. 1 (2004-2005) for Justis- og politidepartementet, s. 135.

Kapittel 5
Ansvar for beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner

5.1 Myndighetsansvar fordelt på sektorer

Ansvaret for beskyttelse av kritisk infrastruktur ligger hos eieren og/eller operatøren. Dette ansvaret er ikke løsrevet fra øvrig ansvar som ligger til en eier og/eller operatør av en virksomhet. På sentralt myndighetsnivå innebærer dette at det enkelte fagdepartement har et overordnet ansvar for å ivareta beskyttelsen av kritisk infrastruktur og kritiske samfunnsfunksjoner innenfor sin sektor. Fagdepartementet kan således på selvstendig grunnlag foreslå statlige virkemidler for beskyttelse av kritisk infrastruktur innenfor sin sektor, herunder regulatoriske virkemidler, økonomiske virkemidler, osv.

De gjensidige avhengighetsforholdene mellom kritiske infrastrukturer gjør det imidlertid nødvendig å sikre en god samordning av virkemiddelbruken på tvers av sektorlinjene. Dette gjelder både nasjonalt og internasjonalt.

Myndighetenes ansvar for beredskap og/eller forebygging i kritisk infrastruktur og kritiske samfunnsfunksjoner kan fremstilles på følgende måte i tabellform:

Tabell 5.1 Myndighetenes ansvar for beredskap og/eller forebygging i kritisk infrastruktur og kritiske samfunnsfunksjoner

Kritisk infrastruktur	Departement	Underliggende etat
Elektrisk kraft	Olje- og energidepartementet	Norges vassdrags- og energidirektorat
	Justis- og politidepartementet	Direktoratet for samfunnssikkerhet og beredskap
Elektronisk kommunikasjon	Sektordepartementene	
	Samferdselsdepartementet	Post- og teletilsynet
	Forsvarsdepartementet	Nasjonal sikkerhetsmyndighet
	Justis- og politidepartementet	Nasjonal sikkerhetsmyndighet
	Fornyings- og administrasjons-departementet	
Transport	Samferdselsdepartementet	Luftfartstilsynet
		Jernbanetilsynet
		Vegdirektoratet
	Nærings- og handelsdepartementet	Sjøfartsdirektoratet
	Fiskeri- og kystdepartementet	Kystdirektoratet/Kystverket
	Justis- og politidepartementet	Direktoratet for samfunnssikkerhet og beredskap (transport av farlig gods)
Olje og gass	Olje- og energidepartementet	Oljedirektoratet
	Arbeids- og inkluderings-departementet	Petroleumstilsynet

Tabell 5.1 Myndighetenes ansvar for beredskap og/eller forebygging i kritisk infrastruktur og kritiske samfunnsfunksjoner

Kritisk infrastruktur	Departement	Underliggende etat
Vann og avløp	Helse- og omsorgsdepartementet	Mattilsynet Sosial- og helsedirektoratet Helsetilsynet Nasjonalt folkehelseinstitutt Kommunene
	Miljøverndepartementet	Statens forurensningstilsyn Fylkesmennene Kommunene
	Olje- og energidepartementet Justis- og politidepartementet	Norges vassdrags- og energidirektorat Direktoratet for samfunnssikkerhet og beredskap
Satellittbasert infrastruktur	Nærings- og handelsdepartementet	Norsk romsenter
Kritiske samfunns-funksjoner	**Departement**	**Underliggende etat**
Bank og finans	Finansdepartementet	Kredittilsynet Norges Bank
Matforsyning	Landbruks- og matdepartementet	Mattilsynet Statens landbruksforvaltning
	Nærings- og handelsdepartementet Fiskeri- og kystdepartementet Helse- og omsorgsdepartementet	Mattilsynet Mattilsynet Sosial- og helsedirektoratet Helsetilsynet Nasjonal folkehelseinstitutt
Helse, sosial og trygde-tjenester	Helse- og omsorgsdepartementet	Helsetilsynet Sosial- og helsedirektoratet Nasjonalt folkehelseinstitutt
	Arbeids- og inkluderingsdepartementet	Sosial- og helsedirektoratet Rikstrygdeverket Arbeids- og velferdsetaten (NAV) - sommeren 2006
Politi	Justis- og politidepartementet	Politidirektoratet
Nød- og redningstjeneste	Justis- og politidepartementet	Politidirektoratet Direktoratet for samfunnssikkerhet og beredskap Hovedredningssentralene Næringslivets sikkerhetsorganisasjon (Industrivern)
	Helse- og omsorgsdepartementet	Sosial- og helsedirektoratet Helsetilsynet Kommunene (Brann- og redningsvesen)

Tabell 5.1 Myndighetenes ansvar for beredskap og/eller forebygging i kritisk infrastruktur og kritiske samfunnsfunksjoner

Kritiske sammfunns-funksjoner	Departement	Underliggende etat
Kriseledelse	Sektordepartementene Statsministerens kontor Justis- og politidepartementet	 Politidirektoratet Direktoratet for samfunnssikkerhet og beredskap Hovedredningssentralene
	Kultur- og kirkedepartementet	NRK
Storting og Regjering	Sektordepartementene Statsministerens kontor Fornyings- og administrasjons-departementet	 Departementenes servicesenter (sentraladministrasjonen) Stortingets administrasjon Riksrevisjonen
Domstolene	Justis- og politidepartementet	Domstoladministrasjonen (Tingretten) (Lagmannsretten) (Høyesterett)[1]
Forsvar	Forsvarsdepartementet	Forsvarets militære organisasjon Forsvarsbygg Nasjonal sikkerhetsmyndighet
Miljøovervåkning	Miljøverndepartementet	Direktoratet for naturforvaltning Statens forurensningstilsyn Riksantikvaren Norsk Polarinstitutt
	Helse- og omsorgsdepartementet	Statens strålevern
	Fiskeri- og kystdepartementet	Kystverket
	Kunnskapsdepartementet	Meterologisk institutt
Renovasjon		Kommunene

[1] Domstolene er ikke underlagt Justis- og politidepartementet, men er tatt med på listen for oversiktens skyld.

I tillegg til den sektorvise fordelingen av ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner, har Justis- og politidepartementet et overordnet samordnings- og tilsynsansvar for samfunnssikkerhet og beredskap. Det innebærer et ansvar for å utarbeide overordnede retningslinjer, koordinere og fremme proposisjoner og meldinger til Stortinget, tilrettelegge rammebetingelser, ta initiativ, være pådriver, avklare ansvarsforhold i gråsoner og treffe prinsipielle avgjørelser på samfunnssikkerhets- og beredskapsområdet.[1]

I det følgende redegjøres det for utviklingen av Justis- og politidepartementets samordningsrolle, samt de sektorovergripende virkemidler for å ivareta beskyttelse av kritisk infrastruktur som ligger til dette departementet.

5.2 Utviklingen av Justis- og politidepartementets samordningsrolle

Ved at ansvarsprinsippet er gjort gjeldende for organiseringen av sikkerhets- og beredskapsarbeidet, vil det være regjeringen som kollegium som sitter med det helhetlige ansvaret for kritisk infrastruktur, samtidig som den enkelte fagstatsråd har ansvaret innenfor sitt myndighetsområde. Ansvaret for kritisk infrastruktur er således ikke skilt ut

[1] St.prp. nr. 1 (2005-2006) for Justis- og politidepartementet.

som et eget fagområde løsrevet fra det øvrige ansvar innenfor en sektor. Det foreligger altså ikke et «helhetsprinsipp» for organiseringen av sikkerhets- og beredskapsarbeidet som innebærer at et departement skal ivareta helheten på tvers av fagdepartementene. Det er imidlertid klart at utviklingen av Justis- og politidepartementets samordningsrolle har vært drevet av et ønske om å ivareta et slikt helhetsprinsipp.

Behovet for et samordningsansvarlig departement ble drøftet av Buvikutvalget i 1992.[2] Utvalget mente et mer effektivt og målrettet sivilt beredskap kunne realiseres gjennom overordnet koordinering av et samordningsansvarlig departement. Flere departementer ble vurdert som mulige samordningsdepartement, herunder Forsvarsdepartementet, det tidligere Nærings- og energidepartementet og Justis- og politidepartementet. Ut fra en samlet vurdering, anbefalte utvalget at Justis- og politidepartementet burde ha det overordnede koordineringsansvar for det sivile beredskap. Dette ble blant annet begrunnet ut fra departementets ansvar for Direktoratet for sivilt beredskap og Redningstjenesten.

På bakgrunn av Buvikutvalgets vurderinger, besluttet Regjeringen at Justis- og politidepartementet skulle gis et koordineringsansvar for det sivile beredskap, jf. St. meld. nr. 48 (1993-94) Langtidsplan for det sivile beredskap og kgl. res. av 16. juni 1994 om Justis- og politidepartementets samordningsfunksjon på beredskapssektoren og om rådet for sivilt beredskap. Formålet med dette var å sikre en balansert og ressurseffektiv sivil beredskap på tvers av sektorer.

Justis- og politidepartementets samordningsansvar endrer ikke på prinsippet om at den myndighet som har ansvaret for en sektor til daglig, også har ansvaret for nødvendige beredskapsforberedelser og iverksettelse av tiltak i en krisesituasjon.

Justis- og politidepartementets rolle slik det fremgår av kgl. res. av 16. juni 1994 er å påse at det samlede sivile beredskap blir ivaretatt på en tilfredsstillende måte. Det fremgår av resolusjonen at:

> Justis- og politidepartementets skal utøve sitt samordningsansvar ved å:
> – vurdere den samlede ressursbruk innen beredskapssektoren, herunder vurdere departementenes årlige beredskapsbudsjetter,
> – fremme forslag overfor de andre departementene med sikte på å oppnå en bedre samordning av ressurser til freds- og krigsformål,
> – utøve målstyring og økonomisk rammekontroll som grunnlag for å påpeke eventuell ubalanse i beredskapsforberedelsene,
> – legge frem langtidsplaner og langtidsbudsjetter for Stortinget,
> – initiere samarbeidet mellom de øvrige departementene,
> – ta initiativ overfor andre departementer til behandling og utredning av beredskapsmessige spørsmål.

Justis- og politidepartementets samordningsansvar iht. kgl. res. av 16. juni 1994 innebærer ansvar for den faglige og økonomiske koordineringen av det sivile beredskap. Rådet for sivilt beredskap ble etablert for å gi råd til Justis- og politidepartementet i dette arbeidet.[3]

Justis- og politidepartementets samordningsansvar ble satt på prøve under flommen på Østlandet i 1995, ved at Justis- og politidepartementet samordnet den sentrale kriseledelse. Under krisen ledet Justis- og politidepartementet en interdepartemental gruppe bestående av 11 departementer og DSB. I St.meld. nr. 37 (1995-1996) Om flommen på Østlandet 1995 og kriseberedskap i fred, ble myndighetenes innsats evaluert. Samordningsgruppen på sentralt nivå ble vurdert å fungere tilfredsstillende, og i meldingen varslet Regjeringen at den ville kunne ta initiativ til en slik gruppe ved senere anledninger. I denne forbindelse ba Stortinget Justis- og politidepartementet vurdere å opprette en permanent samordningsgruppe for fredskriser/katastrofer som ble ledet av Justis- og politidepartementet, jf. Innst. S. nr. 256 (1995-96).

Ønsket om en organisatorisk styrking av Justis- og politidepartementets samordningsansvar ble fulgt opp 1. januar 1996 ved at Justis- og politidepartementets ansvar for Redningstjenesten og det sivile beredskap ble samlet i en egen avdeling; Rednings- og beredskapsavdelingen. Ved opprettelsen av avdelingen fikk departementene, fylkesmennene og de øvrige virksomheter med ansvar innen det sivile beredskap et klart definert punkt for samordning.

I St.meld. nr. 25 (1997-98) Hovedretningslinjer for det sivile beredskaps virksomhet og utvikling i

[2] Utvalg for å utrede organisasjon, mål og metode for det sivile beredskap, ledet av tidligere fylkesmann Martin Buvik. Rapport ble avgitt 1992.

[3] Rådet for sivilt beredskap er et rådgivende organ som skal understøtte utøvelse av Justis- og politidepartementets samordningsansvar. Rådet består av representanter for Justis- og politidepartementet, Statsministerens kontor, Administrasjons- og sosialdepartementet, Finansdepartementet, Forsvarsdepartementet, Kommunal- og regionaldepartementet, Landbruks- og matdepartementet, Nærings- og handelsdepartementet, Samferdselsdepartementet, Helse- og omsorgsdepartementet, Utenriksdepartementet, Direktoratet for samfunnssikkerhet og beredskap, Forsvaret, Fylkesmennene og Kommunenes Sentralforbund. Det fremgår av St.prp. nr. 1 (2004-2005) at rådets sammensetning og funksjon er til vurdering.

tiden 1999-2002, gis en rapportering på oppfølgingen av tidligere langtidsperiode. Videre fremgår det av meldingen at en forsterking av samordningen av beredskapsarbeidet på sentralt, regionalt og lokalt nivå er et satsningsområde.

En konkret styrking av Justis- og politidepartementets samordningsrolle skjedde ved kgl. res. av 3. november 2000 om internkontroll og systemrettet tilsyn med det sivile beredskapsarbeidet i departementene. Formålet med dette tilsynet er å sikre god kvalitet på planleggingen og en målrettet og effektiv bruk av ressursene til beredskapsformål, og dette bygger således opp under formålet med kgl. res. av 16. juni 1994.

Et viktig virkemiddel for å ivareta Justis- og politidepartementets samordningsrolle innen det sivile beredskap, var «programområde 05» i statsbudsjettet. Seks departementer fikk bevilget midler til beredskapstiltak over programområde 05; Justis- og politidepartementet, Kulturdepartementet, Nærings- og handelsdepartementet, Olje- og energidepartementet, Samferdselsdepartementet, Sosial- og helsedepartementet.

Fra og med budsjetterminen 2001 ble programområde 05 Sivilt beredskap avviklet. Formålet med denne endringen var å gjøre beredskapsfeltet mer oversiktlig. Budsjettorganiseringen medførte uklar ansvarsfordeling mellom berørte departementer og ble i tillegg ansett å være administrativ uhensiktsmessig.[4] Justis- og politidepartementet er ikke gitt et nytt virkemiddel for å ivareta sitt ansvar for å «vurdere den samlede ressursbruk innen hele sektoren med sikte på en kostnadseffektiv total beredskap,» jf. kgl. res. av 16. juni 1994.

Sårbarhetsutvalget tok i sin utredning NOU 2000:24 Et sårbart samfunn, på nytt opp spørsmålet om å styrke samordningen av det sivile beredskapsarbeidet. Utvalget fremmet forslag om å realisere faglige og økonomiske synergieffekter ved å slå sammen likeartede funksjoner og rendyrke fagansvaret for sikkerhet og beredskap, herunder ansvaret for nasjonal krisehåndtering, i ett departement. På denne måten mente sårbarhetsutvalget at arbeidet med sikkerhet og beredskap vil fremstå som mer målrettet og bedre samordnet.[5]

Regjeringen Bondevik II gikk inn for å følge opp sårbarhetsutvalgets anbefalinger med nødvendige tiltak og forankre totalansvaret for samfunnets sivile sikkerhet i Justis- og politidepartementet.[6] Regjeringens oppfølging fremgår av St.meld. nr. 17 (2001-2002) Samfunnssikkerhet, og de fleste av de oppgavene som sårbarhetsutvalget mente burde samles i ett departement ligger nå til Justis- og politidepartementet:

- Politidirektoratet
- Politiets sikkerhetstjeneste
- Direktoratet for samfunnssikkerhet og beredskap (det tidligere Direktoratet for sivilt beredskap og det tidligere Direktoratet for brann- og elsikkerhet)
- Nasjonal sikkerhetsmyndighet (sivil sektor)
- Hovedredningssentralene
- Fylkesmennenes beredskapsarbeid.

Iht. Kronprinsregentens resolusjon av 4. juli 2003 om fordeling av ansvar for forebyggende sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet, har Justis- og politidepartementet et overordnet ansvar for den forebyggende sikkerhetstjeneste i sivil sektor. NSM er administrativt underlagt Forsvarsdepartementet, men har en faglig rapporteringslinje til Justis- og politidepartementet i sivil sektor. Den forebyggende sikkerhetstjeneste omfatter i Norge alle tiltak for å sikre skjermingsverdig informasjon og objekter mot sikkerhetstruende virksomhet; terrorisme, sabotasje og spionasje.

Kgl. res. av 24. juni 2005[7] fastsetter instruks for Direktoratet for samfunnssikkerhet og beredskap. Instruksen setter rammene for DSBs arbeid med koordineringsoppgaver som gjøres for å understøtte Justis- og politidepartementet i dets koordineringsrolle innenfor arbeidet med samfunnssikkerhet og beredskap. Instruksen viderefører også det koordinerings- og tilsynsansvar som DSB har iht. oppfølging av storulykkesforskriften. Videre er DSB gitt et eksplisitt koordineringsansvar for oppfølging av og tilsyn med aktiviteter, objekter og virksomheter med potensial for store ulykker. Resolusjonen tydeliggjør DSBs ansvar for å ha en god oversikt over sårbarhets- og beredskapsutviklingen i samfunnet på tvers av sektorene, samt å være en pådriver i arbeidet for å forebygge ulykker, kriser og andre uønskede hendelser.

5.3 Privat sektors samfunnsansvar

Å ivareta befolkningens trygghet er blant statens viktigste oppgaver. Sikker leveranse av kritiske

[4] St.prp. nr. 1 (2000-2001).
[5] Ref. Kåre Willoch
[6] Sem-erklæringen
[7] Direktoratet for samfunnssikkerhet og beredskap – det generelle koordineringsansvar og ansvaret for koordinering av tilsyn med aktiviteter, objekter og virksomhet med potensial for store ulykker.

varer og tjenester som kraft, tele, vann, mv. er av stor betydning for befolkningen, og det er et viktig mål for staten at samfunnet skal fungere mest mulig normalt under alle forhold. Det er derfor et statlig ansvar å fastsette ambisjonsnivået hva gjelder sikker leveranse av kritiske varer og tjenester.

En økende del av kritisk infrastruktur og kritiske samfunnsfunksjoner er overlatt til kommersielle aktører å forvalte. Dette løsriver ikke staten fra ansvar for tap ved svikt i leveransene av de kritiske varene og tjenestene, da det i befolkningen er en forventning om at staten ivaretar samfunnets sikkerhet og beredskap på en tilfredsstillende måte gjennom de styringsvirkemidler den har til rådighet. Imidlertid er det i dagens globaliserte og markedsorienterte samfunn begrensninger i statens styringsmuligheter, og staten er i økende grad avhengig av at næringslivet selv ivaretar sitt samfunnsansvar.

5.3.1 Ivaretakelse av samfunnsansvar

Næringslivets hovedoppgave er å skape verdier og økonomiske resultater. Samtidig har næringslivet et samfunnsansvar. Bedriftene virker ikke bare i et marked. De har også en rolle i en bredere samfunnsmessig sammenheng.

Det er derfor grunn til å gå nærmere inn på spørsmålet om det kan forventes av en virksomhet at den frivillig ivaretar et ansvar for samfunnet rundt seg, uten at dette følger som et resultat av statlige styringsvirkemidler.

Næringslivets samfunnsansvar er grundig berørt i flere utredninger den senere tid.[8] Begrepet er en oversettelse av det engelske begrepet «corporate social responsibility». Bedrifters samfunnsansvar innebærer at bedrifter frivillig etablerer målsetninger eller definerer standarder for egen forretningsvirksomhet som ikke er resultat av statlige styringsvirkemidler. Et viktig incentiv for næringslivet til å nedlegge arbeid i dette, er hvilken oppmerksomhet et frivillig initiativ får. Hensynet til lokalsamfunn, ansatte, miljø og menneskerettigheter settes i økende grad på alle bedrifters dagsorden.

Hensynet til å ivareta et godt omdømme blant kunder og investorer, som er opptatt av samfunnsansvar kan være et incitament. Det samme vil ytre press fra andre interessenter, som organisasjoner eller media være.

Diskusjonen om hva som ligger i samfunnsansvar har til nå i stor grad vært fokusert rundt temaer som:

- uskrevne regler innenfor etisk næringsvirksomhet
- norske bedrifters etablering i andre land
- menneskerettigheter
- miljøengasjement
- at bedriftenes samfunnsansvar skal være av frivillig karakter

Derimot har diskusjonen omkring samfunnsansvar i stor grad vært fraværende i sammenheng med sikkerhet og beredskap i kritisk infrastruktur og kritiske samfunnsfunksjoner.

Dette kan ha sin årsak i at sikkerhet og beredskap er sterkt regulert i lover og forskrifter, med en rekke tilsynsorganer som kontrollerer at regelverket overholdes. En uheldig side ved dette kan være at de potensielle gevinster ved å etablere sikkerhet og beredskap utover det som kreves, blir lite synlige for en virksomhet i det daglige. Manglende sikkerhet og beredskap kan være forholdsvis lett å skjule. Dette stiller seg imidlertid annerledes dersom virksomheten utsettes for alvorlige påkjenninger. I en slik situasjon vil måten en virksomhet håndterer en alvorlig hendelse og hvor raskt situasjonen normaliseres etter et driftsavbrudd, være av avgjørende betydning i et konkurransemarkedet. Dette gjelder særlig dersom hendelsen får alvorlige konsekvenser for kunder som er kritisk avhengig av stabil leveranse av varer og tjenester. Virksomheten kan risikere at markedet vil straffe den gjennom krav om dekning av tap, eller etterspørre varer og tjenester fra andre leverandører som fremstår som mer pålitelige.

Samfunnssikkerhet sett i et bredt perspektiv vil omfatte samfunnets evne til å opprettholde tilnærmet normal funksjonalitet uansett påkjenning. Det kan for eksempel tenkes situasjoner med knapphet på kritiske varer og tjenester, med et påfølgende behov for fordeling basert på prioriteringer. I slike situasjoner vil også privat sektor ha et ansvar for at prioriteringene er til beste for samfunnet som helhet. I denne forbindelse påpekes for øvrig at den globaliserte økonomien kan være en viktig forutsetning for å sikre nødvendig tilgang på kritiske varer og tjenester.

Det kan oppstå interessekonflikter mellom myndighetene og næringslivet i de tilfeller hvor næringslivet prioriterer annerledes, eller ikke ser nytten eller behovet for særskilte tiltak for å ivareta

[8] Se blant annet St.meld. nr. 22 (2001-2002) *Et mindre og bedre statlig eierskap*; St.meld. nr. 19 (2002-2003) *En verden av muligheter - globaliseringens tidsalder og dens utfordringer*; NOU 2004:7 *Det direkte statlige eierskap i Norge – omfang og mål*; Utenriksdepartementets hjemmesider, *Økonomi og arbeidsliv* (odin.dep.no/ud/norsk/publ/rapporter/032111-990068/index-hov007-b-n-a.html).

hensynet til rikets sikkerhet og vitale nasjonale interesser. Det kan for eksempel være å bygge kritiske elementer i fjellanlegg eller å ha spesielle kriselagerbeholdninger. Det kan hevdes at denne typen tiltak får uheldige konsekvenser for markedsposisjonen til de virksomhetene tiltakene retter seg mot. I den grad den enkelte virksomhet eller bransjeorganisasjon ikke selv ser nødvendigheten av dette, må myndighetene vurdere å gi pålegg om gjennomføring av nødvendige tiltak.

Det kan i tillegg tenkes at enkelte bedrifter ikke er opptatt av å kartlegge og redegjøre for de samfunnsmessige konsekvensene av sin virksomhet. Dette kan skyldes at det er vanskelig å ha oversikt over alle elementer som kan ha innvirkning på samfunnet, og det kan derfor være heftet stor usikkerhet til vurderingene, herunder vurderinger av konsekvensene av bortfall av virksomhetens varer og tjenester.

På bakgrunn av ovennevnte har utvalget vurdert virkemidler for å etablere et felles minstenivå på sikkerhet og beredskap både i offentlig og privat sektor. Det vises i denne sammenheng til utvalgets vurderinger og anbefalinger knyttet til både sektorovergripende virkemiddelbruk og virkemiddelbruken innenfor den enkelte sektor.

5.3.2 Samarbeid på tvers av offentlig og privat sektor

Arbeidet med beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner må baseres på et tett samarbeid mellom offentlige og private aktører. For at dette arbeidet skal være effektivt, forutsettes gjensidig tillit mellom aktørene. Offentlig-privat samarbeid vil kunne være et viktig supplement til krav stilt i lover og forskrifter, og fylle mangler i de eksisterende systemene.

På andre områder vil slikt samarbeid, dersom det fungerer, kunne ivareta samfunnets sikkerhetsbehov uten at myndighetene vil måtte gå veien om å sette rammevilkår i form av lover og forskrifter.

Skal næringslivet ivareta et samfunnsansvar er det viktig at det finnes arenaer for frivillig utforming av holdninger og strategier. Lover og forskrifter har en viktig rolle i forhold til å sikre at alle oppfyller minstestandarder, men myndighetene bør også se potensialet i det frivillige arbeidet som gjøres i næringslivet for å leve opp til samfunnets og bedriftenes egne krav til ansvarlighet.

Det vil være ønskelig med økt offentlig-privat samarbeid innenfor flere områder. Det vil blant annet være en fordel å etablere arenaer for informasjonsutveksling mellom det offentlige og det private. Slike arenaer er blant annet etablert i Storbritannia og Nederland, der det er sektorvise informasjonsutvekslingsfora mellom offentlige og private aktører innenfor kritisk infrastruktur og kritiske samfunnsfunksjoner. I slike fora er det naturlig å utveksle informasjon om blant annet trusler, risikoer og sårbarheter.

Et annet område hvor det kan være naturlig med et offentlig-privat samarbeid vil være i forhold til arbeid overfor virksomheter med samfunnskritiske oppgaver. Dette kan omfatte samarbeid om hvilke kriterier som skal ligge til grunn for å peke ut en virksomhet som samfunnskritisk og hvordan man kan sikre tjenesteleveranser til disse best mulig. Et slikt samarbeid vil blant annet kunne benyttes i forhold til knapphetssituasjoner (strømbrudd, brudd i vannforsyning mv.), matvareberedskap, bygg- og anleggsberedskap, fordeling av vaksiner, gjenoppretting etter naturkatastrofer og liknende.

Det offentlige og private samarbeidet knyttet til utvikling av standarder for sikkerhetsarbeid, er et viktig område. Det er i dag blant annet etablert internasjonale sikkerhetsstandarder innenfor flytrafikk og skipsfart, som alle aktører må forholde seg til.

Det kan ikke, og vil heller ikke være fornuftig å garantere 100 % leveransesikkerhet på samfunnskritiske varer og tjenester. Noe risiko må virksomheten leve med. Det bør derfor forutsettes at virksomhetene søker å kartlegge sin egen avhengighet av kritisk infrastruktur og kritiske samfunnsfunksjoner. Dersom en virksomhet er kritisk avhengig av visse typer varer og tjenester, bør denne søke å etablere tiltak for å redusere egen sårbarhet, for eksempel i form av nødstrømsaggregat, opplegg for nødvann, kriselager, m.m.

I denne forbindelse er det et spørsmål om ansvaret for risikoen kan deles mellom de ulike aktørene. En måte å gjøre det på er å fordele ansvar for risiko på tre nivåer, slik det er anbefalt at det skal gjøres i forhold til strømforsyning i Sverige (HEL-prosjektet[9]). I dette prosjektet er det anbefalt at ansvar for normalrisiko, definert som bortfall av strøm mellom 0 og 6 timer, dekkes av strømkunden. Bortfall av strøm opp til 3 døgn (behov for samordning/alvorlig påkjenning for samfunnet), er et privat offentlig samarbeid – der risiko deles mellom kraftleverandør og det offentlige. Når det gjelder konsekvenser ut over tre døgns strømbortfall, så vil dette være et offentlig (statlig) ansvar. Gjennom en risikodeling vil det være større incentiv for netteier til å investere i vedlikehold og leve-

[9] Prosjektrapport Energimyndigheten 2004. *Ökad samverkan för den svenska elförsörjingens säkerhet och beredskap*. HEL-projektet.

ringssikkerhet. Denne form for offentlig og privat risikodeling kan også tenkes på andre områder enn strømforsyning.

5.4 Utvalgets anbefalinger

5.4.1 Forslag knyttet til tydeliggjøring av Justis- og politidepartementets rolle

Gjennom de organisatoriske endringene som er foretatt og det ansvaret som nå er gitt Justis- og politidepartementet, er departementet gitt mulighet til å ha et helhetlig perspektiv på sikkerhets- og beredskapsarbeidet. Etter det utvalget kan se, er Justis- og politidepartementet på mange måter innrettet til å være det «Sikkerhetsdepartement» som sårbarhetsutvalget foreslo.[10]

Departementets overordnede ansvar for sikkerhet og beredskap er generelt og omfatter både det årsaksreduserende og konsekvensreduserende arbeidet som innrettes for å møte alvorlige påkjenninger som samfunnet utsettes for, herunder svikt i kritisk infrastruktur og kritiske samfunnsfunksjoner.

Ut fra en risiko- og sårbarhetstankegang bør ivaretakelse av sikkerheten og beredskapen i virksomheter med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner gis høyeste prioritet.

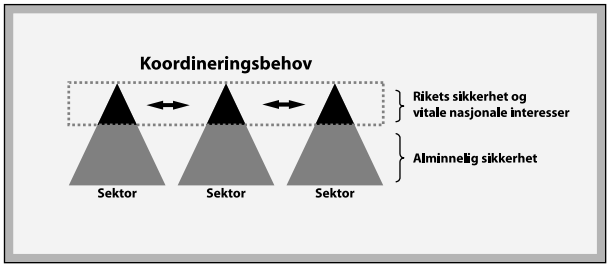
Utvalget vil påpeke viktigheten av å tydeliggjøre Justis- og politidepartementets rolle og ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner, samt viktigheten av å prioritere denne delen av departementets generelle ansvar for samfunnets sivile sikkerhet og beredskap. Dette innebærer at departementet må innta en tydeligere koordinerende rolle for å påse at hensynet til rikets sikkerhet og vitale nasjonale interesser blir ivaretatt på tvers av sektorene. Ikke minst for å unngå uklarheter på departementalt nivå og gi klare signaler med hensyn til mål og akseptnivå knyttet til sikkerhet og beredskap.

Skadepotensialet som følge av de gjensidige avhengighetsforhold mellom kritiske infrastrukturer og kritiske samfunnsfunksjoner gjør det nødvendig å sikre god koordinering av sikkerhets- og beredskapsarbeidet på tvers av sektorer og mellom de ansvarlige aktører. Utvalget mener at ett departement bør utpekes som ansvarlig for å ivareta en koordinerende rolle knyttet til kritisk infrastruktur og kritiske samfunnsfunksjoner og at denne rollen faller naturlig innenfor Justis- og politidepartementets eksisterende ansvar for samfunnets sivile sikkerhet og beredskap. Justis- og politidepartementet med underliggende virksomheter besitter spesialkompetanse knyttet til kritisk infrastruktur og kritiske samfunnsfunksjoner og ivaretar allerede utstrakt kontakt med aktørene på dette feltet både nasjonalt og internasjonalt.

I figur 5.1, er Justis- og politidepartementets tverrsektorielle koordineringsansvar søkt illustrert. Det er også søkt tydeliggjort at Justis- og politidepartementets koordinerende rolle knyttet til virksomheter av betydning for rikets sikkerhet og vitale nasjonale interesser ikke forutsettes å bryte med ansvarsprinsippet, men at koordineringsrollen må ivaretas gjennom et samarbeid med de relevante aktører.

Utvalget mener at viktige koordineringsoppgaver for Justis- og politidepartementet vil være å:

- Være rådgivende myndighet i spørsmål knyttet til sikkerhet og beredskap i kritisk infrastruktur og kritiske samfunnsfunksjoner.
- Være pådriver og tilrettelegger for samarbeid og informasjonsdeling mellom virksomheter med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner.
- Etablere og videreutvikle oversikt over kritisk infrastruktur og kritiske samfunnsfunksjoner i Norge, gjennom en felles metode og system for utpeking og klassifisering av kritisk infrastruktur og kritiske samfunnsfunksjoner.
- Bidra til koordinering mellom arenaer for samarbeid og informasjonsdeling knyttet til kritisk infrastruktur og kritiske samfunnsfunksjoner.
- Systematisere og koordinere trussel-, risiko- og sårbarhetsinformasjon knyttet til kritisk infrastruktur og kritiske samfunnsfunksjoner, herunder å etablere et system for innhenting og formidling av relevant informasjon. Dette må skje på basis av informasjon fra andre myndigheter og i samarbeid med de andre fagdepartementene.
- Kunne opptre som nasjonalt kontaktpunkt og nasjonal representant ved internasjonalt samar-



Figur 5.1 Justis- og politidepartementets koordineringsansvar sett i forhold til sektoransvaret.

[10] Det vises til Sørli, Kjetil 2005. *Oppfølging av sårbarhetsutvalgets rapport. Delrapport til Utvalg for sikring av landets kritiske infrastruktur.* Direktoratet for samfunnssikkerhet og beredskap – i del 2, vedlegg 7.

beid knyttet til beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner.
- Ta initiativ til avklaring av ansvarsforhold i de tilfeller dette ikke er gjort eller ansvarsforholdene synes uklare.
- Gjennom et samarbeid med aktuelle myndigheter, utarbeide felles målsetninger og strategier knyttet til kritisk infrastruktur og kritiske samfunnsfunksjoner.
- Frembringe tverrsektorielle problemstillinger eller forslag uten en bestemt ansvarlig adressat.
- Koordinere igangsettingen og oppfølgingen av tverrsektoriell forskningsaktivitet innen sikkerhet og beredskap, herunder BAS-studiene og SAMRISK (se kapittel 13).

5.4.2 Forslag knyttet til tydeliggjøring av nasjonale mål/akseptnivå

I et stadig mer avansert samfunn kan toleransen mot tekniske sammenbrudd og naturkatastrofer bli mindre. I et samfunn der koblingen mellom samfunnsfunksjoner og virksomheter er større enn før, vil også skadevirkningene av en hendelse fort bli mer omfattende enn tidligere (dominoeffekter). Det er derfor sentralt å arbeide med sikkerhet innen alle sektorer og virksomheter.

Generelt er det viktig med gode kvalitetsnormer, tydelige krav og effektivt tilsyn med ivaretakelsen av slike krav. Det bør være en klar forventning innen alle samfunnssektorer om gjennomføring av risiko- og sårbarhetsanalyser, vurdering av akseptnivå og utforming av handlingsplaner. Og det bør være en viss sammenheng mellom nivåene på sikkerhet på tvers av gjensidig avhengige sektorer («en kjede er ikke sterkere enn det svakeste leddet.»).

Tydeliggjøringen av nasjonale mål og akseptnivå må basere seg på vurderinger av sikkerhetsutfordringer fra en rekke kompetansemiljøer, og dette arbeidet forutsetter derfor en bred tilnærming.

Utvalgets anbefalinger

1. Det må innarbeides som premiss i aktørenes risiko- og sårbarhetsanalyser at risiko mot og sårbarheten innen kritisk infrastruktur og kritiske samfunnsfunksjoner er i sterk utvikling. Det er viktig at gjeldende risikovurderinger gjennomgås med sikte på at det er tatt tilstrekkelig høyde for usikkerhet om risiko og sårbarhet («føre var» - prinsipp).
2. Justis- og politidepartementet bør gi nærmere retningslinjer for gjennomføring av risiko- og sårbarhetsanalyser innenfor de ulike sektorene.[11] Det bør på sikt undersøkes om sikringsnivået innen de ulike sektorene er godt nok samordnet, særlig med tanke på gjensidig avhengighet mellom sektorene.
3. Det bør utvikles et forpliktende program for regelmessige risiko- og sårbarhetsanalyser tilknyttet kritisk infrastruktur og kritiske samfunnsfunksjoner. Dette antas også å være en viktig betingelse for at Justis- og politidepartementet skal kunne presentere faste redegjørelser for Regjering og Storting om sikkerhets- og beredskapsnivået i samfunnet. Ved å etablere et system med regelmessige samlede fremstillinger av risiko, sårbarhet og sivile beskyttelsesbehov, som igjen kobles til de regelmessige forsvarsanalysene, skapes et:
   - Grunnlag for tverrsektorielle avveininger innenfor det sivile samfunnssikkerhetsfeltet.
   - Grunnlag for en risikobasert prioritering av Forsvarets støtte til det sivile samfunn.
   - Grunnlag for en helhetlig analyse og politikk for det sivile og militære sikkerhetsarbeid.

Det er en økende grad av gjensidig avhengighet mellom aktiviteter, objekter og virksomheter med potensial for store ulykker. Det blir tilsvarende viktig å forbedre vår evne til å identifisere gjensidige avhengighetsforhold, sårbarheter og utfordringer og utvikle vår evne til å håndtere disse. Utvalget legger til grunn at Direktoratet for samfunnssikkerhet og beredskap gjennom sitt ansvar iht. Kgl.res. av 24. juni 2005 (tilsyn med aktiviteter, objekter og virksomheter med potensial for store ulykker), følger opp og bistår de forskjellige fagmyndigheter med å bringe inn tverrsektorielle problemstillinger i de sektorvise analysene, samt bistår med å tilrettelegge arenaer hvor fagmyndigheter, bransjeforeninger og andre kompetansemiljøer kan drøfte og finne løsninger på utfordringer.

5.4.3 Forslag knyttet til forholdet mellom NSM, PST og DSB

Ansvar og oppgaver som er tillagt NSM, PST og DSB kan oppfattes som delvis overlappende. Dette

[11] I USA er det utarbeidet en metode for *Risk Analysis and Management for Critical Assets Protection (RAMCAP)*. Tilsvarende arbeid er i gang i flere land. Ved å tilnærme seg problemstillingen fra en ROS-analysevinkling, får man frem formodet uakseptabel risiko, som støtte for politisk beslutningstager. Vi ser slike metoder utviklet og dels i bruk i Sveits, Tyskland, Danmark, Canada og Storbritannia, med det formål å komme frem til en overgripende nasjonal ROS-vurdering.

gjelder først og fremst den forebyggende virksomhet som rådgivning, veiledning og andre typer informasjonstiltak. For eksempel har både POD/PST og NSM utarbeidet veiledninger i egenbeskyttelse mot terror[12]. Det innebærer at ansvaret for å koordinere veiledningene ligger til virksomhetene, samtidig som det ikke kan utelukkes at det for virksomhetene fremstår som uklart hvilke råd som gis fra myndighetene. Et annet eksempel på delvis overlappende oppgaver er de rapporter og vurderinger som de tre direktoratene utarbeider knyttet til sikkerhetsutfordringer, jf. kapittel 4.3. Vurderinger gjort i ett direktorat brukes som innspill til vurderinger som gjøres i et annet direktorat. På denne måten er vurderingene komplementære. Dette vil i utgangspunktet være positivt og nødvendig, ettersom virksomhetene har ulike tilnærminger til sikkerhets- og beredskapsarbeidet. Utfordringen oppstår imidlertid når vurderingene skal distribueres, da ansvaret for å koordinere den informasjonen som gis fra myndighetene påhviler mottakeren. Virksomheter med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner er i stor grad adressater for disse direktoratene. Det er i denne forbindelse viktig å understreke at de tre direktoratene har et ansvar for at den informasjonen som kommer fra myndighetene er koordinert, slik at mottakeren har klart for seg hvordan informasjonen skal brukes for å oppnå god sikkerhet og beredskap. Det må således være tydelig for mottakeren hvilken rådgivning og informasjon de ulike myndighetene bidrar med, og hvordan disse forholder seg til hverandre.

Etter utvalgets mening er det svært viktig at fagmiljøene i de tre direktoratene samarbeider godt. Utvalget viser til at det er gjennomført og fortsatt pågår prosesser mellom direktoratene for å avklare ansvar og oppgaver, samt legge forholdene til rette for samarbeid der dette er hensiktsmessig. I tillegg til å understreke viktigheten av dette, vil utvalget anbefale sterkere koordinering av mål og resultatkrav som gjelder for direktoratene i de styrende dokumenter (regelverk, stortingsproposisjoner, tildelingsbrev). Utvalget mener at Justis- og politidepartementet gjennom en koordinert styring av direktoratene kan legge forholdene til rette for bedre brukertilpasning og faglige synergieffekter, samt bidra til å tydeliggjøre ansvarsforholdene mellom direktoratene.

I denne sammenheng har utvalget merket seg at forsvarskomiteen i Innst. S. nr. 234 (2003-2004), jf. St. prp. nr. 42 (2003-2004), ber departementet sørge for at det ikke hersker tvil om at det er Forsvarsdepartementet som har etatsstyringsansvaret for Nasjonal sikkerhetsmyndighet. Utvalget viser til ansvarsdelingen mellom Justis- og politidepartementet og Forsvarsdepartementet hva gjelder de faglige rapporteringslinjene til NSM, og understreker at dette ikke må begrense Justis- og politidepartementets muligheter til å se NSMs myndighetsutøvelse i sivil sektor i sammenheng med det øvrige sivile sikkerhets- og beredskapsarbeidet. Utvalget stiller spørsmål ved hvorvidt det i praksis er mulig å skille klart mellom etatsstyringsansvar og faglig ansvar.

5.4.4 Forslag knyttet til prinsipper for god sikkerhetskultur

Gjensidige avhengighetsforhold mellom virksomheter og samfunnssektorer innebærer at det er svært vanskelig for en enkelt bedrift å vurdere de totale konsekvensene av manglende innsats for preventive tiltak utenfor bedriften. Virksomhets- og sektorovergripende løsninger vil således være en forutsetning for å redusere samfunnets sårbarhet som følge av gjensidig avhengighet.

Eiere og driftsansvarlige i virksomheter med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner, er alle opptatt av at fornuftige beslutninger skal fattes på bakgrunn av innhentet og bearbeidet informasjon. I en slik sammenheng vil informasjon om sårbarheter og kunnskap om trussel- og risikobildet være en helt nødvendig forutsetning for beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner. Nedenfor følger noen prinsipper for god sikkerhetskultur, som utvalget mener bør legges til grunn i alle virksomheter med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner:

1. Godt lederskap og god virksomhetsstyring må påse at sikkerhets- og beredskapstiltakene følges opp av alle innenfor organisasjonen. Sikkerhets- og beredskapsarbeidet må ha høy status innenfor organisasjonen, og understøttes av alle.
2. Sikkerhet og beredskap bør inngå som en integrert del av virksomhetens drift og må omfatte både fysiske og IT-relaterte tiltak.
3. Sikkerhets- og beredskapstiltakene må baseres på trussel-, risiko- og sårbarhetsinformasjon og vurderes som en del av virksomhetens risikostyring. I denne forbindelse bør virksomheten ha system for jevnlige evalueringer og oppdateringer av sikkerhets- og beredskapsnivået. Dette forutsetter at virksomheten setter seg mål eller standarder for sikkerhets- og beredskapsarbeidet.

[12] NSMs veiledning ble utgitt i 2002, veiledningen fra POD/PST kom i 2006. Begge er gradert BEGRENSET

4. Virksomheten bør ha system for kompetansebygging innen sikkerhet og beredskap, herunder kursing, trening og øvelsesaktiviteter.
5. Virksomheten bør ha system for deling av relevant informasjon, både internt og eksternt.
6. Det bør systematisk opprettholdes fullstendige lister over roller og ansvar innenfor organisasjonen.
7. Virksomheten bør ha planer for å opprettholde drift gjennom tiltak som kan iverksettes ved økt trusselnivå, tiltak som kan iverksettes for å håndtere og redusere konsekvensene av alvorlige uønskede situasjoner og tiltak som kan gjenopprette normal drift etter en slik hendelse.

Gode rådgivnings- og veiledningstjenester er et helt sentralt virkemiddel for etableringen av en god sikkerhetskultur. Dette er spesielt viktig for virksomheter med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner. En rekke myndighetsorganer tilbyr slike tjenester, men innenfor ulike spesialområder og med forskjellige tilnærmingsmåter. Utvalget vil understreke betydningen av at myndighetsrollene er tydeliggjort, og vil derfor anbefale at det utarbeides en informasjonshåndbok hvor det fremgår hva de ulike myndighetsorganene kan tilby av råd og veiledning knyttet til sikkerhet og beredskap. Denne informasjonshåndboken bør utarbeides i nært samarbeid med næringslivet.

Utvalget viser til den integrering av helse-miljø-, og sikkerhetshensyn som har skjedd i deler av norsk næringsliv. I denne forbindelse vil utvalget understreke at hensiktsmessig virkemiddelbruk er en forutsetning for god sikkerhetskultur. Det vises i denne sammenheng til utvalgets vurderinger og anbefalinger knyttet til virkemiddelbruken.

Kapittel 6
Virkemidler[1]

Offentlige virksomheter instrueres direkte av overordnet myndighet. Med bakgrunn i Stortingets budsjettvedtak utarbeides årlige tildelingsbrev hvor det ansvarlige fagdepartementet presenterer de økonomiske rammene for virksomheten samt beskriver prioriteringer, resultatmål og andre forhold, slik at virksomhetene i sitt arbeid med virksomhetsplanlegging kan ta hensyn til føringer som fremgår av St.prp. nr. 1 for det aktuelle år. I tildelingsbrevene delegeres også de nødvendige fullmakter og budsjettmidler for virksomheten i det kommende budsjettåret. Forhold av betydning for virksomhetens ivaretakelse av hensynet til rikets sikkerhet og vitale nasjonale interesser, kan således innarbeides som direkte pålegg i virksomhetens tildelingsbrev.

Når virksomhet skilles ut fra det offentlige og organiseres som selvstendige rettssubjekter, må instruksjon og etatsstyring erstattes av andre typer styringsvirkemidler.

Virkemidlene kan grupperes på følgende måte:
- Juridiske, for eksempel lover, forskrifter, konsesjoner, lisenser, prisreguleringer.
- Organisatoriske, for eksempel utskilling av kommersielle enheter, selskapsdannelser og etablering av tilsynsorganer.
- Økonomiske, for eksempel tilskudd, kjøp av varer og tjenester, skatter og avgifter.
- Pedagogiske, for eksempel informasjon, øvelser og opplæring.

I tillegg til disse generelle virkemidlene, kommer mulighetene for eierstyring der det er heleide offentlige selskaper.

Det påpekes at de ulike virkemidlene kan påvirke hverandre direkte. For eksempel vil bruken av økonomiske eller organisatoriske virkemidler være regulert av et lov- eller regelverk. Utvalget finner det likevel hensiktsmessig å operere med et analytisk skille mellom ulike typer virkemidler for å skape en mer oversiktlig fremstilling.

[1] Kapittelet er basert på notat til utvalget fra Statskonsult, Statskonsult 2005. *Statlige styringsmidler – Sikkerhet og beredskap* – i del 2, vedlegg 8.

6.1 Juridiske virkemidler

Lov og regelverk er sentralt i reguleringen av ulike samfunnsområder og for å nå viktige samfunnsmål. Regelverket normerer og angir andre virkemidler som kan eller skal nyttes på en sektor, og det angir hvordan virkemidlene skal innrettes. Juridiske eller rettslige virkemidler er sentrale for å ivareta samfunnspolitiske målsettinger på sektorer der det har skjedd en selskapsdannelse.

Det benyttes ulike rettslige virkemidler for å nå politiske målsettinger. Viktige i denne sammenhengen er blant annet:
- Lover og forskrifter
- Konsesjoner
- Reguleringer: For eksempel prisreguleringer og regulering av markedsadgang og eierskap
- Vedtekter

6.1.1 Lovgivning

Alle offentlige og private bedrifter reguleres av en rekke forskjellige og generelle lover. Det kan være lover som regulerer arbeidsrettslige forhold, arbeidsmiljøet, forholdet til det eksterne miljøet og lignende. Det er i tillegg en rekke lover som regulerer enkeltområder eller sektorer av samfunnet. Det er ikke noe klart og stringent skille mellom det vi kan kalle generell lovgivning og sektorlovgivning. Både generell lovgivning og sektorlovgivning er viktige styringsformer.

Lovregulering er et viktig virkemiddel for å ivareta sikkerhets- og beredskapshensyn, og en rekke forhold på området reguleres gjennom lov eller forskrift. Lovgivningen kan regulere krav knyttet til beredskapsplaner, beredskapsøvelser, fysiske sikringstiltak og kontroll, kompensasjonsordninger, spesielle beredskapsfunksjoner og beredskapsorganer, opplæring, tilgjengelighet av varer og tjenester, sanksjonsmuligheter, mv.

Gjennom lovverket gis hjemmel for bruk av andre virkemidler på området, både organisatoriske (som etablering av tilsyn og komiteer) og økonomiske (avgifter og gebyrer).

6.1.2 Konsesjoner

En konsesjon er en tillatelse eller løyve fra offentlige myndigheter. Å få tildelt konsesjon medfører nærmere fastsatte rettigheter og/eller plikter som både kan være positivt og negativt formulert. Konsesjoner kan ha svært ulik utforming fra sektor til sektor. Konsesjonens innhold vil ofte innebære koblinger til andre virkemidler. Muligheten til å gjøre bruk av konsesjoner må være hjemlet i lov. Regelverket på en gitt sektor gir ofte rammer for innhold og vilkår som settes i konsesjonene.

Konsesjoner er viktige virkemidler i styringen av sektorer som har vært igjennom en markedseksponering og fristilling av statlig virksomhet. Konsesjoner benyttes innenfor mange områder, men det er betydelige forskjeller med hensyn til hvordan de er innrettet og på hvilke krav som kan stilles til konsesjonsinnehaver. Konsesjonsbetingelsene kan variere fra enerett og plikt til å utføre samfunnspålagte oppgaver, til å regulere hvem som skal få rett til innpass på et marked (kvalitetssikring) og enkelte forpliktelser knyttet til dette.

Konsesjoner er lite brukt som virkemiddel for å pålegge virksomheter sikkerhets- og beredskapsoppgaver.

6.1.3 Enerett- og monopolordninger

Formelle enerettsområder eller monopoler er normalt regulert gjennom lovgivning. Monopoler vil vanligvis være begrunnet ut fra hensynet til å nå samfunnsmessige mål ved utnyttelse av stordriftsfordeler. Det kan også være eksempler på naturlige geografiske monopolvirksomheter, der det ikke vil være regningssvarende å bygge opp konkurrerende virksomhet. På de områdene utvalget har sett på er det monopol på deler av oppgavene/nettet.

6.2 Organisatoriske virkemidler - tilsynsorganer

I en forvaltningspolitisk utvikling der virksomheter flyttes ut av staten og der det legges vekt på delegering, ser vi at styring med vekt på forhåndskontroll, blir erstattet av styring gjennom etterkontroll, rapportering og evaluering. I en slik utvikling får de nærmere 40 statlige tilsynsorganene en viktig rolle i å kontrollere at tjenester blir utført i henhold til fastlagte krav.

I forbindelse med at statlige forvaltningsorganer eller forvaltningsbedrifter er blitt omdannet til selvstendige selskaper eller foretak, er det blitt etablert egne tilsynsorganer som har et ansvar for tilsyn og kontroll innenfor sektoren. Tidligere var tilsynsvirksomheten ofte en integrert del av forvaltningsorganet eller forvaltningsbedriften. Det legges stor vekt på at tilsynene skal ha faglig og organisatorisk selvstendighet. I flere tilfeller er skillet mellom statens ulike funksjoner blitt forsterket ved at tilsynsorganet er underlagt fagdepartementet, mens eieransvaret for selskapet er overført til Nærings- og handelsdepartementet. Dette gjelder blant annet for Statkraft og Telenor. I St.meld. nr. 17 (2002-2003) om Statlige tilsyn er det lagt stor vekt på hensynet til uavhengighet og rolleklarhet og på hensynet til faglig kvalitet i tilsynene. Det legges opp til at det på flere områder skal foretas en lovmessig avskjæring av statsrådenes instruksjonsrett og at klager på tilsynenes vedtak skal behandles i uavhengige klagenemnder.

I noen tilfeller ligger eieransvar, faglig ansvar og tilsynsansvar fortsatt i samme departement. Dette er hovedsakelig på områder der virksomhetene i betydelig grad er faglig og/eller formålsmessig definert. Det gjelder blant annet for NRK, Statnett og Posten Norge.

Tilsynenes arbeidsoppgaver omfatter blant annet utarbeidelse av forskrifter, behandling av konsesjons- og dispensasjonssøknader, direkte inngrep, kontroller og aktivt forbedringsarbeid overfor dem man fører tilsyn med.

Tilsynene har en sentral rolle i myndighetenes arbeid for å ivareta sikkerhet og beredskap.

6.3 Økonomiske virkemidler

Økonomiske virkemidler kan være fastsettelse av avgifter og gebyrer, kjøp av tjenester, tilskudd, lån og garantier. Avgifter eller gebyrer kan brukes for å sikre at sektorpolitiske hensyn blir ivaretatt. På sektorer med markedsorganisering, kan det offentlige kjøpe tjenester fra private og/eller offentlige tjenesteleverandører på mer avgrensede felt der det kan oppstå markedssvikt. Tilskudd/kjøp av tjenester kan også benyttes for å etablere eller opprettholde et tjenestetilbud når dette ikke er bedriftsøkonomisk lønnsomt.

6.3.1 Avgifter og gebyrer

Avgifter er et mye brukt statlig virkemiddel. Bruken av avgifter på de områdene som er aktuelle her, kan ha ulike begrunnelser eller formål:

– En del avgifter er begrunnet ut fra statsfinansielle hensyn og vil i hovedsak ha som formål å skaffe inntekter til statskassen.

– Noen avgifter er begrunnet med at de skal fungere som betaling for ytelser på området. Nivået er satt for å dekke utgiftene og for å regulere prisnivået, slik at alle kan betale.
– Andre avgifter kan ha en spesifikk sektorpolitisk betydning. Et typisk eksempel er særavgiften på omsetning av alkohol, som primært er et virkemiddel for å begrense alkoholforbruket i befolkningen. Et annet eksempel er miljøavgifter, blant annet avgiften på utslipp av karbondioksyd.

Et viktig poeng med avgifter som styringsvirkemiddel, er nettopp at det i stor grad er brukere av tjenestene eller markedsaktørene som betaler. På enkelte områder vil dette være formålstjenlig og bidrar til direkte styring av for eksempel omfang eller tilgjengelighet. Dette ser vi blant annet ved at avgifter på flytrafikk delvis er knyttet til miljøhensyn.

Begrepene gebyrer og avgifter går noe over i hverandre. Men mens avgifter har en mer generell karakter, vil gebyrer ofte være koblet direkte til bruk og finansiering av en konkret tjeneste.

Tilsynsvirksomhet kan finansieres helt eller delvis gjennom gebyrer eller avgifter fra brukerne. Dette gjelder også tilsynenes virksomhet innenfor sikkerhet og beredskap, blant annet Direktoratet for samfunnssikkerhet og beredskap, Luftfartstilsynet, Mattilsynet, Post- og teletilsynet, Norges vassdrags- og energidirektorat, m.fl. Slike finansieringsordninger har karakter av øremerkede indirekte skatter.

6.3.2 Kjøp av tjenester - tilskudd

Det offentlige kan kjøpe tjenester fra, eller gi tilskudd til, virksomheter for å opprettholde et tilbud av tjenester som ikke kan drives bedriftsøkonomisk lønnsomt, og som det er av samfunnsmessig interesse å opprettholde. Slike tjenestekjøp kan skje på grunnlag av en anbudsrunde eller ved direkte kjøp. Anbud innebærer at det avholdes konkurranse om retten til å levere en vare eller tjeneste. På sektorer som er liberalisert vil det vanligvis brukes anbudskonkurranser. Dersom det bare er en aktuell leverandør eller andre tungtveiende hensyn kan staten benytte direkte kjøp.

Staten kjøper tjenester direkte fra blant andre Posten Norge AS, Avinor AS og NSB AS for å opprettholde tjenester i distriktene eller av miljømessige grunner. Statskog SF betales for utføringen av sin myndighetsutøvende virksomhet. I forbindelse med slike kjøp, spesifiseres det hva som skal leveres og til hvilken pris.

Tilskudd eller kjøp av tjenester benyttes i noen grad for å ivareta sikkerhets- og beredskapshensyn, for eksempel kjøpte Samferdselsdepartementet i flere år tjenester knyttet til sikkerhet og beredskap direkte fra Telenor. Et annet eksempel er legemiddelområdet, der Sosial- og helsedirektoratet har inngått en avtale med NMD grossisthandel AS som skal sikre forsyningsberedskapen.

6.4 Pedagogiske virkemidler

Pedagogiske virkemidler omfatter et forholdsvis vidt spekter av virkemidler som kan ha til hensikt å informere, lære opp eller bevisstgjøre befolkningen eller bestemte målgrupper. De pedagogiske virkemidlene har ikke vært spesielt fremtredende på sektorer der det har skjedd selskapsdannelser eller avvikling av statlige monopoler. Dette betyr imidlertid ikke at de ikke blir benyttet. Blant annet er informasjon om leverandører og priser et virkemiddel som blir brukt for å få markedene til å fungere bedre. Et eksempel på dette er Konkurransetilsynets offentliggjøring av strømpriser. Post- og teletilsynet publiserer halvårlige statistikker om telemarkedet og driver forbrukerportalene telepriser.no, nettvett.no og bredbåndsporten.no for å gjøre forbrukerne i stand til å orientere seg i markedet.

Virkemidler som hører inn under kategorien pedagogiske virkemidler ser ut til å være forholdsvis viktige på sikkerhets- og beredskapsområdet. Virkemidler som beredskapsplaner og beredskapsøvelser er viktige, og i flere tilfeller er det nedfelt i lovverket at det kan pålegges aktørene å utarbeide beredskapsplaner og å gjennomføre beredskapsøvelser. Opplæring av personell er sentralt når det gjelder sikkerhet og beredskap. Mange tilsyn har blant sine oppgaver å bidra til bevisstgjøring, kompetanseheving og veiledning overfor operatører, brukere og andre aktører og å arrangere felles øvelser mellom operatørene. Informasjon til befolkningen er også et virkemiddel som benyttes for å ivareta sikkerhet og beredskap.

6.5 Eierstyring

Regjeringen og departementet har en generell myndighet til å instruere alle virksomheter som er organisert innenfor staten (forvaltningsorganer). Dette betegnes gjerne som etatsstyring. Når en virksomhet er organisert som selvstendig rettssubjekt, kan ikke departementet benytte instruk-

sjon, og må i stedet styre gjennom andre virkemidler eller gjennom eierstyring. Instruksjonsmyndigheten kan i prinsippet benyttes på en omfattende og lite regulert måte. At staten i stedet for må benytte eierposisjonen, legger mer begrensninger på styringens form og innhold.

Styrene for heleide statlige aksjeselskaper og for statsforetakene oppnevnes av generalforsamlingen eller foretaksmøtet, som for disse selskapene vil si statsråden. Bortsett fra kravet til ansattes representasjon, er det få formelle krav til styresammensetning.

Det er den sittende statsråden i det departementet som forvalter eierskapet som er generalforsamlingen/foretaksmøtet i selskapet. Statsråden utøver dermed den øverste myndigheten i selskapet. I statsforetaksloven er det presisert at departementets myndighet i selskapet ikke kan utøves utenom foretaksmøtet. Det samme følger av aksjeloven for statsaksjeselskapene.

Aksjeloven tillegger styret et selvstendig ansvar for utbyttepolitikken i og med at det «ikke kan besluttes utdelt høyere utbytte enn styret foreslår». For statsaksjeselskap og statsforetakene ligger imidlertid utbyttemyndigheten hos generalforsamlingen eller foretaksmøtet.

Ved å bruke myndigheten til å fastsette vedtekter for virksomhetene kan staten som eier bidra til å tilpasse organisasjonsformene til de særlige behov som virksomhetene måtte ha. Et statsaksjeselskap kan for eksempel ha en bestemmelse i vedtektene om en mer omfattende kontakt mellom selskap og eier enn aksjeloven krever. Flere norske statsaksjeselskaper har en slik § 10 i vedtektene. Paragrafen sier at «alle saker som antas å være av vesentlig, prinsipiell, politisk eller samfunnsmessig betydning» skal forelegges generalforsamlingen. Styrene i selskaper med denne bestemmelsen skal hvert år legge frem en plan for virksomheten for generalforsamlingen der forhold som kommer inn under § 10 skal omtales. I tillegg skal departementene rapportere om selskapenes virksomhet til Stortinget i egen melding annet hvert år. Det er få eksempler på at slike rapporteringer har ført til instruksjon av styret.

Statsforetakslovens § 23 andre ledd, er en parallell til § 10 i vedtektene for statsaksjeselskapene, men innebærer en noe mer omfattende rapporteringsplikt. Bestemmelsen gir styret i statsforetaket en plikt til å legge frem saker av vesentlig betydning eller saker som vil endre virksomhetens karakter for eier. Dersom eier ønsker å gripe inn i en slik sak, må det skje gjennom foretaksmøtet. Etter statsforetakslovens § 24 tredje ledd, skal styreprotokollene i statsforetakene sendes eier innen to uker etter styremøtet.

Hensynet til sikkerhet og beredskap kan være ett (av flere) argument for statlig eierskap, for valg av selskapsform og for at statens eierinteresser skal forvaltes av sektordepartementet og ikke av Nærings- og handelsdepartementet. I en normalsituasjon vil dette ikke nødvendigvis virke inn på eierstyringen, men eierstyring gir andre styringsmuligheter enn dem som følger av de generelle regulatoriske virkemidlene. Behovet for en slik styringsmulighet kan endres over tid, og kan også anses som en sikkerhetsforanstaltning for mulige situasjonsbestemte styringsbehov.

6.5.1 Kontroll med eierstyring

I sum vil en kombinasjon av bruk av mange styringsvirkemidler overfor et selskap gi en omfattende myndighetsstyring. Når det gjelder selskapskontrollen, er Riksrevisjonens oppgave å kontrollere at statsrådene forvalter statens interesser på en lovlig og økonomisk forsvarlig måte, og i samsvar med de vedtakene og forutsetningene som Stortinget har angitt. Den løpende regnskapsrevisjonen er derimot ikke Riksrevisjonens oppgave. Hovedprinsippene for selskapskontrollen er nylig vurdert og foreslått videreført i utkastet til ny lov og instruks.

Stortinget behandlet den 25. februar 2003 Dokument nr. 3:2 (2002–2003) Riksrevisjonens kontroll med statsrådens (departementets) forvaltning av statens interesser i selskaper, banker med videre for 2001, jf. Innst. S. nr. 123. (2002–2003). Stortinget besluttet da å utvide Riksrevisjonens kontroll til også å gjelde oppgaver av ikke-økonomisk art, for eksempel oppgaver knyttet til bredere samfunnsinteresser, sektorpolitikk eller andre oppgaver som er pålagt av Stortinget som ledd i selskapskontrollen.

6.6 Utvalgets anbefalinger

6.6.1 Forslag knyttet til lovregulering

Utvalget vil understreke at det må være de samme krav til sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner enten en virksomhet er offentlig eller privat. Det er viktig å sette tydelige minstekrav til dette arbeidet, og ansvarliggjøre alle aktuelle virksomheter.

Utvalget mener det er behov for en harmonisering av regler for sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner. En slik harmonise-

ring skal ikke innebære at reguleringen av spesielle forhold knyttet til bestemte virksomheter eller formål skal oppheves.

Selv om det eksisterer til dels gode lovbestemmelser på dette området, er det likevel grunn til å påpeke noen mangler ved dagens regulering. Herunder viser utvalget til at det ikke er etablert generell beredskapsplikt i kommunesektoren, enkelte regelverk forholder seg ikke til villede hendelser, enkelte regelverk gjelder bare i krig og krigslignende tilstander, samt at enkelte regelverk gjelder i utgangspunktet bare for forvaltningsorganer.

Noen konkrete eksempler på mangler ved dagens regulering ser man i forsyningsloven. Loven gir ikke hjemmel til å pålegge private eller offentlige virksomheter å gjennomføre forberedende tiltak for krisehåndtering i fredstid. Samtidig gir loven virksomhetene plikt til å ta del i fredstids krisehåndtering. Et annet eksempel er sikkerhetsloven. I utgangspunktet omfatter lovens virkeområde bare forvaltningsorganer og bedrifter med spesielle avtaler med Forsvaret. Det vises i denne sammenheng til utvalgets vurderinger og anbefalinger knyttet til sikkerhetsloven i kapittel 7.

I tillegg til lover eksisterer det i dag flere kongelige resolusjoner som gir pålegg om hvordan staten skal innrette og prioritere sikkerhets- og beredskapsarbeidet generelt. Virksomheter med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner vil omfattes av disse bestemmelsene så fremt de er statlige. Med omreguleringer (privatisering og bortsetting) av statlige virksomheter, får imidlertid slike instrukser et mindre virkeområde og redusert betydning.

Som følge av stramme budsjettrammer, er det et kontinuerlig krav at offentlige virksomheter effektiviseres. Dette kan innebære et press i retning av å nedprioritere ikke lovpålagte oppgavene. Eksempelvis er det slik at fylkesmannsembeter og kommuner i økende grad prioriterer lovpålagte oppgaver, og nedprioriterer de ikke lovpålagte oppgavene.

Manglende harmonisering kan føre til at de ulike regelverkene ikke i tilstrekkelig grad ivaretar viktige forhold som gjelder både forebyggende sikkerhet og beredskap på en tilfredsstillende måte, og ut fra felles, overordnede prinsipper. Det er i dag ikke en enkel oppgave å vurdere hvorvidt krav til sikkerhet og beredskap i virksomheter med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner er tilstrekkelig regulert i sektorregelverket, og følgelig heller ingen enkel oppgave å evaluere den reelle sikkerhets- og beredskapssituasjon i samfunnet. I en slik prosess vil det være nødvendig å vurdere en betydelig mengde lover og forskrifter som skal avstemmes i forhold til de krav som er stilt. Det vil være gevinster å hente ved å foreta slike vurderinger opp mot felles minstekrav til de eksisterende sektorregelverk.

Det er etter utvalgets mening behov for en tydeligere forankring av eksisterende generelle bestemmelser knyttet til sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner i sektorregelverkene. Det er etter utvalgets oppfatning viktig med en referanseramme som kan bidra til en harmonisering av bestemmelser i de enkelte sektorene.

6.6.1.1 Forslag knyttet til generell lov om beredskap

Utvalget vil foreslå at det utarbeides en generell, sektorovergripende lov om beredskap. Det bør i denne forbindelse foretas en forvaltningsmessig gjennomgang og avstemming av det eksisterende regelverk på bakgrunn av et felles kriteriesett.

Utvalget viser til Stoltenberg II regjeringens Soria-Moria erklæring, hvor det fremgår at regjeringen vil «foreta en gjennomgang av Beredskapsloven for å avklare og kartlegge beredskapsmessige gråsoner.» Utvalget antar at vurderingene og anbefalingene nedenfor kan være relevant å vurdere i det forestående utredningsarbeidet.

Lovens formål bør være å sikre at hensynet til rikets sikkerhet og vitale nasjonale interesser ivaretas under alle former for påkjenninger i fred, krise og krig. Lovens virkeområde må defineres slik at virksomheter med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner blir omfattet. På denne måten vil loven bidra til å tydeliggjøre eiers ansvar knyttet til kritisk infrastruktur og kritiske samfunnsfunksjoner.

Utvalget mener det er viktig å sikre størst mulig forutsigbarhet når det gjelder hvilke virksomheter som skal gis krav gjennom nye lovbestemmelser. Identifisering av hvilke virksomheter loven skal omfatte må skje gjennom et samarbeid mellom virksomheter, deres organisasjoner og myndighetene. Endelig vedtak om lovens virke for den enkelte virksomhet må gjøres av det departement som forvalter loven. For offentlige organer kan loven likevel gjøres gjeldende på generell basis.

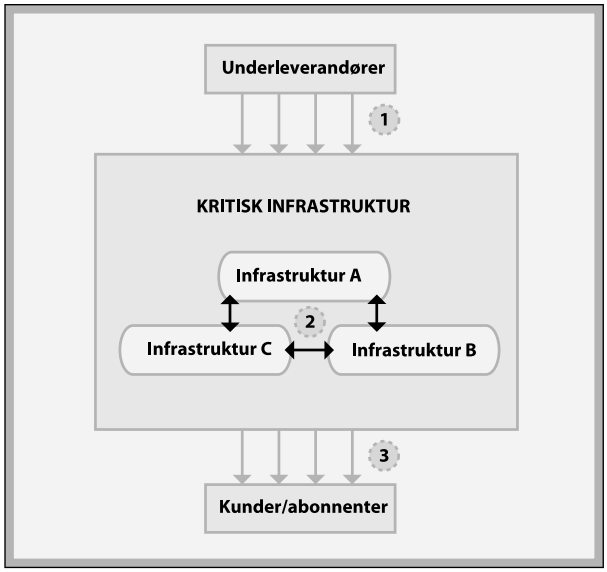
I tillegg til virksomheter med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner, må en generell lov om beredskap også kunne omfatte leverandører av kritiske støttefunksjoner som disse virksomhetene er avhengige av, herunder bygg- og anleggstjenester, vedlikeholdstjenester, vakthold osv. Utvalget vil peke på at det er viktig at

disse støttefunksjonene prioriterer sine ressurser til virksomheter med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner ved knapphetssituasjoner. Samtidig mener utvalget at disse støttefunksjonene må sikres den nødvendige prioritet av kritiske varer og tjenester som de er avhengige av. Det må forutsettes at de enkelte underleverandørene til virksomheter med kritisk infrastruktur og kritiske samfunnsfunksjoner ikke lider urimelige økonomiske tap på bakgrunn av myndighetenes prioriteringer i kriser.

Utover bestemmelser om lovens formål og virkeområde, vil utvalget foreslå at loven inneholder bestemmelser om:

- Definisjoner av sentrale begreper
  - Loven bør inneholde definisjoner av sentrale begreper som brukes i beredskapsarbeidet, herunder begreper som trussel, risiko, sårbarhet, mv. Det bør søkes en harmonisering av definisjonene i lovarbeid knyttet til relevant lov- og forskriftsverk.
- Gjennomføring av risiko- og sårbarhetsanalyser[2]
  - Loven bør regulere en plikt til å utarbeide jevnlige risiko- og sårbarhetsanalyser, eventuelt at slike analyser utarbeides ved behov. Analysene bør inkluderes som en del av virksomhetens beslutningsgrunnlag, herunder danne grunnlag for eventuelle beredskapstiltak, og ses opp mot de vurderingene som utarbeides av myndighetene. Det bør vurderes om det skal gis nærmere retningslinjer for hvordan slike analyser skal utarbeides, for eksempel ved at det henvises til bruk av standarder. Det bør også vurderes en form for rapportering/dokumentasjon til ansvarlig tilsynsmyndighet.
- Drifts- og leveransesikkerhet
  - Loven bør regulere krav til ytelser av varer og tjenester i knapphetssituasjoner, herunder bør loven regulere en gjensidig forsyningsplikt, selv under kriser, mellom de kritiske infrastrukturene som er mest gjensidig avhengige av hverandre (se grensensitt 2 i figur 6.1). Loven bør også gi hjemmel for myndighetene til å kunne gi pålegg om særskilte tiltak, eventuelt ta offentlig kontroll med private ressurser. Det bør imidlertid være opp til den enkelte infrastrukturvirksomheten å inngå avtaler med sine underleverandører som sikrer virksomhetene tilgang på kritiske underleveranser under alle forhold, også i beredskapssituasjoner (se grensesnitt 1 i figur 6.1).
  - Loven bør regulere en plikt til å etablere leveransevilkår mellom virksomhetene og deres kunder, der egenansvar og beredskap hos kundene også blir avklart (se grensesnitt 3 i figur 6.1). Det bør vurderes i hvilken grad loven skal inneholde konkrete krav til driftskontinuitet, for eksempel på de områder som anses mest kritiske for samfunnet.
- Utarbeidelse av beredskapsplaner
  - Loven bør regulere en plikt til å utarbeide beredskapsplaner som skal bidra til å redusere skadefølgene av at virksomheten utsettes for ulike former for påkjenninger. Loven bør regulere en plikt til å oppdatere planene, samt jevnlig gjennomføre kriseøvelser.
- Informasjonsdeling og samarbeid
  - Loven bør inneholde krav til samarbeid og informasjonsdeling mellom private virksomheter og offentlige myndigheter knyttet til beredskap innenfor nærmere definerte samfunnssektorer, herunder elektronisk kommunikasjon-sektoren, kraftsektoren, vann- og avløpssektoren, transportsektoren, olje- og gassektoren, matsektoren, bank- og finanssektoren, helse-, sosial- og trygdesektoren, og ev. andre sektorer ved behov. Loven bør regulere plikt til samarbeid mellom virksomheter og ansvarlige myndigheter om beredskapsplanlegging og nødvendige beredskapstiltak.
- Tilsyn og sanksjonsmuligheter
  - Loven bør regulere hvem som skal være tilsynsmyndighet. Det bør vurderes om tilsynet i medhold av loven skal deles mellom sektortilsynene. I så fall bør et sentralt tilsynsorgan ivareta en koordinerende rolle. Herunder bør ansvarslinjene mellom sektortilsynene, Nasjonal sikkerhetsmyndighet og Direktoratet for samfunnssikkerhet og beredskap vurderes.
  - Det må forutsettes at tilsyn med virksomhetene gjennomføres med fullt innsyn i tilgjengelig dokumentasjon, samt full adgang til virksomhetens fasiliteter. Loven bør også regulere reaksjonsmidler ved manglende etterfølgelse av krav eller ved påvist grov uaktsomhet eller bevisst unndragelse av ansvar for sikkerhet og beredskap.

[2] Utvalget har fått Senter for risikostyring og samfunnssikkerhet (SEROS) til å utarbeide et notat om rammeverk for gjennomføring av risiko- og sårbarhetsanalyser av kritisk infrastruktur. Se Aven, Terje og Wiencke, Herman Steen 2005. *Rammeverk for gjennomføring av risiko og sårbarhetsanalyser av samfunnskritisk infrastruktur.* SEROS Senter for risikostyring og samfunnssikkerhet – i del 2, vedlegg 9.



Figur 6.1 Illustrasjon av grensesnittene i en ny lov om beredskap.

En ny lov om beredskap slik det er beskrevet over, vil ha berøringspunkter i forhold til Lov av 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven). Lovens virkeområde vil omfatte stort sett de samme virksomheter, og prosessen for å identifisere disse vil være ganske lik den utvalget legger opp til for sikkerhetslovens vedkommende.

Mens sikkerhetsloven i hovedsak retter seg mot trusler som følge av villede handlinger (spionasje, sabotasje eller terrorhandlinger), vil en generell lov om beredskap ha et videre perspektiv. Det beredskapsmessige aspektet vil dessuten stå helt sentralt i denne loven.

Utvalgets intensjon med å foreslå en ny lov om beredskap er at denne skal virke sammen med sikkerhetsloven, og at de utfyller hverandre med hensyn til hvilke områder de dekker og de pålegg og tiltak som skal bidra til å oppfylle behovet for sikring av kritisk infrastruktur. Dette tilsier at de nødvendige lovregler må etableres så raskt som mulig.

Utvalget mener det er viktig å organisere arbeidet med å få på plass nødvendige lovhjemler på en måte som sikrer en så rask og smidig gjennomføring som mulig. Utvalget er kjent med at en prosjektgruppe under ledelse av Justis- og politidepartementet har utarbeidet et forslag til lov om sivilforsvar, sivile beskyttelsestiltak og beredskapstiltak som i hovedsak følger de hensyn utvalget ovenfor har skissert et behov for å lovregulere. Hvis det viser seg at de hensyn utvalget etterlyser blir godt ivaretatt i forslaget fra prosjektgruppen, mener utvalget at det er naturlig at dette arbeidet ses i sammenheng med utvalgets forslag om en generell lov om beredskap.

6.6.1.2 Behovet for å se næringslivets rolle under ett

De tiltakene som pålegges næringslivet må ses som elementer i en totalpakke av tiltak som samlet gjør at næringsaktørene kan leve opp til de forventningene samfunnet og myndighetene har til dem når det gjelder å ivareta kollektiv sikkerhet og tilgang på varer og tjenester. Bare gjennom forutsigbare rammer som ikke etterlater gråsoner eller uklare ansvarsforhold eller pålegger bedrifter uforholdsmessige store byrder kan næringslivet fylle sin rolle som forventet. Det er derfor viktig i så stor grad som mulig å se samfunnets behov for sikkerhet og forutsigbarhet i næringslivet under ett.

Den gjeldende beredskapslovgivningen er ikke klar nok i forhold til denne utfordringen. Det er derfor spesielt viktig å ha fokus på dette når man nå gjennomgår og endrer deler av det relevante lovverket. Risiko- og sårbarhetsanalyser og verdivurderinger må danne basis for pålegg til bedrifter om særskilte tiltak. Det er også viktig at behov for organisatoriske tiltak som for eksempel industrivern ses i sammenheng med generelt brannvern og ambisjonsnivået for dette, men også i forhold til bedriftenes rolle som aktører for eksempel innenfor kritisk infrastruktur eller kritiske samfunnsfunksjoner. Siden brann- og eksplosjonsvern er en grunnberedskap som pålegges alle i samfunnet, mens andre typer tiltak og pålegg er mer spesifikt knyttet til en bedrifts rolle i samfunnet kan det være hensiktsmessig at de funksjonene som ivaretas av Næringslivets sikkerhetsorganisasjon i større grad ses i sammenheng med næringspolitikk og -beredskap.

6.6.1.3 Forslag knyttet til revisjon av sivilforsvarsloven

Utvalget er kjent med at en prosjektgruppe under ledelse av Justis- og politidepartementet arbeider med revisjon av lov om sivilforsvar m.v.

Utvalget anbefaler at dette arbeidet vurderes i sammenheng med utvalgets forslag om en generell lov om beredskap.

Utvalget vil vise til viktigheten av å se regulering på dette området i et helhetlig perspektiv, som en del av andre nødvendige juridiske justeringer for å regulere samfunnssikkerheten. Dette gjelder blant annet arbeidet med revisjon av sivilforsvarsloven og innføringen av kommunal beredskaps-

plikt, revisjon av plan- og bygningsloven samt behovet for en referanse i kommuneloven om kommunens ansvar når det gjelder samfunnssikkerhet. Til dette siste kan det for eksempel i kommuneloven innarbeides en generell bestemmelse om at kommunene plikter å bidra til trygghet og sikkerhet for sine innbyggere.

6.6.1.4 Forslag knyttet til forsyningsloven

De gjeldende planleggingsforutsetningene for sivilt beredskap legger opp til at næringslivet i større grad skal ansvarliggjøres. Samtidig er også en stadig større del av de kritiske infrastrukturene og de kritiske samfunnsfunksjonene konkurranseutsatt. Det er derfor viktig at arbeidet med samfunnssikkerhet organiseres slik at næringene får rom for markedstilpasning i kriser samtidig som samfunnets forventninger om tilgang til varer og tjenester ivaretas.

Nærings- og handelsdepartementet har i flere år arbeidet med å tilpasse sine beredskapssystemer til det gjeldende trusselbildet, dagens næringsstruktur og departementets generelle næringspolitiske strategi. De endringer som har vært gjort har vært innenfor rammene som gjeldende beredskapslovgivning setter.

Det videre arbeidet er i stor grad avhengig av endringer i lovverket og eventuelt endringer i de økonomiske virkemidlene. Nytt lovverk på området bør være nærings- og eierskapsnøytralt og omfatte alle former for kommersiell produksjon og omsetning av varer og tjenester.

Utvalget anbefaler at en ny generell lov om beredskap ivaretar de utfordringer som kravene til en modernisering av forsyningsloven stiller. En ny forsyningslov bør gi hjemler til å iverksette realistiske og hensiktsmessige forberedelser og tiltak i kriser i fred og krig. Den bør være næringsnøytral og eierskapsnøytral og omfatte alle former for kommersiell produksjon og omsetning av varer og tjenester. Det er sannsynlig at en ny forsyningslov naturlig bør forankres i Justis- og politidepartementet. Det bør i kjølvannet av lovarbeidet også vurderes om Nærings- og handelsdepartementets koordineringsansvar for matvareberedskap bør bortfalle.

6.6.1.5 Forslag knyttet til plan- og bygningsloven

Det såkalte Planlovutvalget ble oppnevnt ved kongelig resolusjon 23. oktober 1998. De avga sin andre innstilling til Miljøverndepartementet 13. mai 2003.[3]

Utvalgets oppdrag var å gå gjennom reglene om regional og kommunal planlegging i nåværende plan- og bygningslov og foreslå forbedringer. I sitt forslag til endring understreket utvalget viktigheten av å unngå å bygge inn ny risiko og sårbarhet i samfunnet. Det ble blant annet vist til at planleggingen skal bestå både i å forebygge risiko for skade og tap av liv, helse, miljø og viktig infrastruktur, samt å ha en beredskap for ulykkessituasjoner med videre. Dette dreier seg til dels om god fysisk planlegging for å unngå at det skjer utbygging i områder som er særlig utsatt for flom, ras, skred, akutt forurensing og så videre. Utvalget mente videre at det må være et mål for samfunnsplanleggingen å sette klare grenser gjennom arealplanleggingen som bidrar til å hindre eller fjerne ugunstige etableringer.

Bygging av de fleste infrastrukturer vil også måtte lokaliseres til et areal. Infrastruktursikkerhet vil i så måte være preget av den iboende sårbarhet eller risiko som arealet er eksponert for. Det at viktige infrastrukturer ikke lokaliseres til områder som er utsatt for noen form for risiko bør derfor være logisk. For å avdekke en eventuell risiko eller sårbarhet i arealet må en eller annen form for analyse gjennomføres. Per i dag stilles det få juridiske krav til slike kartlegginger.

Fra Planlovutvalgets side ble det foreslått å styrke arbeidet med helse- miljø og sikkerhet (HMS), med spesielt fokus på risiko- og sårbarhetsanalyser. Det ble tydeliggjort gjennom et særskilt lovforslag (§1-10). Formålet med lovforslaget var at planlegging og utbygging etter loven skal bidra til den enkeltes trygghet for liv, helse og eiendom, sikre samfunnets evne til å fungere teknisk, økonomisk og institusjonelt, og hindre en utvikling som truer viktige forutsetninger for dette. Forslaget til lovtekst var som følgende:

> § 1-10 Samfunnssikkerhet og risiko- og sårbarhetsanalyse
>
> Planleggingen etter loven skal fremme samfunnssikkerhet ved å forebygge risiko for skade og tap av liv, helse, miljø og viktig infrastruktur, materielle verdier m.v.
>
> Ved utarbeiding av arealplan for utbygging skal planmyndigheten påse at risiko- og sårbarhetsanalyse gjennomføres for planområdet, eller selv foreta slik analyse. Analysen skal vise alle risiko- og sårbarhetsforhold som har betydning for om arealet er egnet til utbyggingsformål, og eventuelle endringer i slike forhold som følge av planlagt utbygging. Område med fare, risiko eller sårbarhet avmerkes i planen

[3] NOU 2003:14 *Bedre kommunal og regional planlegging etter plan- og bygningsloven II* .

som hensynssone, jf. § 9-8. Planmyndigheten skal vedta slike bestemmelser om utbyggingen i sonen, herunder forbud, som er nødvendig for å avverge skade og tap.

Utvalget anbefaler at samfunnssikkerhetsperspektivet i større grad enn i dag legges inn i ny plan- og bygningslov. Utvalget anbefaler videre at hensynet til konsekvenser av både tilsiktede og utilsiktede hendelser skal ligge til grunn.

Planlovutvalgets forslag har siden 2003 ligget i Miljøverndepartementet uten at det er fremmet en lov. Utvalget mener at en viktig del av å sikre landets kritiske infrastruktur innebærer å ha en plan- og bygningslov som ivaretar Planlovutvalgets bemerkninger slik de fremkommer i § 1-10. I tillegg ønsker utvalget å gjøre oppmerksom på at også konsekvenser ved tilsiktede hendelser må legges til grunn for utarbeidelse av en arealplan for utbygging. Dette kan eksempelvis gjelde bygninger som på grunn av sin funksjon kan sies å ha en forhøyet risiko for tilsiktede hendelser. Det kan gjelde for utenlandske ambassader, bygninger som innehar større mengder kontanter og andre som kan være særlig utsatte.

Etter hva utvalget erfarer, arbeider Miljøverndepartementet for tiden med et forslag til lovtekst på bakgrunn av høringen av NOU 2003:14 Bedre kommunal og regional planlegging etter Plan- og bygningsloven II. Forslagene som Planlovutvalget har fremmet i tilknytning til samfunnssikkerhet blir i hovedsak fulgt opp ved at innholdselementene videreføres i departementets forslag, selv om det blir foretatt lovtekniske og språklige justeringer. Lovens formålsbestemmelse utformes etter mønster av Bygningslovutvalgets forslag, jf. NOU 2005:12 Mer effektiv bygningslovgivning II.

6.6.2 Forslag knyttet til tilsynsvirksomhet

I Norge er det ikke etablert en ensartet modell eller praksis for tilsynsvirksomhet. Tilsynsvirksomheten varierer med hensyn til oppgaver og roller, fullmakter, organisering og tilknytning til statsforvaltningen. Hele virkemidlet tilsyn har lenge vært gjenstand for debatt. Klager fra næringsliv og bransjeforeninger over den tunge reguleringsbyrden har vært uttrykk for frustrasjoner som kan være både reelle og vel begrunnede.

Det er ikke mulig å forebygge alle uønskede hendelser, verken gjennom regulering eller på andre måter. Dette tilsier en vurdering av hva som kan forebygges, hvordan det kan gjøres og på hvilke områder innsatsen vil gi størst effekt. Denne typen kunnskap er det produsert svært lite av i Norge, og det som finnes andre steder er i liten grad utnyttet. Utvalget kan derfor bare anta at variasjonene er store hva gjelder grad av måloppnåelse opp mot ressurser og innsatsfaktorer. Det er derfor nærliggende å tro at potensialet for en mer effektiv bruk av innsatsfaktorer er ganske stort. Videre er det ikke utenkelig at det opprettholdes tilsyn på områder uten nevneverdig effekt, samtidig som det finnes tilsyn hvor den positive effekten av å øke innsatsen ville blitt merket umiddelbart. Dette tilsier at det er behov for en kritisk gjennomgang av tilsynsvirksomheten generelt. Et annet problem er oppfølging av områder der det ikke er noen klare sektortilsyn eller der det er uklare grenser til andre sektortilsyn.

Utvalget viser til at det generelt er et mål å samordne tilsyn. Dette gjelder også på sikkerhets- og beredskapsområdet. Det er i denne forbindelse viktig å påpeke at det kan være forskjeller i hva som legges i begrepet samordning, herunder samordning av tilsynsmetodikk, samordning på tid (inspeksjoner gjennomføres samtidig), samordning på tema, og overordnet samordning (koordinering). Når det gjelder samfunnssikkerhet og beredskap ved virksomheter med potensial for store ulykker og i forhold til virksomheter som omfattes av storulykkeforskriften, bemerker utvalget at den overordnede koordineringen av tilsynsvirksomheten er lagt til DSB, jf. instruks gitt ved kgl. res. av 24. juni 2005.

Utvalget er generelt opptatt av at ansvarsforholdene knyttet til sikkerhet og beredskap i kritisk infrastruktur og kritiske samfunnsfunksjoner er avklart, ikke minst at dette er ryddig når det gjelder forholdet mellom tilsynsorgan og tilsynsobjekt. Utvalget er opptatt av at det i utgangspunktet må være virksomhetene selv som ivaretar sitt ansvar for å gjennomføre de tiltak som er nødvendige ut fra en selvstendig risikovurdering (i samsvar med internkontrollprinsippet).

Utvalget ser at det kan være uheldig at et departement både innehar det faglige ansvar for et sektortilsyn og er eier av virksomheter som dette sektortilsynet fører tilsyn med innenfor sektoren. I slike tilfeller kan det tenkes interessekonflikter mellom ivaretakelse av hensynet til sikkerhet og beredskap og virksomhetens avkastningsmål.

Etter utvalgets mening er det også et problem at enkelte av sektortilsynene i liten grad bruker ressurser på å følge opp problemstillinger knyttet til sikkerhet mot villede hendelser. Dette kan følge av mangler i reguleringen, eller av sektortilsynene risikoforståelse. Utvalget er for øvrig opptatt av betydningen av at tilsynene i sin virksomhet finner en god balanse når det gjelder å måle og fange opp forbedringsbehov i virksomhetenes samlede risi-

kohåndtering, dvs. alt fra små uhell og ulykker med stor sannsynlighet og over til store sammenbrudd og katastrofer med lav sannsynlighet.

Med bakgrunn i ovennevnte vil utvalget anbefale at tilsynsvirksomheten på området kritisk infrastruktur og kritiske samfunnsfunksjoner utredes nærmere. Formålet med en slik utredning bør være å sikre at tilsynsvirksomheten på dette området er mest mulig mål- og resultatorientert i forhold til sikkerhets- og beredskapsbehovene. Utvalget vil anbefale at det i denne sammenheng vurderes en samordning av tilsynsvirksomheten og en prinsipiell drøfting av forholdet mellom tilsyn som ivaretar overordnede interesser og tilsyn som ivaretar sektorinteresser (horisontale vs. vertikale tilsyn). Til en viss grad vil det også være relevant å vurdere forholdet mellom tilsyn på den ene siden og uavhengige undersøkelsesorgan som Havarikommisjonen for transport på den andre. Det bør vurderes om det er satt av tilstrekkelig med ressurser til forvaltningen av helheten i tilsynsvirksomheten på sikkerhets- og beredskapsområdet, eller om ressursene kan brukes annerledes.

Dernest anbefaler utvalget at det utarbeides en nasjonal strategi for tilsynsvirksomheten knyttet til sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner. Utvalget viser til DSBs overordnede samordningsansvar (jf. blant annet kgl. res. av 24. juni 2005), og anbefaler at DSB gis en sentral rolle i utarbeidelsen av strategien.

Utvalget viser til de mer konkrete anbefalingene knyttet til tilsynsvirksomhet innenfor enkelte samfunnssektorer, jf. kapittel 10 og 11[4].

6.6.3 Forslag knyttet til etablering av tilskuddsordning

Staten har det helhetlige ansvaret for at det er god sikkerhet og god beredskap i det norske samfunnet. Dette omfatter også et finansieringsansvar. Dette ansvaret må ses i sammenheng med virkemiddelbruken generelt. Offentlige virksomheters utgifter til sikkerhet og beredskap vil være styrt av politiske mål og prioriteringer samt krav som stilles i lover og forskrifter. Utgiftene dekkes over de offentlige budsjetter, og nye tiltak finner sin inndekning gjennom regjeringens budsjettrammefordeling og Stortingets budsjettvedtak.

Det følger av dette at alle typer sikkerhets- og beredskapstiltak må gjennomføres og finansieres innenfor de til enhver tid gjeldende budsjettrammer for hver enkelt offentlig virksomhet. Dette innebærer at virksomhetene planlegger, prioriterer og om nødvendig samordner tiltakene i forbindelse med utarbeidelsen og disponeringen av sine årlige budsjetter. Det er i denne sammenheng viktig å påpeke at oppfølgingen av tiltakene skjer iht. de krav som er stilt i økonomireglementet til kontroll og styring med budsjettmidler, og er således underlagt Riksrevisjonens og Stortingets kontroll.

Dette innebærer en særlig utfordring når det er snakk om tiltak av tverrsektoriell betydning, eller tiltak som ikke har en klart definert sektoransvarlig myndighet. Det presiseres at det i dag ikke faller inn under Justis- og politidepartementets samordningsrolle å sikre finansieringen av sikkerhets- og beredskapstiltak innenfor andre departementers fagområder. Justis- og politidepartementets rolle kan være å ta initiativ til å få tiltakene iverksatt, uten nødvendigvis å bære noe finansielt ansvar. En fordel med denne finansieringsmåten er at man unngår uenighet mellom fagdepartementene om prioritering og innretting av tiltak. En ulempe kan være at prosessen for å finne tilstrekkelig finansiering av tiltakene blir unødvendig tidkrevende, eller at viktige tiltak rett og slett nedprioriteres.

Det kan for eksempel være behov for å gi tilskudd i forbindelse med utbygging av reservekraft (nødaggregater) for å sikre drift av særlig viktige samfunnsfunksjoner, deteksjonstiltak mot ABC-midler på offentlige steder osv. Andre viktige tverrsektorielle tiltak som kan finansieres av en tilskuddsordning er forskning og utredning på gjensidige avhengigheter mellom kritiske infrastrukturer, og finansiering av eventuelle forbedringstiltak som forskningsprosjektet avdekker, jf. kapittel 13. Etter utvalgets mening må slike aktiviteter avgrenses til konkrete objekter og systemer. For eksempel vil analyser av punkter i elektroniske overføringsnett og punkter i strømnettet kunne avdekke behov for tiltak som reduserer sårbarhet som følge av gjensidige avhengigheter dem i mellom.

Virksomhetens utgifter til sikkerhet og beredskap vil på sin side være styrt av virksomhetens egne mål- og prioriteringer samt krav som stilles i lover og forskrifter. Bedriftsøkonomiske vurderinger vil således være styrende for innføring av sikkerhets- og beredskapstiltak som går utover de krav som stilles i lover og forskrifter. Dette er ingen garanti for at virksomheten ivaretar hensynet til rikets sikkerhet og vitale nasjonale interesser.

Staten, kommunene og private selskaper legger ikke alltid samme hensyn til grunn når de vurderer risiko. For eksempel kan private selskaper

[4] Det vises for øvrig til del 2, vedlegg 13 for en tabell over ytre etater (direktorater og tilsyn) som har ansvar for sikkerhet som en del av sin virksomhet.

ha fokus på sikkerhet for å bevare eget omdømme, merkevareoppbygging og markedsposisjoner (i tillegg til liv, helse og miljøhensyn), mens det offentlige i tillegg har ansvar for tilstrekkelig tilgang til varer og tjenester til befolkningen. Private selskaper vil heller ikke nødvendigvis vurdere trusler knyttet til store hendelser, sikkerhetspolitiske kriser og krig når de vurderer egen risiko. Videre vil staten kunne vurdere en gitt funksjon som så viktig at det er behov for redundans ut over det aktøren selv er villig til å betale for. Staten og private selskaper vil også kunne operere med ulik tidshorisont når de vurderer risiko.

For funksjoner der bortfall kan ha bedrifts- og sektorovergripende konsekvenser, vil de eksterne kostnadene ved bortfall kunne være betydelig større enn kostnaden for den bedriften der funksjonssvikten inntreffer. Her vil det være sprik mellom bedriftens snevre økonomiske interesser og samfunnets interesser, noe som kan motivere myndighetsinngrep. Det kan enten skje via lovregulering, offentlig overtakelse, offentlige kjøp av bedriftsøkonomisk ulønnsomme tjenester, eller offentlige tiltak som gjør at bedriftens og samfunnets interesser blir sammenfallende. Sistnevnte kan skje ved at bedriften pålegges en straff som reflekterer de eksterne kostnadene for manglende beredskaps- og sikkerhetstiltak, ordninger tilsvarende KILE, eller ved positive økonomiske incentiver som fanger opp verdien for andre enn den utførende bedriften av slike tiltak. Det vil imidlertid bare være offentlige kjøp og positive økonomiske incentiver som fører til en såkalt vinn-vinn-situasjon.

Hensynet til forutsigbarhet og like rammebetingelser i markedet kan bli et hinder for staten til å pålegge én enkelt virksomhet sikkerhets- og beredskapstiltak som ivaretar andre sikkerhets- og beredskapshensyn enn de som omfattes av virksomhetens ansvar. Grensene for en virksomhets ansvar for sikkerhets- og beredskapstiltak vil først og fremst bli tydeliggjort i forbindelse med erstatningssaker. Det vil i slike saker bli vurdert hvor grensene for aktsomhet går, både i forhold til virksomhetens egen drift og i forhold til de konsekvenser uaktsomhet kan ha for samfunnet for øvrig.

Virkemidlene for å ivareta hensynet til rikets sikkerhet og vitale nasjonale interesser må være til beste for samfunnet. Målet må være å skape en vinn-vinn situasjon slik at sikkerhet og beredskap blir lønnsomt. Det er utvalgets oppfatning at dette kan gjøres gjennom ulike former for offentlig-privat-samarbeid.

På bakgrunn av ovennevnte mener utvalget at det er behov for en statlig tilskuddsordning. Ordningen må være rettet mot tiltak som klart faller utenfor virksomhetens eget ansvar og som anses nødvendig av hensyn til rikets sikkerhet og vitale nasjonal interesser. En tilskuddsordning vil bøte på mangler i dagens system gjennom:

- Å sikre at tverrsektorielle tiltak uten en hovedinteressent blir igangsatt og fulgt opp.
- Å bidra til å finansiere den statlige delen i en risikofordeling mellom offentlige og private interessenter.
- Å finansiere nødvendige sektorovergripende tiltak og følge opp sektorovergripende infrastrukturer.
- Å ivareta et helhetlig perspektiv og følge opp tiltak ut i fra både hensynet til sikkerhet mot villede- og ikke-villede uønskede hendelser.

Det bør være en forutsetning for å motta et slikt tilskudd at det kan dokumenteres et reelt behov gjennom en ROS-analyse. Det bør i denne forbindelse forutsettes at det er myndighetene som initierer hvilke tiltak som skal gis tilskudd. Det bør også være en forutsetning at tiltak finansieres gjennom en kostnadsdeling.

Redundans i tele- og kraftsystemer, spesielle kriseledelseslokaler, nasjonal analysekapasitet for deteksjon av spesielle agens i vann, drift av kryptert samband og lagre av viktige varer, er eksempler på tiltak som kan dekkes gjennom ordningen.

For å ivareta et helhetlig perspektiv, bør en tilskuddsordning forvaltes av sektorovergripende organer. I og med at det ikke alltid er sammenfall mellom sikkerhets- og beredskapsarbeid, bør en slik tilskuddsordning forvaltes av Justis- og politidepartementet.

Utvalget mener tilskudd bør fordeles på to nivåer, én fordeling innenfor «samvirkeområder» og én til sektorovergripende tiltak. Inndelingen av samvirkeområder kan være sektoriell, faglig eller geografisk. En sektoriell inndeling av samvirkeområdene vil kunne bryte med ansvarsprinsippet, og forholdet til sektoransvarlige myndigheters ansvar må derfor vurderes spesielt. Utvalget kan dessuten ikke se at faglige hensyn ivaretas i tilstrekkelig grad ved en geografisk inndeling av samvirkeområder. For å ivareta ansvarsprinsippet, faglige hensyn og hensynet til fleksibilitet i fordelingen av midlene, bør inndelingen av samvirkeområder være faglig og av tverrsektoriell karakter. Inndelingen i samvirkeområder bør vurderes nærmere, og ta utgangspunkt i politiske mål og prioriteringer. Herunder bør koblingen til eksisterende samvirkeområder vurderes. Eksempler på samvirkeområder kan være:

- Energiforsyning
- Olje- og gassikkerhet

- Elektronisk kommunikasjon
- Vannforsyning
- Transport
- Virksomheter med farlige stoffer
- Vern av sivilbefolkningen
- Lokal og nasjonal kriseledelse
- Informasjonsberedskap

For øvrig viser utvalget til at en tilsvarende tilskuddsordning er etablert i Sverige og forvaltes av Krisberedskapsmyndigheten (KBM).[5]

6.6.4 Forslag knyttet til offentlige innkjøp

Etter utvalgets mening bør det offentlige gå foran med et godt eksempel i utviklingen av en sikkerhetskultur i Norge. I virksomheter med god sikkerhetskultur, vil det være naturlig å etterspørre sikkerhet. Det offentlige og næringslivet møtes også i markedet. Stat og kommuner er store kunder i Norge. Det offentlige kjøper årlig inn varer og tjenester for flere milliarder kroner. Det kan stilles spørsmål ved hvorvidt det offentlige i dag i tilstrekkelig grad er aktive nok med hensyn til å spesifisere og kreve tilstrekkelig nivå på sikkerhet og beredskap ved sine anskaffelser. Dette vil være av avgjørende betydning dersom det gjelder anskaffelser som har betydning for rikets sikkerhet og vitale nasjonale interesser.

Etter utvalgets mening bør det derfor være et krav at det ved offentlige innkjøp skal vurderes sikkerhets- og beredskapsmessige konsekvenser ved bortfall av de varer og tjenester som leveres. Det må herunder også stilles krav til sikkerhet og beredskap i forhold til underleverandører.

6.6.5 Forslag knyttet til bruk av standarder og standardiserte metoder

Standarder beskriver et produkt, et system eller en arbeidsprosess, eller deler av disse. En standard er et forslag til valg av alternativ, men utelukker ikke andre løsninger. Det som kjennetegner åpne standarder[6] er at de utarbeides av interessegrupper som ønsker felles spilleregler i markedet. Prosessen er basert på prinsipper om åpenhet, frivillighet og konsensus. Dette betyr at alle som ønsker det kan delta, enten det er bedrifter, myndigheter, forskningsinstitusjoner, forbrukere, arbeidstakere, m.v. Siktemålet med alt standardiseringsarbeid er å oppnå enighet mellom de ulike interessenter.

Standarder kan brukes som spesifikasjon av krav og retningslinjer til produkter, tjenester og prosesser. Innenfor sikkerhet og beredskap kan standarder nyttes på følgende måter:

- Som virkemiddel for å oppfylle myndighetenes regelverk, for eksempel beskrivelser som grunnlag for oppfølging av nasjonale lover og forskrifter, spesifikasjoner ved offentlig anbud, mv.
- Som ledelsesverktøy for å ivareta kvalitet, helse, miljø og sikkerhet.
- For å sikre like konkurransevilkår, kjente spilleregler og forutsigbarhet, herunder spesifikasjoner ved kjøp og salg, retningslinjer for krav til produkter og tjenester, mv.
- For å harmonisere kvalitetskrav mellom de gjensidig avhengige virksomheter.
- For å sikre effektiv drift og økt lønnsomhet.
- Som underlag for samsvarsbedømming og tilsyn, herunder regler for prøving, sertifisering og akkreditering.

Det påpekes at en standard er frivillig å bruke. Det er imidlertid ikke uvanlig at standarder adopteres som en del av regelverket innenfor et område, blant annet ved at regelverket peker på en bestemt standard som oppfyller de regler som er satt.[7]

Personopplysningsforskriftens kapittel om informasjonssikkerhet er et eksempel på samspillet mellom forskriftsbestemmelser og standarder. Utgangspunktet for disse bestemmelsene er ISO 17799 om administrasjon av informasjonssikkerhet. Det finnes i dag en sertifiseringsordning i forhold til denne standarden, og Datatilsynet anser at virksomheter som har slik sertifisering også oppfyller bestemmelsene i forskriften.

Det er utviklet en rekke standarder nasjonalt og internasjonalt som kan være nyttige i forhold til sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner. I tillegg er det igangsatt en rekke standardiseringsprosjekter som kan ha relevans i forhold til dette området, blant annet er det satt i gang et arbeid for å utvikle en standard for kriseberedskap.

---

[5] KBM fordeler årlig tilskudd på i størrelsesorden 2 mrd. SEK til sikkerhets- og beredskapstiltak innenfor 6 områder: Kritisk infrastruktur, sentralforvaltningen, finanssektoren, transportsektoren, telesektoren (Post- og telestyrelsen fordeler midlene som mottas fra KBM) og energisektoren (sikkerhet og beredskap finansieres både av midler fra KBM og gjennom avgifter). Midlene fordeles på bakgrunn av søknader fra aktørene. Søknadene må også inneholde en ROS-analyse.

[6] Utvalget drøfter ikke proprietære standarder.

[7] Standard Norge (SN) er en medlemsorganisasjon som utvikler standarder på de fleste områder. Et annet eksempel er Norsk elektroteknisk komité (NEK) som lager alle standarder/normer for elektrisitet.

Den vellykkede integreringen av helse, miljø og sikkerhet (HMS) i næringslivet har delvis vært mulig fordi behovet for dette har vært så tydelig og delvis fordi det er utviklet gode standarder på området. Denne utviklingen må også tilskrives effektiv tilsynsvirksomhet og økt fokus på HMS som følge av alvorlige ulykker. I dag er HMS en integrert del av all forretningsdrift, og etter hvert går flere bedrifter over fra en «oppfølgingskultur» til en sikkerhetskultur (fra en reaktiv til en proaktiv virksomhetskultur). En standard for sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner kan bidra til å etablere et internasjonalt rammeverk for å identifisere og vurdere risikoer og sårbarheter, samt retningslinjer for fysisk og logisk sikring mot villede hendelser, utarbeidelse av kriseplaner og planer for driftskontinuitet, øvelser og andre tiltak for å bedre evnen til å handtere kriser. En slik standard bør også inneholde retningslinjer for egenkontroll og revisjon.

Innenfor HMS har tilnærmet alle virksomheter krav om å:

> [...] kartlegge farer og problemer og på denne bakgrunn vurdere risiko, samt utarbeide tilhørende planer og tiltak for å redusere risikoforholdene, jf. internkontrollforskriften § 5, 6.ledd.

For virksomhetene innebærer dette at det må gjøres en risikoanalyse for å avdekke risiko for deretter å iverksette tiltak som skal redusere risikoen. Dette skal dokumenteres skriftlig og blir fulgt opp gjennom tilsyn. Det er ikke krav til spesielle metoder, men Norsk Standard 5814 for risikoanalyse blir som oftest benyttet. Etter det utvalget kjenner til anbefaler blant annet Næringslivets sikkerhetsorganisasjon sine medlemmer at de også skal integrere sikring mot villede hendelser i sine risikoanalyser. De mest sikkerhetsbevisste virksomhetene og de virksomhetene som stilles overfor krav fra blant annet kunder gjør dette.

Etablering av et system med standarder og sertifiseringsordninger vil kunne være et virkemiddel for å heve kvaliteten på sikkerhets- og beredskapsarbeidet, samt være et bidrag til forenklet regulering på dette området. Det vil også kunne gjøre det lettere å etterspørre sikkerhet i markedet.

Med bakgrunn i ovennevnte vil utvalget anbefale at det etableres et forprosjekt som beskriver nærmere hvordan standarder kan bidra til sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner i Norge. I denne sammenheng vil det være viktig å delta aktivt i forhold til internasjonalt standardiseringsarbeid. Arbeidet bør i størst mulig grad bidra til å forenkle oppfølgingen av regelverk på området, og dette forutsetter at myndighetene må bidra aktivt i forhold til å definere mål, rammer og nivå på sikkerhetstilstanden for slike standarder.

Utvalget vil understreke viktigheten av at standardiseringsorganisasjonenes arbeid på dette området videreføres og at dette arbeidet skjer i nær dialog med aktuelle aktører. I den forbindelse finner utvalget grunn til å påpeke viktigheten av at dette arbeidet følges opp i tilstrekkelig grad av ansvarlige myndigheter.

6.6.6 Forslag knyttet til samarbeid og informasjonsdeling

Under utvalgets arbeid er det kommet frem ulike synspunkter på formidling og tilretteleggingen av trussel-, risiko- og sårbarhetsinformasjon. I møter med utvalget har flere virksomheter etterlyst mer regelmessig kontakt med etterretnings- og sikkerhetstjenestene og konkrete råd om hvordan de skal forholde seg til den informasjonen som formidles. Samtidig har virksomhetene selv relevant informasjon og kompetanse som er nyttig å dele med andre, også myndighetene.

Utvalget viser til at manglende kontakt mellom myndighetenes sikkerhets- og etterretningsorganisasjoner og private virksomheter kan bety at det etter hvert utvikler seg et større marked for private sikkerhets- og etterretningsfirmaer. Utvalget vil advare mot en for stor privatisering av etterretnings- og sikkerhetstjenester, og understreker betydningen av at sikkerhets- og etterretningsorganisasjoner er underlagt demokratisk kontroll. Dette kan etter utvalgets vurdering kun gjøres ved at staten har ansvaret for disse tjenestene. I Norge er de tre sikkerhets- og etterretningsorganisasjonene underlagt Stortingets kontroll gjennom det såkalte EOS-utvalget.

Utvalget vil understreke viktigheten av samarbeid og dialog mellom det offentlige og det private om sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner. Eiere og driftsansvarlige i slike virksomheter er alle opptatt av at fornuftige beslutninger skal fattes på bakgrunn av innhentet og bearbeidet informasjon. I en slik sammenheng vil informasjon om sårbarheter og kunnskap om trussel- og risikobildet være en helt nødvendig forutsetning.

Formidling av etterretnings- og sikkerhetsvurderinger er etter utvalgets mening et viktig virkemiddel for sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner. De sentrale myndighetsorganene vil være primærleverandører av informasjon om trusselsituasjonen, mens informasjon fra virksomhetene er avgjørende for vurderin-

ger knyttet til sårbarhets- og risikobildet. Det er derfor viktig at de ulike interessene ivaretas på en god måte.

Det er imidlertid ikke sikkert at all relevant informasjon deles. Det kan skyldes virksomhetens egne ansvarsbetraktninger knyttet til erstatningsansvar som følge av påført skade eller tap, eller usikkerhet om hvorvidt informasjonen blir godt nok ivaretatt.

For myndighetene er det en plikt til å beskytte informasjon som er sikkerhetsgradert. Denne type informasjon kan bare formidles til virksomheter som er omfattet av sikkerhetsloven, som har implementert foreskrevne tiltak for å kunne beskytte informasjonen og hvor de ansatte i nødvendig utstrekning er sikkerhetsklarert. Sikkerhetsgradert informasjon skal bare deles med de som har et saklig behov for tilgang til den[8], Det bør imidlertid forutsettes at myndighetene ikke holder tilbake informasjon som kan bidra til å redusere trussel-, risiko- og sårbarhetsnivået i samfunnet fra de virksomhetene som har de nødvendige virkemidlene for å gjøre noe med dette. Informasjonen må likevel legges til rette slik at virksomhetene får informasjon som kan dekke deres behov uten at sikkerhetsgraderte eller andre særlig sensitive opplysninger spres. Det vil uansett være viktig å vektlegge betydningen av tette relasjoner og tillit innenfor et samarbeid om deling av informasjon. Samarbeidet må altså være slik innrettet at ulike problemstillinger kan tas opp konfidensielt, samtidig som interessene til den som formidler informasjonen vernes.

Utvalget viser til sårbarhetsutvalgets forslag i NOU 2000:24 Et sårbart samfunn, kapittel 22, der det blant annet fremgår:

> Et koordineringsorgan bør gis følgende ansvar og funksjoner:
> - Være et bindeledd mellom sivile myndigheter og EOS-tjenestene.
> - Innhente og prioritere sivile myndigheters behov for informasjon fra etterretnings-, overvåkings- og sikkerhetstjenestene. Når det gjelder bidrag fra Forsvarets etterretningstjeneste må dette som hovedregel tas opp med Forsvarssjefen eller Forsvarsdepartementet.
> - Samle inn og bearbeide informasjon om aktuelle sårbarhets- og trusselvurderinger fra EOS-tjenestene, Kripos, Økokrim, Tollvesenet, Utenriksdepartementet, Direktoratet for sivilt beredskap og Senter for informasjonssikring (kapittel 6), og gjøre dette tilgjengelig for overordnet statsråd og andre relevante statsråder og departementer. Koordineringsorganet må selv vurdere behovet for råd og informasjon fra andre miljøer.
> - Foreta fortløpende vurderinger og gi anbefalinger om eventuelle tiltak til de berørte statsråder i forhold til etterretningstrusselen.
> - Ta nødvendige initiativ overfor alle aktuelle departementer.
> - Anbefale kriterier som bør legges til grunn for beskyttelse av informasjon og objekter.

I forlengelse av sårbarhetsutvalgets forslag, mener utvalget at koordineringen av etterretnings- og sikkerhetstjenestene bør styrkes ytterligere. Det vises i denne sammenheng til det ansvar og de oppgaver som er tillagt Koordineringsutvalget for etterretnings- og sikkerhetstjenestene (KRU), jf. kapittel 4. Utvalget anser KRU og etableringen av det faste sekretariatet for dette utvalget som en delvis oppfølging av sårbarhetsutvalgets forslag knyttet til koordineringen av etterretnings- og sikkerhetstjenestene.

Utvalgets anbefalinger

Utvalget anbefaler en styrking av samarbeid og informasjonsdeling knyttet til sikkerhet og beredskap, særlig mellom virksomheter med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner. Dette gjelder både innenfor, og på tvers av, offentlig og privat sektor. Utvalget vil også understreke viktigheten av bransjesamarbeid på dette området, herunder den viktige rollen organisasjonene kan spille i dette arbeidet.

Utvalget anbefaler at det etableres et tettere og mer forpliktende samarbeid mellom de sentrale myndighetene med ansvar for overordnede trussel-, risiko og sårbarhetsvurderinger. Dette samarbeidet må i det minste inkludere PST, NSM og DSB. Det kan tenkes ulike løsninger for samarbeid og informasjonsformidling, alt etter hvor viktig informasjonen er, eller hvor mye det haster å formidle den.

Et slikt samarbeid kan for eksempel etableres innenfor rammene av KRU. Det kan vurderes en ordning med sekondering fra de aktuelle myndighetsorganene i KRUs permanente sekretariat. KRU bør i tillegg styrke sin koordinerende rolle ved å tilrettelegge for at etterrettelig informasjon om trusler, risikoer og sårbarheter tilkommer alle aktuelle aktører med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner på en forståelig og handlingsorientert måte, til lik tid og uten unødig opphold. Utvalget mener for øvrig at forholdet mellom KRU og DSB bør styrkes, for eksempel

[8] Det såkalte *need to know*-prinsippet

ved at organet utvides med en representant fra DSB.

En annen løsning kan være å etablere et permanent samordningsorgan på direktoratsnivå bestående av personell som sekonderes fra NSM, DSB og PST. Disse direktoratene ivaretar alle sentrale roller knyttet til sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner, og det synes naturlig at direktoratene ivaretar et felles ansvar for samarbeidsorganet. Alle de tre direktoratene er faglig underlagt Justisdepartementet, og etableringen av et slikt organ vil tydeliggjøre Justisdepartementets koordinerende ansvar knyttet til sikringen av kritisk infrastruktur.

Når det gjelder hvordan DSB, NSM og PST skal samarbeide, kan det vises til erfaringene fra National Infrastructure Security Co-ordination Center (NISCC) i Storbritannia.[9] Selv om NISCCs oppgaver primært retter seg mot logisk sikring av kritisk infrastruktur, har den organisatoriske modellen overføringsverdi til norske forhold og sikring av kritisk infrastruktur generelt. Det synes ikke å være sterke grunner for å skille mellom samarbeidsorganer knyttet til fysisk og logisk sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner.

NISCC er bygget opp ved at ressurser og kompetanse fra ulike etater og virksomheter er samlet. En slik modell har flere likhetstrekk med vårt eget Varslingssystem for digital infrastruktur (VDI) som ble etablert gjennom et samarbeidsprosjekt mellom NSM, PST og E-tjenesten. Erfaringene fra Storbritannia tilsier at effektiv sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner bare kan oppnåes gjennom et organisatorisk samarbeid mellom overordnede fagmiljøer.

Det bør vurderes om organet skal forankres administrativt i et av de tre direktoratene. Det bør være et mål å se fysisk og logisk sikring av kritiske infrastruktur og kritiske samfunnsfunksjoner i sammenheng. Representasjon fra andre samarbeidende tjenester kan også vurderes, for eksempel Post- og teletilsynet, Norges vassdrags- og energidirektorat, mv.

Det må forutsettes at målet med formidling av trussel-, risiko- og sårbarhetsinformasjon fra sentrale myndigheter, er at informasjonen blir fulgt opp på en effektiv måte i de berørte virksomhetene. Dette vil ikke minst være viktig i de situasjoner hvor det er aktuelt å heve trusselnivået, og hensynet til rikets sikkerhet og vitale nasjonale interesser tilsier raskest mulig oppfølging. Ulike ståsteder kan gjøre at bedrifter ikke uten videre følger opp myndighetsinformasjonen med de handlinger myndighetene finner hensiktsmessige ut fra samfunnets behov. Et effektivt system for kontroll med oppfølgingen av den informasjonen som er gitt, vil derfor være en nødvendig forutsetning for å kunne uttale seg om det faktiske sikkerhets- og beredskapsnivået ved en trusselsituasjon.

Det anbefales at det etableres møteplasser der offentlige og private virksomheter drøfte hva det aktuelle trussel-, risiko- og sårbarhetsbildet har å si for deltakerne, hvilke handlingsalternativer som kan og bør iverksettes, samt oppfølgingen av iverksatte tiltak. Utvalget har ikke vurdert eksisterende møteplasser for denne typen samarbeid, men anbefaler at de tre etterretnings- og sikkerhetstjenestene samt DSB vurderer dette sammen.

En forutsetning for å etablere slike møteplasser er at sikkerhetsloven er gjort gjeldende for alle de virksomheter som deltar, og at alle som har behov for tilgang til slik informasjon har den nødvendige sikkerhetsklarering. Informasjonen til aktørene bør derfor kunne deles i både en ugradert og en gradert versjon om nødvendig, slik at det ikke foretas unødvendige personklareringer.

[9] Det er dessuten etablert et *Joint Terrorism Analysis Centre* (JTAC) i Storbritannia. JTAC skal forbedre samordningen mellom de ulike tjenestene og statlige organene som har sentrale roller i terrorbekjempelse i Storbritannia. Tilsvarende organer er også etablert, eller er under etablering, i en rekke andre land.

Kapittel 7
Sikkerhetsloven og den forebyggende sikkerhetstjenesten

7.1 Bakgrunn for Lov om forebyggende sikkerhetstjeneste

Ved behandlingen av St.meld. nr. 39 (1992-93) Om overvåkingstjenesten, besluttet Stortinget 18. juni 1993 å styrke den parlamentariske kontrollen ved å opprette et eget kontrollorgan som skal føre kontroll og tilsyn med EOS-tjenestene.

Den såkalte Skaugekommisjonen ble oppnevnt ved kgl. res. av 24. sept. 1993, og fikk til oppgave å utrede og klargjøre de spørsmål som etableringen av et slikt felles kontrollutvalg reiser. Kommisjonen anbefalte på denne bakgrunn at det iverksettes arbeid med sikte på å gi en egen lov om EOS-tjenestene, dvs. om deres organisering, oppgaver og beføyelser. Lovgrunnlaget skulle også hjemle kontroll med tjenestene. Ifølge kommisjonen ville hovedhensikten med en slik lovgivning være å bedre tilliten til tjenestene, skape klarhet om grensene mellom tjenestene og forenkle kontrollen med disse.

Lov av 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven) trådte i kraft 1. juli 2001 sammen med en rekke utfyllende forskrifter. Regelverket erstatter et tidligere sett av fagspesifikke instrukser på området som kun gjaldt for statsforvaltningen.

7.1.1 Lovens formål. Ansvar og utførelse

Sikkerhetsloven har som formål å redusere risiko for sikkerhetstrusler som spionasje, sabotasje og terrorhandlinger gjennom forebyggende defensive tiltak. Disse tiltakene gjennomføres i det alt vesentlige i virksomhetene lokalt, gjennom for det første utvelgelse av informasjon og objekter som trenger beskyttelse ut fra en vurdering av deres betydning for rikets sikkerhet og selvstendighet og andre vitale nasjonale sikkerhetsinteresser.

For det andre gjennomfører virksomhetene forebyggende defensive tiltak ved å iverksette beskyttelsestiltak som innebærer barrierer, deteksjon, reaksjon og gjenoppretting i forhold til anslag eller forskjellige former for sviktsituasjoner som kan tenkes å oppstå. I det daglige iverksettes tiltakene som minimumstiltak. I situasjoner hvor trusselbildet tilsier det, skal virksomhetene iverksette påbyggingstiltak som i størst mulig grad er forhåndsplanlagt og øvet.

Et annet viktig formål med sikkerhetsloven er å ivareta den enkeltes rettssikkerhet. En del av de forebyggende sikkerhetstiltakene kan være meget inngripende overfor enkeltpersoner. Enkelte tiltak er også av en slik art at de kan misbrukes og rettes mot enkeltpersoner. Samfunnet har derfor funnet det nødvendig å underkaste den forebyggende sikkerhetstjeneste særskilte kontrollmekanismer utover de som på generelt grunnlag er etablert for forvaltningen gjennom Riksrevisjonen, sivilombudsmannen og ombudsmannen for Forsvaret. Denne særskilte kontrollen er hjemlet i en egen lov og utøves av et utvalg (EOS-utvalget), nedsatt av Stortinget.

Gjennom at den offentlige myndighetsutøvelse i forhold til personkontroll er regulert i lov vil dette, sammen med det særskilte kontrollorganet som er nevnt over, bidra til å styrke rettssikkerheten på dette området. Det samme gjelder for de øvrige delene av den forebyggende sikkerhetstjeneste. Lovens tredje formål (å «trygge tilliten til og forenkle grunnlaget for kontroll med forebyggende sikkerhetstjeneste») vil dermed også kunne oppfylles.

Nasjonal sikkerhetsmyndighet (NSM) har som generelle oppgaver å koordinere de forebyggende sikkerhetstiltak og å kontrollere (føre tilsyn med) sikkerhetstilstanden. Med koordinering menes her først og fremst det å gi informasjon, råd og veiledning, samt foreslå forbedrede tiltak. Sikkerhetstilstanden kontrolleres ved forskjellige former for tilsyn. I tillegg skal NSM utføre en rekke konkrete myndighetsoppgaver som følger av loven og forskriftene til loven, herunder sikkerhetsklareringer, godkjenninger, sertifiseringer osv.

Forsvarsdepartementet og Justis- og politidepartementet er overordnede departementer etter loven for henholdsvis militær og sivil sektor av samfunnet, jf kronprinsregentens resolusjon av 4. juli 2003. Forsvarsdepartementet er i tillegg regelverksforvalter for sikkerhetsloven med utfyllende forskrifter. Etatsstyringen av NSM tilligger Forsvarsdepartementet. NSM rapporterer om sikker-

hetstilstanden i militær og sivil sektor til respektive departementer.

7.1.2 Hva er forebyggende sikkerhetsarbeid?

Sikkerhetstjenestens oppgave er defensiv og forebyggende, ved at sikringstiltakene i prinsippet gjennomføres i forebyggende hensikt, uavhengig av konkrete mistanker om sikkerhetstrusler.

Et fundamentalt prinsipp innen sikkerhetstenkning er at ikke alt er like vesentlig å beskytte. Dette innebærer at man må utvikle systemer for ikke bare å kunne identifisere hva som har sikkerhetsmessig verdi, men også kunne klassifisere det i forhold til andre sammenlignbare verdier. Denne klassifiseringsprosessen er en utfordring så vel å utvikle som å etterleve når konkrete verdier skal klassifiseres.

Sikkerhetslovens forebyggende defensive tiltak inngår som et viktig ledd i den samlede innsats for å sikre et robust og trygt samfunn. Som komplementære tiltak til sikkerhetslovens barrierer, deteksjons-, gjenopprettings- og skadebegrensningstiltak finner vi a) offensive forebyggende tiltak som ivaretas av Politiets sikkerhetstjeneste (PST), b) polisiære beskyttelsestiltak i spesielle situasjoner (eventuelt med støtte av militære avdelinger), c) etterforsking og påtale d) beredskapsmessige forberedelser for håndtering av skade på person, materiell og miljø og e) forebyggende tiltak på HMS-området.

Sikkerhetslovens tiltak inngår også i en annen dimensjon hvor andre (og mindre krevende) sikkerhetstiltak utfyller bildet. Sikkerhetsloven ivaretar nasjonale hensyn. Nedslagsfeltet er informasjon og objekter av betydning for rikets sikkerhet og selvstendighet og andre vitale nasjonale sikkerhetsinteresser. Nedenfor disse finner vi tiltak som søker å ivareta sikkerheten for enkeltvirksomheter og enkeltmennesket enten det dreier seg om informasjonssikkerhet eller objektsikkerhet.

7.1.3 Rikets sikkerhet og vitale nasjonale sikkerhetsinteresser

Begrepene «rikets sikkerhet» og «vitale nasjonale sikkerhetsinteresser» benyttes i lovteksten. Disse (og lignende) begreper benyttes i flere sammenhenger der sikkerhet for samfunnet omtales.

Selv om begrepene etter hvert er blitt innarbeidet i lover og forskrifter, er ikke meningsinnholdet gitt noen «autoritativ» beskrivelse. Forholdet er snarere at man erkjenner at begrepene ikke er statiske. Endringer i samfunnet, i trusselbildet og sårbarheter bidrar til at det blir behov for å oppdatere hva som bør legges i begrepene.

Begrepet «vitale nasjonale sikkerhetsinteresser» kom med sikkerhetsloven. Hensikten med å innføre begrepet var «å bli kvitt den skjønnsmessige formuleringen om å gradere opplysninger av sikkerhetsmessig verdi».[1] Det understrekes i proposisjonen at det ligger i begrepet andre vitale nasjonale sikkerhetsinteresser, ut fra ordlyden, en klar indikasjon på at dette bare gjelder helt avgjørende og samfunnsviktige sikkerhetsinteresser. Og videre:

> Den detaljerte tolkningen av begrepet må på vanlig måte, i likhet med forståelsen av begrepet 'rikets sikkerhet', overlates til å finne sin presise avklaring gjennom forvaltningspraksis, juridisk teori, domstolspraksis, uttalelser fra Stortingets ombudsmann for forvaltningen osv.

Det vises ellers til drøftingen av disse begrepene i kapittel 3.

7.2 Om lovens virkeområde

Sikkerhetsloven gjelder i utgangspunktet for forvaltningsorganer i stat og kommune. I forarbeidene til loven heter det at begrepet «forvaltningsorgan» skal tolkes på samme måte som etter forvaltningslovens §1 og offentlighetslovens §1. Loven sier at Kongen i tvilstilfelle kan bestemme om et organ er å regne som forvaltningsorgan.[2]

Utviklingen med endring av selskapsform for en del tidligere forvaltningsorganer var godt i gang på det tidspunkt lovforslaget ble fremmet. Både offentlig og privateide aksjeselskaper kan vise seg å besitte skjermingsverdige objekter og sikkerhetsgradert informasjon. Ut fra de alvorlige skadevirkninger som for eksempel kan oppstå dersom uvedkommende får kjennskap til slik informasjon, mente Forsvarsdepartementet at det var rimelig at de samme sikkerhetsregler måtte gjelde dersom skjermingsbehovet var likt, uavhengig av den rettslige status til den virksomhet dette angikk.

I stedet for å angi i loven hvilke konkrete private virksomheter eller enkeltpersoner som skulle omfattes av loven eller å gjøre lovens virkeområde generelt, ble det foreslått at Kongen skulle kunne

[1] Ot.prp. 49 (1996-97) *Om lov om forebyggende sikkerhetstjeneste (sikkerhetsloven)*, side 35.

[2] I tilfellet med Avinor AS kom Samferdselsdepartementet og Justis- og politidepartementets lovavdeling til at både offentlighetsloven og forvaltningsloven kom til anvendelse på Avinor AS som sådan. Forsvarsdepartementet la etter dette til grunn at Avinor AS rettslig sett var å regne som forvaltningsorgan og dermed omfattet av sikkerhetsloven.

bestemme hvilke andre rettssubjekter enn forvaltningsorganer og leverandører loven skal gjelde for (helt eller delvis). Denne myndigheten er senere gitt til Forsvarsdepartementet jf. kgl. res. av 27. juni 2003.

7.2.1 Har loven et tilstrekkelig virkeområde i dag?

Lovens formål er i utgangspunktet å legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet, og andre vitale nasjonale sikkerhetsinteresser.

Begrepet «vitale nasjonale sikkerhetsinteresser» er nærmere drøftet ovenfor. Innholdet i dette begrepet har endret seg over tid. I tråd med utviklingen til det samfunnet vi har i dag, er det en alminnelig oppfatning at vitale nasjonale sikkerhetsinteresser omfatter funksjonsdyktigheten til den kritiske infrastrukturen og de kritiske samfunnsfunksjonene i samfunnet.

Utviklingen går i retning av en stadig sterkere liberalisering når det gjelder eierskap til virksomheter som har ansvar for store deler av den kritiske infrastrukturen og de kritiske samfunnsfunksjonene. I praksis innebærer dette at virkeområdet for loven om forebyggende sikkerhet for samfunnet blir stadig snevrere.

I noen grad kompenseres dette ved at lovens mulighet til å bestemme om utvidelse av virkeområdet benyttes. For en del virksomheter er rettstilstanden noe uklar. Dette gjelder statsaksjeselskaper som fortsatt har enkelte forvaltningsoppgaver, og det gjelder for statsforetak.

På enkelte områder (typisk innen finanssektoren) har loven eller tidligere tilsvarende bestemmelser aldri hatt rekkevidde.

To forhold er viktig å bemerke i forhold til at lovens virkeområde slår så forskjellig ut. For det første at lovbestemmelser om forebyggende sikkerhet ikke virker innenfor hele det området som det ville være naturlig å beskytte med disse bestemmelsene. For det andre vil det faktum at loven gjøres gjeldende for enkelte privatrettslige virksomheter kunne føre til ulike forretningsmessige konsekvenser i forhold til andre i markedet.

Det kan virke unaturlig at mens sektorvise lover, forskrifter og bestemmelser normalt ikke diskriminerer mellom forvaltningsorganer, offentlige eide aksjeselskaper og rene privateide virksomheter, gjelder den tverrsektorielle sikkerhetsloven i utgangspunktet bare for visse virksomhetstyper.

7.2.2 Privatrettslige virksomheter som er omfattet av sikkerhetsloven

Etter at Forsvarsdepartementet fikk delegert myndigheten til å gjøre enkeltvedtak om utvidelse av lovens virkeområde, har dette vært gjort for noen virksomheter. I tilfellet med Avinor AS var ikke dette nødvendig, da virksomheten ble definert å være et forvaltningsorgan.

Til i dag er det gjort vedtak om at sikkerhetsloven skal gjøres gjeldende for følgende privatrettslige virksomheter som ikke er forvaltningsorganer:

- Senter for informasjonssikring (SIS)
- CargoNet AS
- Posten Norge AS
- Telenor ASA
- NSB AS

En rekke private virksomheter innen jernbanesektoren og sivil luftfart er til vurdering i Forsvarsdepartementet.

I tillegg til de virksomheter som loven gjøres gjeldende for ved enkeltvedtak, vil en del virksomheter bli omfattet av tiltak i loven når de leverer varer eller tjenester som omfattes av kapittelet i loven om sikkerhetsgraderte anskaffelser (se kapittel 7.3.5).

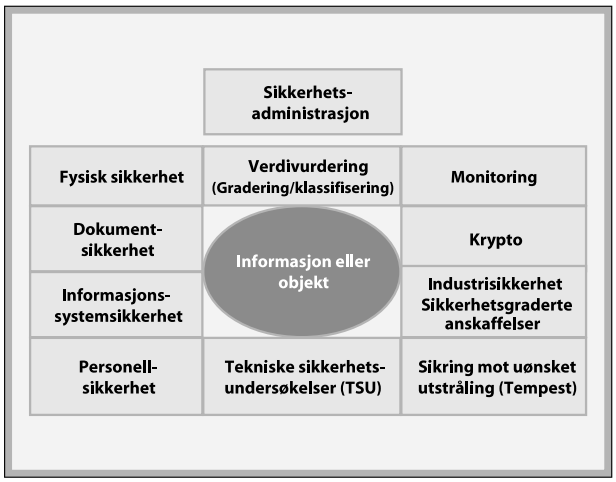
7.3 De sentrale elementene som utgjør virkemidlene i loven

Sikkerhetsloven er i seg selv et viktig virkemiddel for å gi et nødvendig rammeverk for det forebyggende sikkerhetsarbeidet. For de virksomheter og organer loven gjelder for bidrar den også til at det faktisk utføres et forebyggende sikkerhetsarbeid mot sikkerhetstruende virksomhet.

Loven med tilhørende forskrifter regulerer og gir (til dels detaljerte) bestemmelser om hvordan skjermingsverdig informasjon skal beskyttes. Når det gjelder skjermingsverdige objekter er det foreløpig ikke gitt utfyllende bestemmelser i forskrifts form.

Figur 7.1 gir en oversikt over de virkemidler og fagområder som finnes innen den forebyggende sikkerhetstjeneste.

Forskrift om sikkerhetsadministrasjon skal sikre at gjennomføringen av lovens kapittel 2 om ansvar for og utøvelse av forebyggende sikkerhetstjeneste blir ivaretatt på en best mulig måte[3]. Den enkelte virksomhets sikkerhetsadministrasjon skal samordnes og ses i sammenheng med forhold



Figur 7.1 Virkemidler og fagområder innen den forebyggende sikkerhetstjeneste.

Kilde: Nasjonal sikkerhetsmyndighet

som skal motvirke andre tilsiktede hendelser, som for eksempel alminnelig vinningskriminalitet og skadeverk, og utilsiktede hendelser, som for eksempel naturkatastrofer og ulykker.

Virkeområdet for denne forskriften gjelder sikkerhetsadministrasjon innen og på tvers av fagområdene informasjonssikkerhet, personellsikkerhet og sikkerhetsgraderte anskaffelser.

Forskriften fastslår at det er virksomhetens leder som har det overordnede ansvaret, og at denne plikter å avsette nødvendige ressurser for å ivareta sikkerhetstjenesten. Videre gis en del bestemmelser om organiseringen av arbeidet, blant annet krav om å utpeke en sikkerhetsleder i organisasjonen.

En meget viktig del av forskriften gjelder pålegg om å utøve risikohåndtering av skjermingsverdig informasjon. Fastsetting av sikkerhetstiltak utover minimumstiltakene skal eksempelvis skje etter en risikovurdering.

Forskriften gir også en del bestemmelser om reaksjon ved sikkerhetstruende hendelser.

7.3.1 Personellsikkerhet

Lovens kapittel 6 og forskrift om personellsikkerhet regulerer gjennomføringen av personkontroll og prosessen med sikkerhetsklarering av personer som skal gis tilgang til sikkerhetsgradert informasjon. Det gis også bestemmelser om autorisasjon for faktisk tilgang til slik informasjon.

Personkontroll og sikkerhetsklarering skal gjennomføres når en person vil kunne få tilgang til skjermingsverdig informasjon som er sikkerhetsgradert KONFIDENSIELT eller høyere. For tilgang til informasjon gradert BEGRENSET kreves ikke sikkerhetsklarering, men vedkommende må være autorisert.

Loven krever altså sikkerhetsklarering for tilgang til sikkerhetsgradert informasjon. Det er ikke et tilsvarende krav for å få tilgang til skjermingsverdige objekter. Bare dersom slik tilgang vil kunne innebære tilgang til skjermingsverdig informasjon, vil kravet om sikkerhetsklarering være tilstede. Et objekt som anses skjermingsverdig ut fra sin vitale funksjonalitet i samfunnet alene kan ikke beskyttes med dette tiltaket med mindre informasjon knyttet til objektet er sikkerhetsgradert eller adgang til objektet vil kunne åpenbare sikkerhetsgradert informasjon. Kongen kan dog bestemme at klarering også kan kreves for adgang til skjermingsverdige objekter.

7.3.2 Hvem kan det kreves sikkerhetsklarering for?

En klareringsprosess kan som nevnt ovenfor iverksettes hvis en autorisasjonsansvarlig har behov for å gi en person tilgang til sikkerhetsgradert informasjon gradert KONFIDENSIELT eller høyere. Autorisasjonsansvarlig vil typisk være forvaltningsorganer. Et firma som har et gradert oppdrag for forvaltningen (eller privat rettssubjekt som er omfattet av loven) og som har behov for å oppbevare eller tilvirke gradert informasjon utenfor oppdragsgivers lokaler, vil også være autorisasjonsansvarlig etter sikkerhetsloven.

Sikkerhetsklarering alene vil ikke være et adekvat virkemiddel i forhold til beskyttelse av gradert informasjon. Bestemmelsene om informasjonssikkerhet, herunder oppbevaring og håndtering av gradert informasjon, må også kunne oppfylles. Dette forutsetter at loven gjelder for vedkommende virksomhet.

Prosessen med sikkerhetsklarering kan også iverksettes hvis enkeltpersoner vil kunne få tilgang til gradert informasjon, selv om de i prinsippet ikke skal autoriseres for tilgang. Typiske eksempler er vaktpersonale og rengjøringspersonell hvor det ut fra stillingens art er en særlig risiko for at disse kan komme over gradert informasjon.

Loven gir også Kongen adgang til å bestemme at det kreves sikkerhetsklarering for den som vil

[3] Sikkerhetsadministrasjon: Internkontroll ved gjennomføring av systematiske tiltak for å sikre at virksomhetens aktiviteter planlegges, organiseres, utføres og revideres i samsvar med krav fastsatt og i medhold av sikkerhetsloven.

kunne få tilgang til skjermingsverdig objekt. Til i dag er det ikke gitt slike bestemmelser.

En persons eller virksomhets eventuelle ønske om sikkerhetsklarering er imidlertid ikke grunn eller hjemmel for iverksettelse av sikkerhetsklareringsprosessen.

7.3.3 Forskrift om informasjonssikkerhet

Forskriften er meget omfattende og omhandler mange områder som er knyttet til beskyttelse av skjermingsverdig informasjon:

- Sikkerhetsgradering
- Tilgang til sikkerhetsgradert informasjon
- Dokumentsikkerhet
- Informasjonssystemsikkerhet, herunder sikkerhet mot utstråling (tempest)
- Fysisk sikring mot ulovlig inntrenging
- Administrativ kryptosikkerhet
- Kurerposttjeneste
- Sikring av konferanserom mot uønsket avlytting og innsyn
- Tekniske sikkerhetsundersøkelser
- Monitoring av og inntrenging i informasjonssystemer

På en rekke av disse områdene kreves i mange tilfeller spesiell godkjennelse fra NSM for at gradert informasjon kan behandles.

Hensikten med tekniske sikkerhetsundersøkelser (TSU) er ved forebyggende kontrollvirksomhet og sikkerhetstiltak å påvise sikkerhetmessig sårbarhet som kan utnyttes til uønsket avlytting og innsyn og å avdekke og motvirke forsøk på uønsket avlytting og innsyn.

Tekniske sikkerhetsundersøkelser i Forsvaret og i utenrikstjenesten kan bare utføres av NSM. For øvrig kan NSM generelt eller for det enkelte tilfelle fastsette at en bestemt type TSU kan utføres av virksomhet som bemyndiges av NSM for dette formål.

7.3.4 Forskrift om sikkerhetsgraderte anskaffelser

Bestemmelsene om sikkerhetsgraderte anskaffelser er en viktig del av det forebyggende sikkerhetsarbeidet, og omhandler hvordan sikkerhetsloven vil kunne få virkning også for virksomheter (leverandører og underleverandører) som i utgangspunktet ikke omfattes av loven.

Med leverandør forstås et rettssubjekt som ikke er forvaltningsorgan og som leverer varer eller tjenester i forbindelse med en sikkerhetsgradert anskaffelse.

Dersom en leverandør kan få tilgang til skjermingsverdig informasjon gradert KONFIDENSIELT eller høyere, eller dersom det av andre grunner er nødvendig, skal leverandøren ha gyldig leverandørklarering. I slike saker er det Nasjonal sikkerhetsmyndighet som er klareringsmyndighet.

Ved vurdering av om leverandørklarering skal gis, kan følgende opplysninger knyttet til leverandøren vektlegges:

- Økonomiske forhold, herunder muligheten for insolvens
- Eierform og eierinteresser
- Sikkerhetsmessige forhold for daglig leder og styre
- Sikkerhetsorganisasjonen
- Gjennomføring av sikkerhetstiltak i samsvar med forskriftens § 2-7
- Mulige straffbare forhold, herunder forhold som kvalifiserer til foretaksstraff
- Andre forhold som kan gi grunn til å frykte at leverandøren vil kunne opptre i strid med sikkerhetsmessige interesser

Pr. i dag er om lag 100 private virksomheter gitt leverandørklarering for KONFIDENSIELT eller HEMMELIG.

7.3.5 Om objektsikkerhet

Spesielt for objektsikkerhet er at dette er det eneste området hvor det ikke er utarbeidet forskrift med utfyllende bestemmelser. Det foreligger likevel en plikt til å utpeke og beskytte skjermingsverdige objekter. Uavhengig av disse bestemmelsene utøver en rekke etater og virksomheter et godt arbeid på objektsikkerhetsområdet. Dette er delvis regulert gjennom sektorvise bestemmelser.

Behovet for en overordnet koordinering av det forebyggende regelverk på området tas opp i forarbeidene til loven. Det uttrykkes at oppbygging av en koordinert og faglig kompetent forebyggende objektsikkerhetstjeneste nok vil være kostnadskrevende på kort sikt, men vil ved muligheten for koordinering ha et langsiktig ressurssparingspotensial.

Under arbeidet med å forberede utfyllende bestemmelser om objektsikkerhet er det vurdert hvorvidt det bør iverksettes adgang til å kunne kreve personkontroll og sikkerhetsklarering av ansatte og andre som skal få adgang til spesielt viktige objekter. En eventuell slik bestemmelse vil naturlig inngå i sikkerhetsloven eller dens forskrifter, sammen med bestemmelse om hvordan skjermingsverdige objekter skal klassifiseres. På den måten vil kravene til når sikkerhetsklarering skal

kreves bli like, og virkemiddelet i seg selv vil bli omfattet av den kontroll som allerede skjer fra EOS-utvalgets side.

7.4 Om forholdet til andre lover og (sektorvise) bestemmelser

Overordnet, tverrsektorielt regelverk eksisterer side om side med mer spesifikke bestemmelser (også i form av forskrifter) for den enkelte sektor.

På informasjonssikkerhetsområdet finnes ingen «konkurrerende» regelverk, bare tilgrensende og komplementære (dvs. ingen andre regelverk har som formål å ivareta de hensyn som sikkerhetsloven søker å ivareta). Eksempler på slikt komplementært regelverk er beskyttelsesinstruksen og personopplysningsloven.

På objektsikkerhetsområdet stiller det seg annerledes. En rekke sektorer i samfunnet har sikkerhetsbestemmelser nedfelt i lov eller forskrift som helt eller delvis kan sies å omfatte de sikkerhetshensyn som sikkerhetsloven på objektsikkerhetsområdet også søker å ivareta. Der disse hensyn fullt ut er ivaretatt i sektorbestemmelsene vil sikkerhetsloven stå tilbake for disse.

Der hensynene delvis er ivaretatt gjennom sektorbestemmelsene, vil sikkerhetsloven som tverrsektoriell standard virke reparerende, slik at det helhetlige nasjonale sikkerhetsbehovet knyttet til defensiv forebygging av spionasje, sabotasje og terrorhandlinger blir ivaretatt.

Det kan vises til (norske og) internasjonale standarder når det stilles krav i lov og forskriftsverk til de enkelte tiltakene. Bruk av, og referanse til anerkjente standarder er et viktig element for å sikre gode løsninger. Det gir et godt grunnlag for å evaluere og sammenlikne sikkerhetsnivåer hos ulike virksomheter. Standarder gjør innføring av tiltak enklere for virksomhetene, og de gjør det mulig å kommunisere med andre om hvordan løsninger skal implementeres best mulig.

Bestemmelser som tar sikte på forebyggende tiltak mot brann, eksplosjon, flom osv. diskriminerer ikke mellom ulike organisasjonsformer. Disse bestemmelsene skiller heller ikke mellom årsaker som skyldes overveide, planlagte handlinger eller naturlige årsaker, rutinesvikt eller uaktsomhet.

I noen sektorer finnes bestemmelser som tar sikte på å ivareta sikkerhet i forhold til villede, tilsiktede handlinger. De klareste eksemplene finnes innen luftfarten, sjøfarten og kraftforsyningen.

Regelverkene innen luftfart og sjøfart er begge resultat av internasjonale avtaler som Norge er forpliktet til å følge, og de enkelte bestemmelsene er ofte rene oversettelser av engelske tekster som er vedtatt i internasjonale fora som EU og IMO.

Forskrift om forebyggelse av anslag mot sikkerheten i luftfarten har som formål «å forebygge anslag mot sikkerheten i sivil luftfart» (§1). Forskriften fokuserer altså klart på tilsiktede handlinger (terrorisme, sabotasje). Selv om bestemmelsene først og fremst tar sikte på å styrke sikkerheten (liv og helse) for de reisende og ansatte på bakken og i luften, vil gjennomføring av tiltakene også ha effekt i forhold til å opprettholde flytrafikken.

Et liknende perspektiv gjelder for de forholdsvis nye bestemmelsene som er gitt for sikring av skip og havn, ISPS-koden (International Ship and Port facility Security Code). Denne har resultert i en norsk forskrift, «Forskrift om sikkerhet og terrorberedskap i norske havner». I §1 om formålet heter det: «Forskriftens formål er å forebygge og hindre terroranslag mot fartøy i internasjonal fart og mot havneterminaler som betjener slike fartøy. Den stiller krav til etablering, iverksettelse og oppfølging av sikkerhets- og terrorberedskapstiltak for norske havneterminaler».

Sikkerhetsbestemmelsene for kraftforsyningen skiller seg ut fra mange andre sektorvise bestemmelser i forhold til formålsbeskrivelsen. Med bakgrunn i energiloven ble det så tidlig som i 1991 fastsatt «Sikkerhetsbestemmelser for kraftforsyningen». Her finnes et formål som entydig retter seg mot det å sikre funksjonalitet:

> 1. Sikkerhetsbestemmelser for kraftforsyningen omhandler tiltak for sikring mot skade ved krigshandling eller sabotasje på bestående anlegg, anlegg under bygging eller planlagte anlegg som er eller trolig vil bli av betydning for landets kraftforsyning. Bestemmelsene skal hindre uvedkommende i å skaffe seg informasjon om og adgang til kraftforsyningsanlegg i den hensikt å forstyrre eller ødelegge virksomheten.

For kraftforsyningen er også utarbeidet en egen forskrift om beredskap, med en tilhørende omfattende veiledning.

Felles for regelverkene innen luftfart, skip/havn og kraftforsyning er at de (i ulik grad) refererer til bestemmelser i den tverrsektorielle sikkerhetsloven. Det gjelder først og fremst bestemmelsene om beskyttelse av informasjon (sikkerhetsgradering) og om personkontroll (sikkerhetsklarering). Det er altså en sammenheng mellom de særskilte bestemmelsene innen den enkelte sektor og de overordnede bestemmelsene om forebyggende sikkerhet, i dette tilfellet sikring av informasjon.

Sikkerhetsbestemmelsene for kraftforsyningen minner oss om at sikring av nasjonale interesser og kritisk infrastruktur ikke bare er et spørsmål om fysisk sikring av objekter, men at beskyttelse av skjermingsverdig informasjon (også gjennom personellsikkerhetstiltak) også er en viktig del av dette. Sikkerhetsloven har i dag et detaljert regelverk for dette.

Sikkerhetsloven oppfyller for så vidt en del kriterier som bør stilles til bestemmelser for sikring av den kritiske infrastrukturen. Slik loven er i dag, gis det et pålegg om å identifisere skjermingsverdige objekter og å treffe tiltak for å sikre disse. Ansvaret for dette plasseres på objekteier.

Fordi sikkerhetsloven foreløpig har svært knappe bestemmelser som gjelder objektsikkerhet, er ikke loven noen utdypende klargjøring av hva dette omfatter utover definisjonen i §3: «Skjermingsverdig objekt; eiendom som må beskyttes mot sikkerhetstruende virksomhet av hensyn til rikets sikkerhet eller alliertes sikkerhet eller andre nasjonale sikkerhetsinteresser».

To utvalg har arbeidet med forslag til utfyllende bestemmelser om objektsikkerhet. I dette arbeidet har det kommet frem ytterligere nyansering av hva slags objekter det kan dreie seg om.

Opprettholdelse av funksjonalitet i kritisk infrastruktur vil være en hovedmålsetting ved objektsikkerhetsarbeidet i fremtiden. Det er påpekt at det må dreie seg om objekter som etter en skadevurdering anses helt essensielle for samfunnsviktige sikkerhetsinteresser. Terskelen for å utpeke et objekt som skjermingsverdig etter sikkerhetsloven vil således være høy.

Sikkerhetsloven retter seg først og fremst mot det som er rikets sikkerhet og vitale nasjonale sikkerhetsinteresser. Loven er gitt på bakgrunn av at informasjon og objekter som kommer inn under disse begrepene må beskyttes med særskilte tiltak. Det er i stadig sterkere grad en erkjennelse av at vår kritiske infrastruktur og kritiske samfunnsfunksjoner er av særlig, nasjonal interesse.

7.5 Utvalgets anbefalinger

Et viktig formål med sikkerhetsloven er å ivareta den enkeltes rettssikkerhet. En del av de forebyggende sikkerhetstiltakene kan være meget inngripende overfor enkeltpersoner. Samfunnet har derfor funnet det nødvendig å underkaste den forebyggende sikkerhetstjeneste særskilte kontrollmekanismer utover de som på generelt grunnlag er etablert for forvaltningen. Denne særskilte kontrollen er hjemlet i en egen lov og utøves av et utvalg (EOS-utvalget) nedsatt av Stortinget[4].

Det har nylig blitt foretatt endringer i sikkerhetsloven for ytterligere å styrke personvernet i forhold til personkontroll og sikkerhetsklarering som loven gir adgang til.

Innføres lov eller forskrift med krav om sikkerhetsklarering som kan innebære at arbeidstaker må gå fra en stilling vedkommende er tilsatt i før loven ble vedtatt, vil dette kunne stride mot Grunnlovens § 97 med forbud mot lover med tilbakevirkende kraft. I den grad det skulle oppstå tilfeller der sikkerhetsmessig uskikkede personer innehar stilling ved objekter hvor det i medhold av et nytt regelverk kreves sikkerhetsklarering, vil det måtte forutsettes at personens arbeidstagerrettigheter ivaretas. Det er derfor utvalgets vurdering at innføringen av et krav om sikkerhetsklarering for adgang til skjermingsverdige objekter, ikke kan være grunnlag for oppsigelse i slike tilfeller.

7.5.1 Forslag knyttet til objektsikkerhet

Sikkerhetsloven inneholder i dag bestemmelser om objektsikkerhet, men disse er meget knappe. Utvalget har i sitt arbeid registrert at mange virksomheter etterspør slike bestemmelser.

Utvalget er kjent med at det i lengre tid har vært arbeidet med forslag til lovendring og forskrifter knyttet til utfyllende bestemmelser om objektsikkerhet. I en omfattende høringsrunde høsten 2003 uttalte en rekke virksomheter seg om et utkast til nye lov- og forskriftsbestemmelser om objektsikkerhet. Selv om de ulike høringsinstansene i hovedsak var positive til å få utfyllende bestemmelser på dette området, fremkom det også en del motforestillinger knyttet til mulige konsekvenser av forslaget. Dette gjaldt særlig usikkerhet med hensyn til hvilke økonomiske belastninger virksomhetene kunne bli påført gjennom nye pålegg om sikringstiltak. Videre var enkelte bekymret for konsekvensene dersom det skulle bli krav om sikkerhetsklarering av arbeidstakere i vesentlig større utstrekning enn i dag.

Det er flere grunner til at utvalget anser det nødvendig å få på plass utfyllende bestemmelser om objektsikkerhet. En riktig utpeking av skjermingsverdige objekter forutsetter at det finnes et felles klassifiseringssystem. Videre må regelverket anvise generiske krav til de sikkerhetstiltakene som må settes i verk. Et klassifiseringssystem vil bidra til at tiltakene kan balanseres riktig, og at det

[4] Lov av 3. feb. 1995 nr. 7 om kontroll med etterretnings-, overvåknings- og sikkerhetstjeneste

ikke benyttes for kostbare og for inngripende tiltak for det enkelte objekt.

I rapporten fra Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur[5] påpekes også at det enda ikke, sju år etter at loven ble vedtatt, er utarbeidet forskrift om skjermingsverdige objekter. Forsvarsdepartementet svarte da at arbeidet med dette er stilt i bero i påvente av dette utvalgets (Infrastrukturutvalgets) rapport.

Å få operasjonalisert objektsikkerhet i sikkerhetsloven vil også medføre at man vil få en overordnet koordinering av det forebyggende sikkerhetsarbeidet på dette området. Det er et sterkt behov for å sikre at avhengigheter på tvers av sektorer i samfunnet blir ivaretatt når objekter vurderes med hensyn til behov for beskyttelse.

For de virksomheter som allerede er underlagt sikkerhetsloven, er det nødvendig å kunne forholde seg til mer konkrete bestemmelser for at lovens formål skal oppfylles. Også virksomheter som i dag ikke omfattes av loven, men som ut fra egen vurdering av ansvarsområde og betydning for samfunnet vil kunne anta at bestemmelsene vil bli gjort gjeldende, har interesse av at loven gjøres mer utfyllende også på objektsikkerhetsområdet.

Utvalget mener at identifisering av hvilke private virksomheter som bør omfattes av sikkerhetsloven etter § 2, tredje ledd bokstav a) må skje gjennom en prosess med et samarbeid mellom virksomhetene, deres organisasjoner og myndighetene. Utgangspunktet for dette vil være risiko- og sårbarhetsanalyser som eventuelt vil avdekke mulige skjermingsverdige objekter i virksomhetens besittelse. Dette vil være tilsvarende den prosess som er beskrevet under forslaget om en generell lov om beredskap i kapittel 6.6.1.1.

Utvalget anbefaler at nødvendige endringer i sikkerhetsloven som gjelder objektsikkerhet bør foretas, og at arbeidet med å gi utfyllende forskriftsbestemmelser på dette området samt utvikle standarder og standardiserte metoder bør gjennomføres.

I dagens lovbestemmelse om objektsikkerhet slås fast at det er objekteier som er ansvarlig for sikringen av egne skjermingsverdige objekter. I dette ligger implisitt at det kan medføre kostnader knyttet til etablering av tiltak som objekteier må bære. Dette vil følgelig gjelde for de deler av næringslivet som etter den prosess som er beskrevet over vil bli omfattet av bestemmelsene i sikkerhetsloven; tilsvarende vil være tilfelle når det gjelder en ny generell lov om beredskap. Det vises for øvrig til kapittel 14 om administrative og økonomiske konsekvenser.

Det er viktig å presisere at tilsynsmyndigheter i de enkelte sektorer vil ha en viktig oppgave i forhold til å påse at den praktiske gjennomføring av bestemmelser om objektsikkerhet skjer på en tilfredsstillende måte. Hvilke konkrete tiltak som blir aktuelle innen de enkelte sektorer vil variere fra sektor til sektor. Kraftforsyningen har særegne objekter som damanlegg, kraftstasjoner, ledningsnett. Petroleumssektoren særegenhet er blant annet knyttet til objekter off-shore, mens andre sektorer igjen har sine spesielle forhold. Det er sektortilsynene som best kjenner forholdene innen sine ansvarsområder.

NSM er gjennom sikkerhetsloven pålagt å føre tilsyn med at den enkeltes virksomhets plikter etter nevnte lov overholdes. Det vil være naturlig at utøvelsen av denne tilsynsmyndigheten skjer på et overordnet nivå, hvor også tverrsektorielle hensyn ivaretas.

Utvalget vil foreslå at det i sikkerhetsloven og forskiftene gis utfyllende bestemmelser om objektsikkerhet.

7.5.2 Forslag knyttet til sikkerhetslovens virkeområde

Sikkerhetslovens virkeområde har vært et sentralt tema i forbindelse med to forskjellige utredninger som er gjort på oppdrag av Forsvarsdepartementet. Utvalget mener at lovens innretting og virkemidler er av en slik karakter at det ikke vil være hensiktsmessig å gjøre loven generelt gjeldende for alle rettssubjekter. Å lage bestemte kriterier i loven for å angi hvilke virksomheter loven skal omfatte vil etter utvalgets mening være for upresist, og vil kunne medføre behov for lovendringer dersom justeringer ble påkrevd.

Utvalget viser til at sikkerhetsloven gjelder forvaltningsorganer. Utover dette kan Kongen bestemme at loven helt eller delvis også skal gjelde for ethvert annet rettssubjekt. Denne fullmakten er i dag delegert til Forsvarsdepartementet, jf. kgl. res. av 27. juni 2003. Det er imidlertid Justis- og politidepartementet som har et ansvar for forebyggende sikkerhet på sivil side i dag. Enkeltvedtak om å gjøre sikkerhetsloven gjeldende for andre rettssubjekter vil nødvendigvis være rettet mot sivil virksomhet. Det synes derfor rimelig at denne vedtaksmyndigheten ligger til Justis- og politidepartementet.

[5] Dokument nr. 3:4 (2005-2006). *Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur.*

Sikkerhetsloven angir to mulige forutsetninger for at loven kan gjøres gjeldende for andre rettssubjekt. Det er slike

a) som eier eller på annen måte har kontroll over eller fører tilsyn med skjermingsverdig objekt, eller
b) som av et forvaltningsorgan gis tilgang til sikkerhetsgradert informasjon.

Det kan også være at virksomheter har behov for å motta sikkerhetsgradert informasjon som krever gjennomføring av sikkerhetstiltak i henhold til sikkerhetsloven, og følgelig kommer inn under bokstav b). Loven dekker derimot ikke det tilfellet at et privat rettsubjekt selv har behov for å tilvirke informasjon som kan være skjermingsverdig.

Utvalget mener det bør vurderes å endre loven på dette punkt, slik at et dokumentert behov for å tilvirke skjermingsverdig informasjon i seg selv kan være et grunnlag for å gjøre loven gjeldende for den aktuelle virksomheten.

Utvalget anbefaler videre at sikkerhetslovens virkeområde utvides ved enkeltvedtak i samsvar med dagens regulering, og at Justis- og politidepartementet har denne fullmakten.

7.5.2.1 Virksomhetsklarering med hjemmel i sikkerhetsloven

Spørsmålet om det skal være krav om sikkerhetsklarering av private virksomheter som eier eller råder over visse skjermingsverdige objekter har vært drøftet i de nevnte utredningsarbeidene.

Sikkerhetsloven har allerede bestemmelser om virksomhetsklarering. Loven omtaler dette i dag som leverandørklarering i forbindelse med sikkerhetsgraderte anskaffelser. Når en leverandør kan få tilgang til skjermingsverdig informasjon som er sikkerhetsgradert KONFIDENSIELT eller høyere, skal leverandøren ha gyldig leverandørklarering for angitt sikkerhetsgrad.

Dersom manglende sikkerhetsklarering av en privat virksomhet som objekteier skulle føre til konsekvenser i forhold til eierskapet, vil dette ha karakter av ervervskontroll. Ervervsloven, som regulerte betingelser for eierskap, ble opphevet i 2002.

I forbindelse med behandlingen i Stortinget av forslaget om oppheving av loven, uttalte imidlertid komitéflertallet i Innst. O. nr. 72 (2001-2002) på side 4:

> Fleirtallet har merka seg at Forsvarets overkommando – Sikkerhetsstaben (FO/S), Forsvarsdepartementet og Direktoratet for sivilt beredskap (DSB) meiner oppheving av lova er uheldig i forhold til departementet sine høve til å ivareta beredskapsføremål, og at FO/S meiner oppheving av lova bør utsetjast til tryggingsmessige omsyn er ivareteke i anna lovverk, medan Forsvarsdepartementet, Justis- og politidepartementet og DSB i ei totalvurdering støttar departementet sitt forslag om oppheving. Fleirtallet ber regjeringa sørgje for at beredskapsomsyn og tryggingsomsyn blir innarbeidd i anna regelverk, om lova blir oppheva.

Utvalget mener derfor at det er mulig å gi bestemmelser om virksomhetsklarering for visse objekteiere. Dette bør i så fall kun gjelde for virksomheter som eier eller råder over objekter som er spesielt kritiske for samfunnet.

Kapittel 8
Ivaretakelse av sikkerhets- og beredskapshensyn ved omreguleringer og omorganiseringer[1]

I dette kapittelet gis det først en redegjørelse for drivkreftene bak omregulering og omorganisering de siste tiårene. Deretter gis en redegjørelse for hvordan sikkerhets- og beredskapshensyn ble vektlagt og ivaretatt under og etter disse prosessene. Det gis videre en oppsummering av hvordan disse hensynene har vært ivaretatt i omreguleringsog omorganiseringsprosessenene i telesektoren og kraftsektoren.

8.1 Drivkreftene bak omregulering og privatisering

Knappe offentlige budsjetter og stadig økende etterspørsel etter offentlige tjenester, den teknologiske utviklingen samt internasjonaliseringen og globaliseringen har vært de sentrale drivkreftene bak omreguleringen av offentlig virksomhet de siste tiårene.

8.1.1 Knappe offentlige budsjetter og stadig økende etterspørsel etter offentlige tjenester

Trangere budsjetter innenfor offentlig virksomhet har gjort det nødvendig med en nærmere vurdering av hva som er det offentliges primære ansvarsområder i samfunnsøkonomien og hva som kan og i noen tilfeller også bør overlates til privat sektor. Det er alminnelig enighet om at det offentliges kjernevirksomhet er å sørge for et adekvat tjenestetilbud på områder der markedet ikke fungerer. Det gjelder særlig for det som går under betegnelsen fellestjenester som retter seg mot tilfredsstillelse av grunnleggende, kollektive behov slik som rettsikkerhet, forsvar og ordensvern, beredskap og sikkerhet for liv og helse. På disse områdene har det offentlige et særlig ansvar for at et tilfredsstillende tjenestetilbud eksisterer.

Det sentrale spørsmålet er hva et offentlig ansvar innebærer, og hvordan det skal ivaretas. En aktuell problemstilling er hva det offentlige bør gjøre selv i form av offentlig tjenestetilbud og hva som kan settes ut til private gjennom anbudskonkurranse. Et viktig tema i den sammenheng er om kommersielle aktører har de samme incentiver til å ivareta hensynet til kvalitet når det går på bekostning av virksomhetens økonomiske resultat på kort sikt. Et synspunkt her er at det offentlige bør selv ha kontroll med tjenestetilbudet på områder der det er vanskelig å observere kvaliteten på en objektiv måte. På andre områder som renovasjon, elektronisk kommunikasjonstjenester, eiendomsforvaltning og desslike bør det være mindre motforestillinger mot konkurranseutsetting.

8.1.2 Den teknologiske utvikling

Naturlige monopoler har vært en annen arena for offentlig virksomhet. Det gjelder i særlig grad de nettverksbaserte naturlige monopolene innenfor tele, post, elektrisitet, jernbane, vann og avløp. Behovet for grenseoppgang mellom offentlig og privat ansvar og oppgaver har ført til gjennomtenking av hva som egentlig begrunner offentlig virksomhet også på disse områdene. Dette har ført til en erkjennelse av at det er nettverket som utgjør det naturlige monopolelementet i disse virksomhetene og ikke den nettbaserte produksjonen eller tjenesteytingen. Unntaket fra denne regelen er vann- og avløpssektoren, der det av kvalitetsmessige og økonomiske grunner ikke er aktuelt med konkurranse innen tjenesteytingen. Innenfor tele gjelder dette telenettet, innenfor jernbane jernbanenettet, innenfor posten postnettet selv om det ikke har karakter av fysisk infrastruktur, osv. Ut fra dette skulle det offentliges ansvar begrense seg til nettvirksomheten mens den nettbaserte tjenestevirksomheten kunne drives som konkurransevirksomhet. I diskusjonen om omreguleringen av de naturlige nettmonopolene har problemstillingen vært om en skulle tillate vertikal integrasjon mellom det naturlige nettmonopolet og konkurranse-

[1] Kapittelet er basert på notat fra Statskonsult, Statskonsult 2005. *Ivaretagelse av sikkerhet og beredskap i fristillingsprosesser* – i del 2, vedlegg 10.

virksomheten, eller om en burde ha et vertikalt (eiermessig) skille.

På de ulike områdene har en valgt forskjellig i omreguleringsprosessen. Innenfor post og tele har en valgt en modell med vertikal integrasjon, mens en innenfor jernbane og el-sektoren har gått for vertikal separasjon. Ansvaret for jernbanenettet er overlatt forvaltningsvirksomheten Jernbaneverket, mens det i prinsippet er «konkurranse på sporet». Her kunne en også tenke seg «konkurranse om sporet» ved at selskaper fikk monopol på bestemte strekninger innenfor et begrenset tidsrom[2]. Innenfor el-sektoren har en skilt ut det landsdekkende transportnettet som et naturlig monopol som forvaltes av Statnett. Selskapet har ikke anledning til å delta i konkurransevirksomhet på produksjons- eller distribusjonssiden.

8.1.3 Internasjonalisering og globalisering

Internasjonaliseringen av nasjonalt næringsliv har ført til behov for harmonisering av regulatoriske rammebetingelser mellom land. Dette har også påvirket de nasjonale omreguleringsprosessene. For Norge er det først og fremst EUs direktiver som har vært førende for prosessen. Det gjelder hovedsakelig innenfor tele og gass. I denne sammenheng er det spesielt viktig å undersøke om hensynet til beredskap og sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner har blitt tilstrekkelig ivaretatt i denne prosessen.

8.2 Hensynet til sikkerhet og beredskap

Gjennom fristilling er offentlige monopolordninger blitt avviklet og konkurransemarkeder etablert. Det er flere årsaker til at de ulike sektorene ble liberalisert, men både på tele- og kraftområdet var effektivisering og bedre utnyttelse av ressursene viktige hensyn.

På begge områdene ble det i forbindelse med fristillingen understreket at de overordnete samfunnspolitiske målsettingene ville ligge fast etter fristillingene. Dette var i hovedsak målsettinger knyttet til lik tilgang til tjenestene over hele landet, målsettinger om tilnærmet like priser (tele) mv. Hensynet til sikkerhet og beredskap er ikke spesielt drøftet i stortingsdokumenter knyttet til fristillingene, men forpliktelser på dette området for de berørte aktørene ble i stor grad videreført. Eksempelvis ble Telenor forpliktet til fortsatt å videreføre nød- og sikkerhetstjenesten via kystradionettverket for å ivareta samvirkeprinsippet i redningstjenesten. Justis- og politidepartementet dekker kostnadene knyttet til denne tjenesten.

Hensynet til sikkerhet og beredskap ble på begge sektorer ivaretatt gjennom bestemmelser i lovverket. Lovverket ga myndighetene hjemmel for å pålegge aktørene å gjennomføre og dekke kostnadene ved ulike typer sikringstiltak.

På kraftsektoren har NVE gjennom hele perioden hatt et ansvar for sikkerhet og beredskap, og Kraftforsyningens beredskapsorganisasjon ble omtalt i energiloven fra 1990. På teleområdet fikk ikke Post- og teletilsynet et tilsvarende ansvar før i forbindelse med St. meld. nr. 47 (2000-2001) Telesikkerhet og -beredskap i et telemarked med fri konkurranse, dvs. flere år etter at Telenor var blitt aksjeselskap, men omtrent samtidig med at selskapet ble børsintrodusert.

Sikkerhets- og beredskapshensyn er blitt tatt opp med jevne mellomrom i årene etter fristillingen. Dette har ført til større og mindre endringer i organisering, regulering og finansiering av området. Ett inntrykk er at det har vært gjort mest endringer i etterkant på teleområdet. Dette kan skyldes at det tradisjonelt har vært stor oppmerksomhet omkring sikkerhet og beredskap innenfor kraftsektoren fordi dette området er utsatt for vær og vind. Kraftsektoren besto av mange ulike aktører også før energiloven trådde i kraft, slik at myndighetene hadde lengre tradisjon for å jobbe med ulike aktører i denne type spørsmål. På teleområdet hadde ansvaret for sikkerhets- og beredskapsspørsmål i stor grad blitt ivaretatt av Televerket.

Årsakene til at spørsmålet om sikkerhet og beredskap er tatt opp i årene etter fristillingene varierer. På kraftområdet ble dette spørsmålet viet oppmerksomhet etter flommen i 1995, men i særlig grad etter den nedbørfattige sesongen og kraftkrisen i 2002/2003. På teleområdet ble spørsmålet grundig drøftet i stortingsmeldingen i 2000. Dette falt sammen i tid med at forvaltningen av eierskapet til Telenor ble overført fra Samferdselsdepartementet til Nærings- og handelsdepartementet. Mindre endringer er tatt opp i forbindelse med andre revisjoner av lov- og regelverk på området.

[2] I denne sammenheng vises til anbudsrunde om persontrafikk på Gjøvikbanen, sommeren 2005.

8.3 Virkemiddelbruk for ivaretakelse av sikkerhet og beredskap i omregulerings- og omorganiseringsprosesser

Tabellen nedenfor gir en oppsummering av virkemiddelbruken i omregulerings- og omorganiseringsprosessene som har vært på tele- og kraftområdet. Det er klare likheter i hvilke virkemidler som benyttes på de to områdene. Lovregulering er det sentrale virkemiddelet. Vi ser også at tilsynene på begge områder har en svært viktig rolle på sikkerhets- og beredskapsområdet.

Den vesentligste forskjellen i virkemiddelbruk finner vi på det organisatoriske. På energisiden er det etablert en beredskapsorganisasjon der alle enheter som produserer eller distribuerer strøm er medlem. Tilsvarende finner vi ikke på teleområdet. Det er også ulikheter knyttet til eierskapet. Staten er fortsatt eneeier i Statnett. Dette gir mulighet for styring gjennom foretaksmøte/generalforsamling. Dette er imidlertid en mulighet som i veldig liten grad benyttes.

8.4 Finansiering av beredskapstiltak

Finansiering av beredskap på områder der det har skjedd selskapsetableringer er blitt tatt opp i flere sammenhenger. Det er blitt pekt på at avvikling av monopoler kan være gunstig for beredskap fordi det vil være flere aktuelle leverandører. En konkurransesituasjon kan imidlertid føre til prispress som gjør at det ikke investeres nok i sikkerhet og beredskap. [3]

Sentrale problemstillinger knyttet til finansieringen av beredskapstiltak er blant annet spørsmålene om hvor grensen mellom statens ansvar og leverandør/tilbyders ansvar for finansieringen går, samt hvordan en ev. statlig støtte skal innrettes for ikke å virke konkurransevridende og for at ressursene skal kunne utnyttes så effektivt som mulig.

8.5 Utvalgets anbefalinger

8.5.1 Forslag knyttet til innføring av kontrollpunkter ved omreguleringer og omorganiseringer

Etter utvalgets mening bør ivaretakelse av hensynet til sikkerhet og beredskap inngå som en naturlig del av prosessene ved omreguleringer og/eller omorganiseringer av offentlige virksomheter. Det bør også være et krav at slike vurderinger dokumenteres slik at prosessen kan evalueres ved behov.

I 2004 ble det besluttet å utarbeide retningslinjer ved utsetting av forvaltningsoppgaver til selvstendige rettssubjekter og private aktører. En veileder for utskilling av virksomhet fra staten og en sjekkliste for utsetting av forvaltningsoppgaver er til behandling i Fornyelses- og administrasjonsdepartementet.[4] Utvalget bemerker viktigheten av at disse tydeliggjør behovet for ivaretakelse av sikkerhet og beredskapshensyn ved omreguleringer

[3] Dette vil nok ikke gjelde for virksomhetskritiske punkter.

[4] Se sjekkliste for utsetting av forvaltningsoppgaver i Høringsutkast Moderniseringsdepartementet 2005. *En veileder ved utskilling av virksomhet fra staten.* Høringsutkast april 2005. Saken er til behandling i Fornyelses- og administrasjonsdepartementet (januar 2006).

Tabell 8.1 Virkemiddelbruken i omregulerings- og omorganiseringsprosessene innenfor telesektoren og kraftsektoren.

	Kraft	Tele
Lov	Ja	Ja
Konsesjon[1]	Ja	Ja
Tilsyn	NVE	PT
Annen organisering	KBO	Nei
Finansiering av tilsyn	Inngår i generelle gebyrer til tilsynet	Inngår i generelle gebyrer til tilsynet
Finansiering over statsbudsjettet (tilskudd/kjøp av tjenester)	2,6 mill. i 2005	14 mill. kr i 2005
Beredskapsøvelser	Ja	Ja
Beredskapsplaner	Ja	Ja
Eierstyring	Muligheten er til stede gjennom eierskapet i Statnett	Nei

[1] Det er konsesjonsplikt på begge områder, men det pålegges ikke spesielle oppgaver knyttet til konsesjonen.

og omorganiseringer. En er likevel kjent med at det, på bakgrunn av en henvendelse fra NSM, ble tatt inn et avsnitt under samfunnsøkonomisk analyse som peker på nødvendigheten av å vurdere de sikkerhetsmessige forhold ved utskilling av virksomhet fra staten.

Utvalget mener det bør benyttes en liste over kontrollpunkter som sikrer at hensynet til sikkerhet og beredskap blir ivaretatt ved omreguleringer og omstruktureringer av offentlig virksomhet. Et eksempel er ivaretakelse av samvirkeprinsippet i norsk redningstjeneste. Samvirkeprinsippet er et

Tabell 8.2 Forslag til liste over kontrollpunkter ved omorganiseringer og omstruktureringer av offentlig virksomhet

Kontroll-punkt	Problemstilling	Kommentar
1.	Hvordan ivaretas sikkerhet og beredskap i virksomheten?	Sikkerhetskulturen i virksomheten må beskrives.
2.	Hvilke konsekvenser har endringen for ivaretakelse av sikkerhet og beredskap i virksomheten?	Sikkerhets- og beredskapsrelaterte oppgaver må identifiseres, og det må tas stilling til hvordan disse oppgavene skal ivaretas, herunder må oppgaver og deltakelse i nasjonale beredskapsorganer/-løsninger/-planer avklares. Det må redegjøres for hvordan sikkerhets- og beredskapsarbeidet skal organiseres etter endringen.
3.	Påvirker endringen reguleringen av sikkerhet og beredskap i virksomheten?	Forholdet til sikkerhetsloven og aktuelt sektorregelverk må vurderes. Avtaler som regulerer sikkerhet og beredskap i virksomheten må gjennomgås og vurderes.
4.	Påvirker endringen ivaretakelsen av hensynet til rikets sikkerhet og vitale nasjonale interesser?	Det må redegjøres for om virksomheten har ansvar og oppgaver som ivaretar hensynet til rikets sikkerhet og vitale nasjonale interesser. Eksempelvis må det redegjøres for om virksomheten har oppgaver i redningstjenesten og hvordan disse, i henhold til samvirkeprinsippet, skal ivaretas etter omorganiseringen.
5.	Hva er ressursinnsatsen til sikkerhet og beredskap i virksomheten før og etter endringen?	Ressurser avsatt til sikkerhet og beredskap må identifiseres. Endringer i ressursinnsatsen må begrunnes og ivaretakelsen av sikkerhets- og beredskapshensyn må dokumenteres.
6.	Hvilke underleverandører er virksomheten kritisk avhengig av for å opprettholde driftskontinuitet?	Behovet for å avtaleregulere prioritet av varer og tjenester i knapphetssituasjoner bør vurderes.
7.	Leverer virksomheten samfunnskritiske varer og tjenester?	Såfremt det ikke er regulert i lov, må det inngås avtale om hvordan et ev. nasjonalt behov skal dekkes i tilfelle det oppstår en situasjon med knapphet på de varer og tjenester virksomheten leverer.
8.	Hvordan skal spørsmål knyttet til sikkerhet og beredskap håndteres av virksomhetens ledelse og styrende organer?	I den grad virksomheten håndterer informasjon som er sikkerhetsgradert iht. sikkerhetsloven, må det etableres rapporterings- og beslutningssystemer som ivaretar hensynet til rikets sikkerhet og vitale nasjonale sikkerhetsinteresser.

grunnleggende fundament for norsk redningstjeneste, og innebærer at alle offentlige etater med relevante ressurser ved behov plikter å delta i redningstjenesten og må dekke sine egne utgifter. Ved omorganisering/utsetting av forvaltningsoppgaver må en derfor sikre at hensynet til samvirkeprinsippet i redningstjenesten blir ivaretatt på en fullgod måte.

Listen over kontrollpunkter bør etter utvalgets mening ikke være begrenset til visse typer endringer av virksomheten, men kunne brukes som beslutningsverktøy i alle situasjoner som gjelder omregulering og omstrukturering, herunder endring av tilknytningsform, utskilling av offentlig virksomhet helt eller delvis til private aktører, utsetting av forvaltningsoppgaver og omorganiseringer av offentlig virksomhet generelt. Utvalget har utarbeidet et forslag til en slik liste, se tabell 8.2.

Utvalget mener at listen er også nyttig å ta i bruk for endringer som allerede er foretatt. Enkelte av kontrollpunktene vil dessuten kunne brukes som beslutningsverktøy ved endringer av private virksomheter. Det påpekes at listen ikke er ment å erstatte en risiko og sårbarhetsanalyse (ROS).

Listen over kontrollpunkter bør vurderes opp mot en ekstern norm for ivaretakelse av sikkerhets- og beredskapsarbeid i virksomheter. Det vises i denne sammenheng til utvalgets forslag til standarder og standardiserte metoder, jf. kapittel 6.6.5.

Utvalget vil også foreslå at det vurderes innarbeidet krav i utredningsinstruksen om utredning av sikkerhets- og beredskapsmessige konsekvenser av forslag.

8.5.2 Forslag knyttet til å holde sikkerhets- og beredskapsmessige oppgaver som en integrert del av virksomheten

Ved omreguleringer og omorganiseringer søkes det ofte etter kostnadsbesparende tiltak i hele virksomheten. Oppgaver som anses å være utenfor kjerneoppgavene til virksomheten overlates til andre som antas å kunne utføre disse på en mer kostnadseffektiv måte. Utvalget ønsker i den sammenheng å peke på viktigheten av å ikke løsrive de sikkerhets- og beredskapsmessige oppgavene fra ordinær drift i kritisk infrastruktur og kritiske samfunnsfunksjoner. Etter utvalgets oppfatning er sikkerhet og beredskap en sentral oppgave i de delene av en virksomhet som omfatter kritisk infrastruktur og kritiske samfunnsfunksjoner. Utvalget vil på bakgrunn av dette anbefale at sikkerhets- og beredskapsarbeid som knytter seg til kjerneoppgaver i kritisk infrastruktur og kritiske samfunnsfunksjoner holdes som en integrert del av virksomheten.

8.5.3 Forslag knyttet til sammefallende omstillinger i en sektor

Det er utvalgets oppfatning at sikkerheten ikke alltid blir ivaretatt tilfredsstillende ved omstillinger. Statens Havarikommisjon for Transport har vist til det samme for luftfartssektoren når de skriver at: «[...] operatørers og luftfartsmyndigheters prosesser for å ivareta sikkerheten ved innføring av endringer og omstillingsprosesser inneholder en rekke forhold som bør forbedres før de kan sies å være tilstrekkelige for dette formålet.»[5] Utvalget ønsker å understreke at sikkerhetshensyn må ivaretas under omstillingsprosesser i kritisk infrastruktur og kritiske samfunnsfunksjoner. Utvalget ønsker videre å peke på at omstillinger i tilsynsorganer kan føre til at evnen til å utføre tilsyn blir redusert for en periode. Det vil derfor etter utvalgets mening være uheldig å omstille et tilsynsorgan samtidig som sentrale operatører i samme sektor omstilles. Det vil kunne føre til en dobbelt svekkelse av sikkerheten. Utvalget anbefaler derfor at omstillinger i et tilsynsorgan ikke må falle sammen i tid med omstillinger hos sentrale operatører i samme sektor.

[5] SL RAP 35/2005. *Flysikkerhet i norsk luftfart under omstillingsprosesser.* Havarikommisjonen for sivil luftfart og jernbane.

Kapittel 9
Offentlig eierskap

Det store innslaget av offentlig eierskap i norsk økonomi har vært motivert ut fra verdimaksimerende mål og andre samfunnsmessige mål på sentralt og sektorpolitisk nivå.[1] For eksempel har det offentlige eierskapet blitt bruk som virkemiddel for å ivareta næringspolitiske hensyn, fordelingshensyn, samfunnsøkonomiske hensyn, med mer. Det er viktig å ivareta en nasjonal forankring av enkelte vitale virksomheter. Nasjonalt eierskap innebærer blant annet at hovedkontorfunksjonene ligger i Norge. Den nasjonale forankringen sikres best gjennom offentlig eierskap, og foreløpig er det få norske miljøer som kan erstatte det offentliges rolle som garantist for nasjonal forankring av eierskapet til viktige selskaper.

I dette kapittelet gis det først en redegjørelse for hvordan det statlige eierskapet utøves. Deretter drøftes noen generelle begrunnelser for statlig inngripen i markedsøkonomien, før en går over til drøfting av offentlig eierskap knyttet til kritisk infrastruktur. Utvalget berører også spørsmålet om eiermessig skille eller integrasjon mellom forvaltning av kritisk infrastruktur og relatert konkurransevirksomhet. Avslutningsvis drøfter utvalget forholdet mellom regulering og eierskap som virkemiddel for ivaretakelse av hensynet til sikkerhet og beredskap.

9.1 Utøvelse av det statlige eierskap

Utøvelse av det statlige eierskapet har både en regulatorisk side og en praktisk side. Regulatorisk utøves det statlige eierskapet innenfor en ramme av konstitusjonelle og parlamentariske prinsipper. Stortinget har vedtatt lovregler og regjeringen har utarbeidet egne regler som setter rammer for utøvelsen av det statlige eierskapet. Samtidig har utøvelsen av det statlige eierskapet en praktisk side, som vil bli omtalt nærmere nedenfor. Omtalen av hvordan det statlige eierskapet utøves er basert på innspill fra eierskapsavdelingen i Nærings- og handelsdepartementet.

[1] Se NOU 2004:7 *Statens forretningsmessige eierskap,* kapittel 2.

9.1.1 De konstitusjonelle forhold

9.1.1.1 Forvaltningen av det statlige eierskapet

Grunnlovens § 19 fastslår at Kongen (regjeringen) skal forvalte statens aksjer i aksjeselskaper, eierskapet til statsforetak og særlovsselskap. Dette er en oppgave som etter Grunnloven ikke kan tas fra Kongen, et såkalt prerogativ. Kongen delegerer forvaltningen til en statsråd som i henhold til Grunnlovens §12 bestyrer det departement selskapet «hører under». Prerogativet innebærer at Stortinget ikke kan utøve direkte eierstyring overfor selskapene.

I henhold til de parlamentariske prinsipper vårt samfunn styres etter, utøves statsrådens forvaltning av statens eierandeler i selskap under konstitusjonelt og parlamentarisk ansvar. Statsråden er ansvarlig overfor Stortinget for sin håndtering av statens eierskap. På den annen side har det vært en gjennomgående oppfatning på Stortinget at det ikke er mulig eller hensiktsmessig å holde regjeringen ansvarlig for beslutninger av forretningsmessig karakter som i medhold av selskapslovgivningen er lagt til selskapsorganene.

9.1.1.2 Stortingets kontroll av det statlige eierskapet

Uavhengig av regjeringens rett til å forvalte det statlige eierskapet, må Stortinget bli forelagt, og gi sitt samtykke ved endringer i det statlige eierskapet. I tillegg til Stortingets medvirkning, fører Stortinget også etterfølgende parlamentarisk kontroll. Stortinget gjennomfører hovedsakelig kontrollen gjennom Riksrevisjonen, men Stortingets Kontroll- og konstitusjonskomte kan også ta enkeltsaker opp til behandling.

Riksrevisjonen rapporterer årlig til Stortinget. Riksrevisjonens kontroll er hjemlet i Grunnlovens § 75k og i egen lov. Riksrevisjonen kontrollerer at statsråden har utøvet sin oppgave som forvalter av statens interesser i samsvar med Stortingets vedtak og forutsetninger. Riksrevisjonen skal gjøre de undersøkelser som er nødvendige for at de kan ha en kvalifisert oppfatning av hvordan forvaltningen er håndtert. Det innebærer blant annet at Riksrevisjonen kan foreta forvaltningskontroll av heleide statlige selskap. Riksrevisjonen skal også innkalles

til generalforsamling i heleide selskaper. Et viktig utgangspunkt for Riksrevisjonens kontroll er statsrådens årlige rapportering vedrørende det enkelte selskap. Innen 1 måned etter generalforsamling eller foretaksmøte skal det oversendes en redegjørelse for statsrådens (departementets) forvaltning av statens eierskap i selskap med minst 50 % statlig eierskap, og i enkelte andre selskaper hvor staten har en dominerende posisjon på eiersiden, selv om den er lavere enn 50 pst.

9.1.1.3 Regjeringens forvaltning av eierskapet

Utgangspunktet for regjeringens kontroll av eierskapet finnes i Reglementet for Økonomistyring i Staten § 10. I henhold til denne bestemmelsen skal det utarbeides skriftlige retningslinjer for hvordan statens eierskap i selskap skal forvaltes.

Nærings- og handelsdepartementet har for eksempel vedtatt slike retningslinjer for forvaltningen av statlige aksjeselskaper, finansinstitusjoner der staten har eierinteresser og for forvaltningen av eierinteressene i Statkraft AS. Retningslinjene inneholder regler knyttet til eierutøvelsen av eierrollen, avkastningskrav og utbyttepolitikk, resultatoppfølging og kontroll, og endringer i statens kapitalengasjement.

Grunnlaget for eierskapsutøvelsen er for øvrig forankret i de forutsetninger og retningslinjer på feltet som følger av behandlingen av St.meld. nr. 22 (2001-2002) Et mindre og bedre statlig eierskap (Eierskapsmeldingen) og Innst. S. nr. 264 (2001-2002). Et forhold som har særlig stor betydning for utformingen av departementets arbeid er at mange av selskapene også har private eiere og er børsnoterte. I forlengelsen av dette legges det særskilt vekt på å følge aksepterte prinsipper for god eierskapsutøvelse og selskapsledelse («Corporate Governance»). Departementet deltar aktivt i diskusjonen med andre aktører i aksjemarkedet for å avklare og etterleve slike regler.

Som følge av at Nærings- og handelsdepartementets selskaper er blant de mest forretningsmessig orienterte i statens eierskap og eierskapet stort sett ikke har noen sektorpolitiske formål, er det i liten grad særregler for forvaltningen av selskapene ut fra sektorpolitiske hensyn. En del av eieroppfølgingen er likevel de formål som gjelder for det enkelte selskap og som er tatt inn i vedtektenes formålsparagraf.

9.1.1.4 Rolledelingen Regjering – Storting i eiersaker

Stortinget gir regjeringen fullmakter for eierskapsutøvelsen Dette inkluderer blant annet fullmakter til å endre statens prosentvise eierandel i enkelte selskaper. Når saker medfører at det er aktuelt å gå utenfor disse rammene, må saken forelegges og ny fullmakt gis av Stortinget. Typiske eiersaker som behandles i Stortinget er salg av aksjer, emisjoner, omdannelse til en annen selskapsform eller betydelig endring i selskapenes virke og omfang.

Hvis et selskap med statlig eierandel avhender deler av virksomheten, og dette innebærer en vesentlig forandring av statens samlede engasjement, er det også en sak som må forelegges Stortinget. På den annen side er transaksjoner, som for eksempel overdragelse av aksjer i datterselskap eller virksomheter, som er ledd i den forretningsmessige ledelsen av selskapet ikke en sak for Stortinget. Det vises til føringer lagt i forbindelse med Stortingets behandling av NOU 1972:38 Stortingets kontroll med forvaltningen mv. i Dok. nr. 7 (1972-1973), jf. Innst. S. nr. 277 (1976), s. 18-19.

9.1.2 Praktisk eierutøvelse – Beskrivelse av arbeidet rettet mot selskapene

9.1.2.1 Generelt

Det legges vekt på at eiermyndigheten utøves gjennom eierfora som generalforsamlingen/foretaksmøtet. I enkelte selskaper hvor staten eier sammen med en eller et fåtall andre store eiere kan viktige avklaringer skje i særskilte eiermøter uavhengig av selskapet.

Som grunnlag for å forberede synspunkter som skal behandles av generalforsamlingen er det ofte en omfattende kontakt mellom departementet og ledelsen av selskapene. Dette skjer for det første regelmessig i form av kvartalsvise møter med en del selskaper for å gjennomgå deres resultater. Det legges også vekt på å gjennomføre årlige bedriftsbesøk og delta på selskapets presentasjoner sammen med øvrige investorer. I tillegg kan det være behov for annen kontakt og oppdatering i saker av betydning.

Slike kontakter initieres like gjerne fra selskapet som fra departementet og samsvarer i hovedsak med kontakten alle store eiere vil ha. Slik kontakt ses som en forutsetning for at departementet kan utøve eierrollen på en forsvarlig måte. Årsaken er at eieren må ha kunnskap om selskapets virksomhet og være orientert om sentrale spørsmål når det gjelder selskapenes utvikling. Samtidig vil ofte selskapenes styre og ledelse ha behov for å kjenne eiernes vurderinger i forbindelse med utforming av selskapenes

virksomhet og strategi. I tillegg til dette må det samarbeides om grunnlagsmaterialet ved bevilgningsforslag til kapitalutvidelser mv., og om budsjettfremlegg i de selskapene som fremdeles får statstilskudd.

9.1.2.2 Valg av styre

Selskapets styre har en viktig rolle for å sikre at selskapet utvikler seg og driver i samsvar med eiernes interesser. Det er av stor betydning at det er et tillitsforhold mellom eier og styret. Valg av styre ses således som det kanskje viktigste styringsredskapet for departementet. Ved misnøye med selskapenes resultater eller andre uheldige omstendigheter er også utskiftninger i styret departementets mest aktuelle virkemiddel for å sikre endringer. Ansvaret for styresammensetningen ses ikke som begrenset til de periodiske styrevalgene, men som løpende tilsynsansvar med plikt til å gripe inn dersom styret ikke løser sine oppgaver på en tilfredsstillende måte. Der hvor departementet ikke er eneeier og utnevner hele styret, legges det derfor stor vekt på å være representert i selskapenes valgkomiteer som foreslår sammensetning av bedriftsforsamling/representantskap og styre.

Valgene finner i de fleste selskaper sted i samsvar med aksjelovens hovedregel med en funksjonstid på 2 år. Departementet legger stor vekt på at styremedlemmene skal ha integritet og være selvstendige. Styret skal ikke forskjellsbehandle aksjonærene og representerer selskapet overfor alle aksjonærene under ett, ikke bare den største aksjonæren som i mange tilfeller kan være staten. Ved utvelgelse av kandidater følger departementet også opp en del andre forhold:

- Et styremedlem i statlige selskaper kan normalt ikke ha andre verv i konkurrerende virksomheter.
- Det er ikke akseptabelt at et styremedlemskap kombineres med konsulentverv eller andre særskilt lønnede oppdrag for vedkommende selskap.

I selskaper der staten eier sammen med private er det som regel valgkomiteer som arbeider med styrespørsmålene. Gjennom departementets deltagelse i valgkomiteen fremstår dette som et organ for samarbeid mellom de private eiere og den statlige aksjonæren hva gjelder styrevalg og valg av representanter til bedriftsforsamlingen eller representantskapet. I de tilfeller et selskap har bedriftsforsamling eller representantskap, velger denne styret i selskapet etter innstilling fra valgkomiteen.

9.1.2.3 Avkastningskrav og utbyttepolitikk

Nærings- og handelsdepartementet har utarbeidet langsiktige avkastningsmål for samtlige selskaper hvor departementet har eierinteresser og hvor forretningsmessige mål er fremtredende. Arbeidet er basert på de mest vanlige metoder for å beregne markedsmessige avkastningskrav for ulike sektorer. Måltallene benyttes i departementets interne vurderinger, og som grunnlag for oppfølging og dialog med selskapene. Av forretningsmessige årsaker blir de ikke kommunisert eksternt. Slike mål brukes med forsiktighet i det en fortolkning for operativ bruk også må ta hensyn til de begrensninger som ligger i målet anvendet på kortsiktig resultatoppfølging. For slike formål vil departementet med basis i dette langsiktige målet følge opp ulike resultatmål som kan variere fra selskap til selskap.

Det har vært en vurdering av om målene departementene bruker, bør offentliggjøres. Av forretningsmessige grunner er det besluttet ikke å gjøre dette. For selskaper hvor staten ønsker å selge aksjer til private eiere vil en offentliggjøring blant annet kunne påvirke prisingen i eventuelle salgsprosesser. For børsnoterte selskaper anses slik offentliggjøring fra staten som eier å være lite heldig og vil kunne ha uønskede effekter for børskursen på selskapene.

I aksjeselskap med flere eiere er det styret som setter rammene for utdeling av utbytte. I børsnoterte selskaper offentliggjør styret normalt en langsiktig utbyttepolitikk. Departementet utarbeider egne analyser om utbytteforventninger som grunnlag for dialog med selskapene. I heleide selskaper og statsforetak fastsettes utbyttet gjennom budsjettprosessen. Departementet har en løpende dialog også med disse selskapene om utbyttefastsettingen som grunnlag for budsjettarbeidet. I enkelte tilfeller er det i fremlegg til Stortinget signalisert en langsiktig utbyttepolitikk fra eiersiden, men Stortinget har i praksis ofte avveket fra den fastsatte politikken.

Oppfølgningen i forhold til avkastning og utbytte skjer naturlig i forbindelse med selskapets årsregnskap som departementet på grunnlag av forslag fra selskapets styre behandler i den årlige ordinære generalforsamlingen. Eierskapsavdelingen i Nærings- og handelsdepartementet foretar alltid en særskilt gjennomgang av selskapenes årsoppgjør før generalforsamlingen. Foruten å påse at lovgivningens formelle krav til årsregnskapet og styrets årsberetning er oppfylt, vil avkastning og utbytteforslag vurderes. Her vurderes også andre aktuelle spørsmål knyttet til selskapets virksomhet og økonomiske utvikling.

9.2 Generelle begrunnelser for statlig inngripen i markedsøkonomien

Det er myndighetenes ansvar i markedsøkonomien å sørge for en adekvat forsyning av varer og tjenester på områder der markedene svikter.

Markedssvikt oppstår når varer og tjenester ikke vil bli tilbudt i markedet i et ønskelig omfang på kommersielt grunnlag. En viktig årsak til dette er at det kan være vanskelig å individualisere og identifisere den enkeltes forbruk. I slike tilfeller kan den enkelte borger ikke ekskluderes fra å benytte tjenesten. Tilbudet er for alle. Slike varer og tjenester blir kalt fellesgoder, og kjennetegnes av at den enkelte borger får tilgang til varen og tjenesten uansett betaling eller ikke (Dette gir opphav til det såkalte gratispassasjerproblemet). Den vil derfor ikke kunne finansieres i markedet. Tilbudet av varen eller tjenesten må derfor være et myndighetsansvar. Forsvaret, rettsvesenet og ordensvernet blir gjerne fremholdt som de viktigste eksemplene på landsdekkende fellesgoder. Kostnadene for tilbudet av fellesgoder er i hovedsak knyttet til etableringen av tjenesten og er derfor uavhengig av hvor mange som faktisk bruker eller har nytte av dem.

For noen tjenester av typen fellesgoder er det likevel slik at den enkeltes forbruk kan identifiseres, og brukeren kan om ønskelig ekskluderes fra å bruke fellesgodet. Eksempel på dette er TV-programmer distribuert over kabel-TV nett. Slike tjenester blir kalt for fellestjenester med eksklusjonsmulighet på brukersiden. Eksklusjonsmuligheten har betydning for finansieringsformen. Når eksklusjon ikke er mulig, må tjenesten finansieres ved generell beskatning, mens den ved mulighet for eksklusjon også kan finansieres ved brukerbetalingsordninger. Det skjer ved ulike former for tilgangsprising som betalings-TV, vegprising o.l.

Myndighetenes rolle når det gjelder fellesgodene, er først og fremst i fravær av et marked å tre inn i bestillerrollen ved å bestemme et optimalt forsyningsnivå da en ikke har noen markedsbestemt etterspørsel å forholde seg til. Det følger av dette at myndighetene også får finansieringsansvaret, som dekkes dels via generell beskatning og dels via pålagt brukerbetalingsordninger når det er mulig.

Virksomheter med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner støtter opp under rikets sikkerhet og vitale nasjonal interesser gjennom sitt sikkerhets- og beredskapsarbeid. Utvalget mener at sikring av kritisk infrastruktur og opprettholdelse av kritiske samfunnsfunksjoner kan anses som et fellesgode, hvilket forutsetter et klart myndighetsansvar for å oppnå en samfunnsøkonomisk ønskelig situasjon. Dette ansvaret må følges opp med reguleringer enten virksomheten har monopol eller er i konkurranse.

9.3 Privat eller offentlig eiet virksomhet?

Et viktig spørsmål her er hvordan det offentlige bør ivareta ansvaret for forsyningen av varer og tjenester som ikke kan, eller bør, skje på kommersielt grunnlag. I utgangspunktet kan det skje på flere måter. Det offentlige kan stå som eier av virksomhet som produserer goder som ikke kan finansieres, eller som det er uhensiktsmessig å finansiere i markedet. Eierskapet innebærer et finansieringsansvar. På produksjonssiden har det offentlige valget mellom egenproduksjon eller kontraktsstyrt privat produksjon. Sistnevnte skjer ved konkurranseutsetting av hele eller deler av produksjonen. Mer generelt står valget mellom offentlig eierskap og produksjon - eventuelt kombinert med konkurranseutsetting - på den ene siden, eller offentlig regulering av privat eiet virksomhet og produksjon på den andre.

Det økonomiske argumentet for privatisering er at private eiere har et sterkere fokus på den økonomiske bunnlinjen enn det offentlige normalt har, og dette sammen med at privat virksomhet normalt er mer utsatt for konkurranse, fører til at produksjonen gjennomgående drives mer kostnadseffektivt under privat eierskap. Kostnadseffektivisering er derfor det vanligste argumentet i favør av privatisering, dvs. overføring av eierskapet til private. Et annet argument er at private bedrifter på grunn av konkurransesituasjonen kan være mer lydhøre for publikums preferanser slik at en får større variasjon i vare- og tjenestetilbudet. Kostnadseffektivisering er også den viktigste begrunnelsen for konkurranseutsetting. Det gjelder både i privat og offentlig virksomhet.

Kontraktsstyrt ekstern produksjon krever imidlertid at oppdragsgiver har en effektiv overvåkning og oppfølging av kontrakten. Incentivet til kontroll i denne forbindelse vil nok gjennomgående være sterkere i privat eiet virksomhet enn offentlig, hvor eierskapet forvaltes på vegne av den enkelte borger. Fra et rent kostnadsmessig synspunkt er konkurranseutsetting av produksjon i offentlig virksomhet derfor ikke nødvendigvis i ett og alt et fullgodt alternativ til privatisering.

Et viktig problem ved regulering av privat virksomhet er imidlertid at det kan være forhold ved produksjonen som det kan være vanskelig for

reguleringsmyndigheten å observere, og som derfor ikke kan reguleres fullt ut på en tilfredsstillende måte. Som oftest gjelder dette kvalitative egenskaper ved tjenesten. Bedriftsøkonomisk vil økt kvalitet normalt bety økte kostnader. For bedriften kan det da bli et motsetningsforhold mellom kostnadseffektivisering og ønsket om god kvalitet. Det gjelder i særlig grad dersom reguleringsregimet er slik at bedriften beholder gevinstene fra kostnadsreduksjoner uavkortet, samtidig som det kan være vanskelig for en utenforstående reguleringsinstans og for brukerne av den regulerte tjenesten å avdekke kvalitetssvikt på kort sikt. Kommersialisering av virksomheten kan da føre til at kostnadseffektivisering går på bekostning av tjenestekvalitet i vid forstand. Privatisering kan på denne måten føre til betydelige kostnadsreduksjoner, men reduserte kostnader kan ha en motpost i en reduksjon av tjenestekvaliteten. Dersom kvalitetssvikt skyldes for eksempel ufullstendig vedlikehold av underliggende infrastruktur, er det tenkelig at konsekvensene av kvalitetssvikt først materialiserer seg etter en god del tid. Dette problemet gjelder for så vidt også ved konkurranseutsetting.

Inntektsregulering av monopolvirksomheter, offentlig eller privat, gir rammer for inntekter og kvalitetsmessige normer for virksomheten. Dette gir økonomiske incitamenter for både effektiv drift og for å opprettholde kvaliteten. Denne formen for regulering har fungert i 15 år for de elektriske nettselskapene i landet og har bidratt til en samfunnsmessig bedre utnyttelse av ressursene. Reguleringsmyndigheten må med en slik modell være oppdatert på de krav som til enhver tid stilles i samfunnet til kvalitet og til den sikkerhet og beredskap som samfunnet forventer ved krisescenarier slik at disse kan reguleres inn i virksomhetene. Inntektsrammeregulering gir sterke incentiver til kostnadseffektivisering. Et viktig spørsmål i denne sammenheng er om inntektsrammereguleringen er tilstrekkelig fokusert på sikkerhet og beredskap knyttet til den underliggende infrastrukturen. I særlig grad gjelder dette for påregneligheten av en funksjonsdyktig infrastruktur og leveringssikkerheten for de tjenestene som infrastrukturen understøtter. Dette er sider ved virksomheten som er viktige for den alminnelige trygghetsfølelse og som dermed har karakter av rene fellesgoder. Som for fellesgoder generelt er det vanskelig å innkassere den samlede samfunnsnytten av slike tjenester som markedsinntekt.

Når det gjelder de landsdekkende fellestjenestene forsvar, rettsvesen og sivil maktanvendelse, er de ingen som har foreslått å privatisere disse, og så vidt vites, er det heller ingen land som har forsøkt dette i nyere tid i særlig omfang[2]. Her føles det som selvsagt at fellesskapet bør ha kontrollen, og at myndighetene utøver denne på fellesskapets vegne. Det kan da være verdt å tenke nærmere over hvorfor privatisering av disse tjenestene føles som en umulig tanke, og om svaret på dette spørsmålet kan gi retningslinjer for vurderingen av eierspørsmålet når det gjelder annen kritisk infrastruktur og virksomhet som utøver vitale samfunnsfunksjoner.

Det er særlig to hensyn som synes viktige for svaret på spørsmålet som er stilt ovenfor. Det er for det første hensynet til likhet. Disse fundamentale tjenestene bør omfatte alle dem som de nasjonale myndigheter har ansvaret for. De må derfor være landsdekkende. Viktigheten av lik tilgang for alle forsterkes av at der ikke fins brukbare private alternativer. Den tryggheten som et nasjonalt forsvar gir, må gjelde alle. Rettstatens prinsipper og ordensmaktens beskyttelse av liv og eiendom må gjelde alle borgere uansett stand og stilling. Disse fundamentale likhetsprinsippene er riktig nok under press på noen områder. Men som kollektiv er vi på disse vitale områdene best tjent med offentlig eierskap til produksjonsmidler og infrastruktur og med et tjenestenivå som dekker alles behov på lik linje.

Det andre hensynet gjelder viktigheten av å opprettholde kvalitet. På noen områder vil en forringelse av kvaliteten, eller i verste fall bortfall av tjenesten kunne føre til irreparable konsekvenser. Når det gjelder Forsvaret er det åpenbart. Men også en undergraving av rettstaten kan føre til en uheldig utvikling som det kan være svært vanskelig å komme bort fra. Begge disse to fundamentale hensyn taler for full offentlig kontroll. Privatisert virksomhet underlagt offentlig regulering og kontroll føles utilstrekkelig på disse samfunnsbærende områdene. En mulig innfallsvinkel til eierskapsspørsmålet er hvor langt vi kan trekke tankegangen ovenfor, når det gjelder å identifisere hvilke typer kritisk infrastruktur som bør være i offentlig eie.

9.4 Eierskap til kritisk infrastruktur

Det vises til utvalgets definisjon av kritisk infrastruktur og kritiske samfunnsfunksjoner. Ut fra en vurdering av kriteriene for utpeking av kritisk

[2] Det har imidlertid i de senere år utviklet seg et marked for private sikkerhetstjenester som i de fleste tilfeller kan oppfattes som et supplement til det offentlige ordensvernet, men i noen tilfelle kan de også være konkurrerende.

infrastruktur, mener utvalget at landsdekkende kommunikasjonsnett, energinett og vann- og avløpsnett peker seg ut som svært kritisk infrastruktur. Med kommunikasjonsnett siktes det både til elektronisk kommunikasjon og til fysisk transport av personer og varer.

Foruten å være den viktigste energikilden både for husholdninger og næringsliv og for kritiske samfunnsfunksjoner (for eksempel helsetjenester), er elektrisk kraft også nødvendig for elektronisk kommunikasjon. Produksjon og distribusjon av elektrisk kraft er derfor kritisk både for kommunikasjon og livsviktig tjenesteyting, og for samfunnet for øvrig. Vannforsyning og avløp er viktig for liv og helse i et moderne samfunn. Svikt i disse tjenestene fører raskt til katastrofescenarier, spesielt i byer og bynære strøk. Elektroniske kommunikasjonsnett er det limet som binder det moderne samfunnet sammen. Det gjelder både fysiske kommunikasjonsnett som innenfor telesektoren, sømløse nett som mobilnettet, og globale nett som Internett. Elektronisk kommunikasjon er også viktig for fjernovervåking og fjernstyring av viktige samfunnsinnretninger, slik som moderne navigasjonssystemer og fjernstyring av olje- og gassvirksomheten i Nordsjøen. De ovennevnte nettverksfasilitetene har det felles at funksjonssvikt vil ha sektorovergripende konsekvenser. Når det gjelder fysiske transportnett, er fly, båt, bil og jernbane de viktigste.

Kritisk infrastruktur har i de fleste tilfeller karakter av essensiell innsatsfaktor i kommersiell tjenesteproduksjon rettet mot sluttbrukermarkeder. Stordriftsfordeler innebærer at de fremstår som naturlige monopoler slik at det fra et kostnadsmessig synspunkt synes å være samfunnsøkonomisk ulønnsomt å duplisere kritisk infrastruktur. Tidligere var de landsdekkende nettverksvirksomhetene innenfor telekommunikasjon og energi samt vann og avløp ansett som naturlige monopoler og organisert som vertikalt integrert offentlig monopolvirksomhet[3]. I løpet av de siste par tiår er den nettverksbaserte tjenesteproduksjonen innenfor telekommunikasjon, energiforsyning og postdistribusjon åpnet for konkurranse. Vann og avløp er fortsatt offentlig monopolvirksomhet, med konkurranseutsetting av visse funksjoner.

I tillegg til at nettverksfasilitetene på disse sentrale områdene er nødvendig for den løpende tjenesteproduksjonen, er et påregnelig og funksjonsdyktig nettverk en kritisk ressurs for ivaretakelse av sikkerhet og beredskap på viktige samfunnsområder. En potensielt fruktbar innfallsvinkel kan være å se på de nevnte nettverksvirksomhetene som produsenter av dels transmisjons- og distribusjonstjenester som omsettes i markedet, og dels fellesgoder i form av beredskap og sikkerhet som retter seg mot alle som betrakter muligheten for tilgang til et funksjonsdyktig nett som viktig i seg selv uansett om de selv benytter det eller ikke. For post- og telenett blir for øvrig landsdekning betraktet som en samfunnsoppgave med karakter av fellesgode.

Som for fellesgoder generelt er det vanskelig å innkassere betalingsvilligheten i markedet. Selv om skillet ikke alltid er helt klart, kan en i de fleste sammenhenger skille mellom nettets løpende bruksverdi og dets eksistensverdi. Det siste går på verdien av å ha muligheten for tilgang til et velfungerende nett når behovet måtte melde seg. En kan kanskje si at eksistensverdien fanger opp beredskapsaspektet. På disse områdene knytter eksistensverdien seg til påregneligheten og leveringssikkerheten. Bruksverdien blir innkassert i markedet ved den løpende prisingen av nettbruken. Verdien for samfunnet av leveringssikkerhet blir imidlertid ikke fullt ut fanget opp i inntektene fra den løpende bruk av nettet.

Ved regulert privat eierskap og produksjon, som for eksempel ved inntektsrammeregulering, kan det bli et for ensidig fokus på den bedriftsøkonomiske bunnlinjen ved at incentivene til å investere i beredskap og sikkerhet begrenses av at en kan innkassere avkastningen i form av en markedsmessig inntekt. Siden dette er goder som har et fellesgodeaspekt, vil det være vanskelig å høste den samfunnmessige avkastningen på slike investeringer fullt ut i markedet.

En mulig måte å bringe kostnadene ved ufullstendig beredskap og sikkerhet inn i bedriftenes kalkyler på, er å gjøre dem økonomisk ansvarlig for kostnadene ved funksjonssvikt. Det er denne tankegangen som ligger bak ordningen for kompenasjon for ikke levert energi (KILE-ordningen). For funksjonsvikt med moderate konsekvenser kan slike ordninger virke etter hensikten og på denne måten bidra til å optimalisere ressursbruken. Men for mange av de katastrofescenariene som kan inntreffe ved at kritisk infrastruktur blir satt ut av spill, vil kostnadene være så formidable at slike kompensasjonsordninger ville bryte sammen. De vil da ikke være troverdige, og vil derfor ikke ha den ønskede virkning. Det synes derfor å være nødvendig med direkte krav til sikkerhet og beredskap for å dekke slike scenarier.

[3] Vertikal integrering: Samme virksomhet eier både den underliggende infrastrukturen og produksjonen som infrastrukturen understøtter.

Beredskap og sikkerhet er et klart myndighetsansvar. I den tiden nettverksvirksomhetene var vertikalt integrerte offentlig eide monopoler, ble innsats for sikkerhet og beredskap dels finansiert fra et samlet distribusjons- og tjenestemarked og dels av det offentlige ved finansiering over statsbudsjettet. Det gjaldt for eksempel både telekommunikasjon og postdistribusjon. Når de tidligere offentlige nettmonopolene er blitt privatisert og åpnet for konkurranse, er det et problem at ansvaret for sikkerhets- og beredskapstiltak knyttet til den kritiske nettfasiliteten fortsatt hviler på netteieren, samtidig som netteieren i noen tilfelle skal konkurrere i tjenestemarkedene med operatører uten egne nett og følgelig ikke er pålagt slike samfunnsoppgaver. Konkurranse i tjenestemarkedene kan da vri fokus og innsats mot de kommersielle tjenestene på bekostning av preventiv innsats for sikkerhet og beredskap knyttet til den kritiske infrastrukturen.

Utvalget mener at det offentlige, ut fra en sikkerhetsmessig «føre-var»-betraktning, bør eie virksomheter som har ansvar for å legge premissene for de strategiske beslutningene som skal sikre at infrastrukturen blir utviklet, driftet og vedlikeholdt (systemoperatører). Dette er virksomheter som ikke selv eier forbindelsene som inngår i infrastrukturen, men som har som oppgave å opptre nøytralt i forhold til produsentene. Gassco er et eksempel på et selskap som har ansvar for drift og vedlikehold og å samordne utvikling av rørsystemet offshore, uten å eie forbindelsene selv. Forbindelsene er eid av kommersielle selskap som har konsesjon for olje- og gassutvinning. Gassco vurderer også planlagt vedlikehold av alle forbindelser og godkjenner og kontrollerer dette. Operativ systemdrift blir utført av Gassco.

Utvalget har ikke vurdert de sikkerhetsmessige konsekvensene av at en tilsvarende modell i sin helhet hadde blitt innført på kritiske infrastrukturer på land. Statnett har et systemansvar for kraftsystemet og delegerer i prinsippet systemansvaret videre til distributører. Statnett eier dessuten brorparten av forbindelsene i sentralnettet. Øvrig andel eies av kommersielle aktører, selv om disse stort sett er offentlige (og er gjenstand for inntektsregulering). Utvalget anser at sikkerhet og beredskap blir vel ivaretatt med denne modellen.

Systemoperatører av kritisk infrastruktur må sikre at nødvendige ressurser, både menneskelige og materielle, finnes for å drifte og håndtere feil og krisescenarier i nettene. Utvalget anser at private virksomheter vil kunne ha viktige oppgaver i denne sammenheng.

Dersom beredskaps- og sikkerhetshensyn til syvende og sist er et offentlig ansvar, må myndighetene i alle fall ha kontroll- og innsynsrett i virksomheten, som kan innebære pålegg av bestemte sikkerhetstiltak, om en finner det nødvendig. Det kan da bli et spørsmål om en oppnår så mye på kostnadssiden med å privatisere. Det gjelder i særlig grad dersom kostnadseffektivisering i mer snever forstand kan gå utover sikkerhet og beredskap i vid forstand.

Det foreligger så vidt utvalget kjenner til, ingen norske data som bekrefter at det sterke fokus på kostnadssiden ved privat eierskap går ut over andre samfunnshensyn. Utvalgets oppfatning bygger mer på en bekymring knyttet til det forholdet at samfunnets interesser vedrørende kritisk infrastruktur favner videre enn de rent bedriftsøkonomiske. Det er en risiko for at et sterkt fokus på kostnadseffektivisering kan komme til å gå på bekostning av innsats for sikkerhet og beredskap med mindre slike hensyn bygges eksplisitt inn i reguleringsregimet. Men i den sammenheng reises spørsmålet om reguleringsmyndigheten er i stand til å verifisere hva netteierne faktisk gjør for å redusere risikoen for funksjonssvikt og tiltak med sikte på reserveløsninger for å redusere sårbarheten i tilfellet infrastrukturen svikter.

9.5 Eiermessig skille eller integrasjon mellom forvaltning av kritisk infrastruktur og konkurransevirksomhet?

I lys av diskusjonen ovenfor ville det fra et regulatorisk synspunkt ha vært mest ryddig med selskapsmessig skille mellom nettverksfasiliteten i egenskap av kritisk infrastruktur og den nettbaserte produksjonsvirksomheten. På denne måten ville en få et klarere skille mellom samfunnsoppdraget knyttet til infrastrukturen på den ene siden og den kommersielle nettbaserte tjenesteproduksjonen (nedstrømsvirksomheten) på den andre. Denne problemstillingen gjelder både for telenettet, energinettet og postnettet.

Dersom den kritiske nettverksfasiliteten skilles ut som egen nettvirksomhet, oppstår spørsmålet om den bør være offentlig eller privat. Isolert sett trekker kostnadshensyn i retning av privatisering. Siden en privatisert nettvirksomhet i mange tilfelle er ensbetydende med et privat naturlig monopol, vil den ved privat eierskap måtte reguleres. Når nettvirksomheten skal forvalte nettverksfasiliteten på samfunnets vegne, vil det være mest naturlig å legge nettvirksomheten inn under det offentlige.

Det som taler mot vertikalt skille mellom nett og nettbasert tjenesteproduksjon, er tap av eventuelle synergigevinster mellom oppstrøms- og nedstrømsvirksomheten[4]. I telesektoren er dette blitt fremholdt som et viktig argument mot å skille ut fastnettet som en egen offentlig eiet, eller regulert privat eiet, nettverksvirksomhet. I de aller fleste land finner en derfor at de tidligere offentlige telemonopolene driver teletjenesteproduksjon i konkurranse med private operatører samtidig som de fortsatt kontrollerer de deler av nettet som antas å være naturlig monopol, og som konkurrerende aktører er avhengig av tilgang til. Uten vesentlige strukturendringer i form av en konsentrasjon i energibransjen, vil det også her være tap av store synergigevinster ved et eiermessig skille mellom overføring av energi og strømleveranse til sluttbrukermarkedet.

Det har vært en rivende teknologisk utvikling innenfor IKT-sektoren i det siste tiåret. I denne perioden har det også vært en voksende erkjennelse av at de gamle statsmonopolene er for lite tilpasningsdyktige til å kunne følge med på denne utviklingen, samtidig som det å være i fronten for utviklingen innenfor IKT-sektoren er ansett for å være svært viktig for et lands teknologiutvikling og konkurranseevne. Beslutningsstrukturen i offentlig virksomhet er hierarkisk og beslutningsprosessene i stor grad regelstyrt, slik at det kan være grunn til å tro at det ikke er tilstrekkelig fleksibilitet i beslutningssystemet til at offentlig virksomhet kan hevde seg i den sterke innovasjonskonkurransen som nå preger spesielt denne sektoren. Parallelt med omreguleringen innenfor sektoren har derfor de gamle statseide monopolene blitt helt eller delvis privatisert. Den samme utviklingen har vi sett innenfor postdistribusjon.

Den sentrale avveiningen med hensyn til eierskap til kritisk infrastruktur vil derfor dels gå på ønskeligheten av vertikalt skille mellom eierskap til infrastruktur og konkurransevirksomhet, og ved eventuelt skille dels gå på om infrastrukturen bør være privat eller offentlig eiet. Regulatorisk enkelhet taler for et skille, da den regulerte monopolvirksomheten i dette tilfellet får en mer ensartet og oversiktlig agenda.

Dette tilsier offentlig eierskap. Privat eierskap ville her i de fleste tilfeller bety privat monopolvirksomhet og i valget mellom offentlig enerettsvirksomhet og regulert privat monopolvirksomhet, vil offentlig eierskap være å foretrekke, spesielt på områder der reguleringssvikt kan ha store negative konsekvenser.

På den annen side vil sterk synergi mellom underliggende infrastrukturvirksomhet og konkurransevirksomhet tale for vertikal integrasjon. Dette er trolig tilfelle for vannforsyning og avløp. Siden dette er naturlig monopolvirksomhet, er det lite hensiktsmessig med konkurranse, og i valget mellom privat og offentlig monopolvirksomhet, er det mye som taler for offentlig eierskap. Om derimot vertikal integrasjon er mest hensiktsmessig og nedstrømsmarkedet i tillegg er et konkurransemarked, taler regulatorisk ryddighet for privat eierskap til den integrerte virksomheten. Ved dette unngår en mistanke om at myndighetene ikke klarer å etablere tilstrekkelig armlengde mellom sin eierrolle og regulatørrollen. Av aktuelle virksomheter her er først og fremst post og tele[5].

Et annet og kultur- eller samfunnshistorisk argument for offentlig eierskap, er at på grunn av vår historie der mesteparten av det som kan defineres som kritisk infrastruktur har vært i offentlig eie, sitter det offentlige fortsatt med hovedtyngden av den nasjonale kompetansen på mange av disse områdene. I valget av regulatoriske løsninger og eierformer kan en ikke se helt bort fra at den riktige veien videre uansett vil være avhengig av hvordan vi er kommet dit vi er i dag. Slik «stiavhengighet» *(path dependency)* taler for at de institusjonelle løsninger som vi velger for det vi definerer som kritisk infrastruktur, ikke bør bryte for mye med hvordan dette er blitt håndtert tidligere. Dette taler i favør av offentlig eierskap. Det er likevel viktig å vurdere alle muligheter for mer effektiv bruk av knappe ressurser. Når det gjelder eierskap til kritisk infrastruktur, må likevel virkninger for sikkerhet og beredskap veie tungt.

9.6 Forholdet mellom regulering og eierskap som virkemiddel

Utvalget tviler på at problemer knyttet til ansvar og adekvat innsats for beredskap og sikkerhet kan løses på en fullgod måte ved regulatoriske inngrep i forhold til privat sektor for den infrastrukturen som er mest kritisk for samfunnets funksjonsdyk-

[4] Oppstrømsaktiviteter: Aktiviteter eller virksomhet på det forutgående trinn i en produksjons- og/eller distribusjonskjede.
Nedstrømsaktiviteter: Aktiviteter eller virksomhet på det neste trinn i en produksjons og/eller distribusjonskjede.
Eksempel: Produksjon av biler er oppstrømsaktivitet; salg av biler er nedstrømsaktivitet. Vedlikehold og investeringer i det faste telefonnettet er oppstrømsvirksomhet. Bruk av fastnettet til nettbaserte telefonitjenester er nedstrømsvirksomhet.

[5] I Norge er dette problemet løst ved opprettelsen av det uavhengige Post- og teletilsynet.

tighet og borgernes sikkerhet. Virkemidlene må i størst mulig grad rettes inn mot de forhold som er de fundamentale drivkrefter bak atferd og økonomisk tilpasning. Da er det tale om incentivene som ligger til grunn for økonomiske disposisjoner både i privat og offentlig sektor. Det viktigste å notere seg i den sammenheng er at bunnlinjen både er, og bør være, forskjellig for private og offentlige eiere, og derfor vil også incentivene være forskjellige.

Forskjellene går først og fremst ut på at det offentlige har et særlig ansvar for å opprettholde et adekvat tilbud av vitale tjenester som ikke kan tilbys i ønsket omfang på et kommersielt grunnlag i markedsbasert virksomhet. For et gitt tjenestetilbud, både kvantitativt og kvalitativt, krever hensynet til effektiv ressursbruk at også det offentlige driver med så lave kostnader som mulig. Som påpekt foran, kan det argumenteres for at privat virksomhet er gjennomgående mer kostnadseffektiv enn offentlig. Isolert sett taler dette for offentlig regulert privat eierskap til kritisk infrastruktur. Utvalget mener likevel at det er en risiko for at regulering av privates innsats for beredskap og sikkerhet ikke vil gi samfunnet en ønskelig grad av sikring. I betraktning av at funksjonssvikt i kritisk infrastruktur kan ha irreparable samfunnmessige konsekvenser og at myndighetene uansett må ha det endelige ansvaret som *«provider of last resort»* når det gjelder samfunnskritiske tjenester, mener utvalget at dette alt i alt taler for offentlig eierskap.

I den globaliserte økonomien har kostnadskutting og internasjonal konkurranseevne blitt av overordnet betydning både for å være attraktive for internasjonale investorer på kort sikt og for å overleve på lengre sikt. I et slikt scenario er det fare for at innsats for viktige nasjonale samfunnsverdier vil måtte vike dersom det skal ivaretas av kommersielle aktører.

Dersom det skal løses ved lovregulering, vil det kunne kreve inngrep som forrykker konkurransevilkårene mellom virksomhet lokalisert hjemme og ute og dermed også påvirke fremtidig lokalisering i den utstrekning virksomheten er mobil. På lang sikt er all virksomhet mobil, da inngrep som forringer avkastningen på nasjonale investeringer kan medvirke til nedbygging av nasjonal virksomhet ved at kapitalen omplasseres til land med gunstigere rammebetingelser. Det gjelder både for nasjonale og internasjonale investorer.

Et viktig motiv for privatisering har vært at profittmaksimerende private aktører av flere grunner normalt vil være mer kostnadseffektive enn det offentlige. Men dersom det offentlige må ha en tung hånd på rattet via lovregulering for å få dem til å iaktta kritiske nasjonale samfunnshensyn, faller et viktig poeng med privatisering bort. Regulering av privat virksomhet med ansvar for kritisk infrastruktur kan skape problemer knyttet til konkurransenøytralitet både innenlands og i forhold til utlandet. Dertil kommer at det i praksis kan være vanskelig for myndighetene å observere hva private bedrifter faktisk gjør med hensyn til beredskap og sikkerhet slik at effekten av lovregulering kan bli lite målrettet. Ovenfor nevnte argumenter trekker derfor etter utvalgets oppfatning i favør av offentlige eierskap som det mest egnede virkemiddel når det gjelder kontroll med den infrastrukturen som er mest kritisk, samtidig som det skaper større grad av «*levelled playing fields*» (dvs. like rammebetingelser) i privat sektor.

Det er likevel to sektorer der streng lovregulering av privat virksomhet for å ivareta samfunnsmessige hensyn neppe vil ha særlige konsekvenser for virksomhetenes internasjonale konkurranseevne og lokalisering. Det gjelder grunnrentesektorene olje og gass og vannkraftbasert kraftproduksjon. Her er ressursbasen fullstendig immobil og grunnrenten oppstår ved at naturressursen foreligger gratis fra naturens hånd. og den kan dermed betraktes som den avkastningen som tilfaller «naturen». Det offentlige har tiltatt seg eiendomsretten til både olje- og gassressursene og til det meste av vannkraftreservene og innkasserer i kraft av sitt eierskap grunnrenten på samfunnets vegne. I disse to sektorene vil neppe regulatoriske inngrep ha særlig betydning for konkurranseevnen i forhold til andre sektorer så lenge reguleringskostnadene ikke eliminerer hele grunnrenten. For eksempel er interessen for å være med på norsk sokkel fortsatt stor til tross for ekstraskatten på oljeinntekter og strenge nasjonale krav til sikkerhetstiltak.

I olje- og gassvirksomheten er lete-, utvinnings- og salgsvirksomhet satt bort til både utenlandske og nasjonale private operatører og det samme kunne vel i og for seg ha vært mulig også for produksjon av elektrisk kraft der grunnrenten kunne hentes inn av Staten gjennom kraftverksbeskatningen. Forskjellen mellom de to sektorene er likevel at en svikt i elektrisitetsforsyningen vil kunne ha store sektorovergripende konsekvenser mens i offshore-virksomheten vil kostnadene i større grad bæres av det enkelte selskap når vi ser bort fra store forurensningsproblemer.

9.7 Utvalgets anbefalinger

Behovet for sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner er i utgangspunktet uav-

hengig av organiseringen av eierskapet til de underliggende systemer, installasjoner, anlegg og produksjonsfasiliteter. Spørsmålet er imidlertid om offentlig eierskap kan gjøre det enklere og i noen tilfelle kan være en forutsetning for at det offentlige på en tilfredsstillende måte skal kunne ivareta ansvaret for en intakt og velfungerende infrastruktur som anses som helt nødvendig for å opprettholde kritiske samfunnsfunksjoner, samfunnets grunnleggende behov og befolkningens trygghetsfølelse.

Utvalget har festet seg ved tre ulike generiske trekk ved kritisk infrastruktur som kan tale for offentlig eierskap som den mest hensiktsmessige måten å ivareta det offentlige ansvaret på. Det er for det første en kritisk avhengighet av infrastrukturen når det gjelder å opprettholde et tjenestetilbud rettet mot tilfredsstillelse av grunnleggende behov. For det andre at det ikke finnes tjenlige alternativer som kan erstatte infrastrukturen om den skulle falle ut. Den blir dermed helt nødvendig for forsyningssikkerhet av kritiske tjenester og for opprettholdelse av kritiske samfunnsfunksjoner. Disse to egenskapene, kritisk avhengighet og absolutt nødvendighet, som er to relaterte aspekter ved kritikalitetskriteriet, har som konsekvens at funksjonssvikt, uansett grunn, i verste fall vil kunne føre til katastrofale og i noen tilfelle irreparable konsekvenser for individer og samfunn. Siden det offentlige uansett eierskap vil sitte med sluttansvaret for å organisere reserveløsninger og oppretting i tilfelle slik funksjonssvikt, tilsier det at det offentlige også må ha full kontroll over bruk og vedlikehold av kritisk infrastruktur. En slik kontroll sikres best ved offentlig eierskap. En tredje egenskap er tett kobling. Dette kan gjelde mellom ulike komponenter innenfor ett og samme system slik at svikt i én komponent fører til at hele systemet svikter. En annen variant av tett kobling kan skyldes avhengighet mellom systemer slik at svikt i ett system, har negative virkninger for funksjonaliteten i andre systemer og at det dermed får sektorovergripende konsekvenser. Tett kobling, enten det er innenfor et system eller mellom systemer, taler for sentralisert styring og nasjonal kontroll. Begge deler sikres best ved offentlig eierskap.

Disse generiske trekkene ved kritisk infrastruktur er i varierende grad til stede innenfor flere samfunnssektorer. Offentlig eierskap som virkemiddel må derfor vurderes konkret innenfor hver enkelt virksomhet og sektor. Det er viktig at valg av eierskap skjer på grunnlag av en helhetsvurdering der ønskeligheten av offentlig kontroll veies opp mot eventuelle bedriftsøkonomiske fordeler ved privat eierskap. Utvalget vil likevel understreke at ved denne avveiningen må hensynet til samfunnmessig sikkerhet og beredskap veie tungt for infrastruktur som har karakter av å være kritisk (jf. kriteriene ovenfor).

Utvalget vil på generelt grunnlag peke på at vann- og avløpsnett tilfredsstiller kravet om kritisk avhengighet og absolutt nødvendighet både for vannforsyning og avløpstjenester i og med at de er lokalt naturlige monopoler slik at det ikke fins brukbare alternativer. Utover dette peker deler av elektrisitetsnettet, og elektroniske kommunikasjonsnett seg ut; førstnevnte ved at ulike delnett i forsyningskjeden fra produksjon til sluttbruker er tett koblet, og for begge nett ved at funksjonssvikt vil ha sektorovergripende konsekvenser. Fysiske transportnett er også viktige for et velfungerende samfunn, men i mange tilfeller kan det være brukbare alternativer om bestemt transportform blir blokkert. Til slutt vil utvalget peke på at olje- og gassvirksomheten inntar en slik dominerende plass i norsk økonomi at fysiske installasjoner på norsk sokkel og transportnettet for olje og gass må anses som kritisk infrastruktur for det norske samfunnet. Det spesielle for denne sektoren er imidlertid at det i stor grad vil være sammenfall mellom bedrifts- og samfunnsøkonomiske konsekvenser av funksjonssvikt i infrastrukturen. Det enkelte selskap vil derfor her i større grad ha et privatøkonomisk motiv til å ivareta samfunnsøkonomiske interesser med hensyn til sikkerhet og beredskap knyttet til infrastrukturen.

Utvalget vil for øvrig vise til at disse spørsmålene i høyeste grad kan være av politisk karakter. Det anses derfor som avgjørende å sikre mekanismer som medfører hensiktsmessig kommunikasjon og avklaring med politiske myndigheter ved spørsmål om endret organisering og eierskap av kritisk infrastruktur. Utvalget viser i denne forbindelse til utvalgets anbefaling om bruk av kontrollpunkter for omorganiseringer og omstruktureringer av offentlig virksomhet i kapittel 8.5.1.

Utvalget viser for øvrig til sine vurderinger og anbefalinger knyttet til eierskap som virkemiddel på disse områdene i kapittel 10.

Kapittel 10
Kartlegging av kritisk infrastruktur og sektorvise anbefalinger

Det fremgår av utvalgets mandat at det skal kartlegge virksomheter som antas å ha betydning for rikets sikkerhet og vitale nasjonale interesser. På denne bakgrunn har utvalget tolket mandatet til å omfatte en kartlegging av kritisk infrastruktur og kritiske samfunnsfunksjoner.

Det er foretatt en kartlegging av et bredt utvalg av virksomheter for å avdekke hvilke som faller inn under begrepene kritisk infrastruktur og kritiske samfunnsfunksjoner. Med bakgrunn i den informasjon utvalget har innhentet gjennom sin møteaktivitet og dialog med offentlige og private virksomheter, har utvalget laget en indikativ liste over kritisk infrastruktur og kritiske samfunnsfunksjoner. Denne oversikten har vært benyttet som arbeidsunderlag for utvalget både i forhold til vurdering av virkemidler og i forbindelse med beskrivelse av de enkelte sektorer. Dokumentet er sikkerhetsgradert.

For å orientere seg nærmere om enkelte sentrale virksomheter har utvalget også innhentet informasjon om virksomhetenes virkeområder, eierstrukturer, organisering, bemanning og økonomi. Dette er informasjon som har dannet grunnlaget for omtalen i de etterfølgende kapitler i rapporten. Deler av arbeidet er basert på sårbarhetsutvalgets kartlegging av sårbarheter innenfor en rekke samfunnssektorer, herunder sårbarheten i kritisk infrastruktur og kritiske samfunnsfunksjoner.

I dette kapittelet gis en beskrivelse av de kritiske infrastrukturene innen elektronisk kommunikasjon, satellittbasert virksomhet, kraft, vann- og avløp, olje- og gass og transport. Som en del av disse beskrivelsene redegjøres det også for de kritiske samfunnsfunksjonene som knytter seg direkte til de kritiske infrastrukturene. Virkemidler for å ivareta rikets sikkerhet og vitale nasjonale interesser beskrives og vurderes innenfor hvert av områdene. I kapittel 11 gis en beskrivelse av kritiske samfunnsfunksjoner som utvalget har valgt å trekke frem.

10.1 Elektronisk kommunikasjon

Behovet for fungerende kommunikasjonstjenester har i løpet av et par tiår blitt så sterkt at det knapt er noen annen sektor som kan greie seg særlig lenge ved svikt i kommunikasjonsnett, -tjenester og -systemer. Ved siden av kraftforsyningen er elektronisk kommunikasjon avgjørende for opprettholdelse av vitale tjenester i samfunnet.

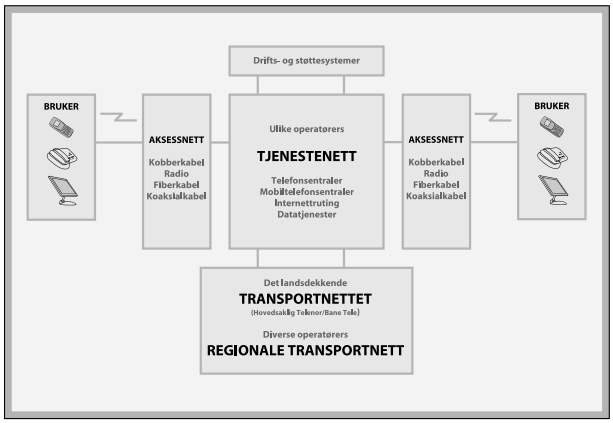
Informasjons- og ledelsesapparatet som trer i kraft ved katastrofer og kriser vil ha store problemer dersom telekommunikasjonen faller ut. Selv om det tilsynelatende kan se ut til at det står flere separate kommunikasjonssystemer til rådighet, er disse i virkeligheten ofte avhengig av de samme transportnettene.

Dataoverføring mellom ulike komponenter i styrings- og produksjonssystemer skjer i stadig større grad via Internett. Dette er mulig fordi man kan etablere såkalte virtuelle private nettverk i det ellers åpne Internett. På den måten kan virksomheter unngå å leie egne og kostbare dedikerte samband. At mange virksomheter går over til slike løsninger gjør selvfølgelig Internett til en enda mer kritisk infrastruktur.

På en del områder finnes det fortsatt reserveløsninger som kan virke en stund ved utfall av tele- og datakommunikasjon. Tendensen er likevel at sanntidskommunikasjon i stadig større grad er en forutsetning for at systemene skal virke som forutsatt.

En rekke kritiske funksjoner som dekker samfunnets grunnleggende behov er avhengig av elektroniske kommunikasjonsnett og -tjenester. Kommunikasjonsnettene utgjør en felles infrastruktur som praktisk talt alle de øvrige sektorene er avhengig av. På liknende måte som for kraftforsyningen er det landsdekkende transportnettet (og i noen grad regionalnettet) særlig viktig. De aller fleste leverandører/tilbydere av elektroniske kommunikasjonstjenester er avhengige av det landsdekkende transportnettet som eies av Telenor ASA. (se likevel nedenfor om BaneTele).

Kommunikasjonsnettene har også i en viss grad karakter av å være et tett koblet system, i den forstand at feil kan spre seg i store deler av nettet. Etter hvert som Internett-teknologi blir bærer av tjenester i stadig større utstrekning vil dette antakelig bli enda mer fremtredende. Stadig sterkere sentraliserte styringssystemer bidrar til sterkere



Figur 10.1 Prinsippskisse elektronisk kommunikasjonsinfrastruktur.

grad av tett koblede systemer. Omfattende driftstans kan eksempelvis oppstå etter logiske og fysiske angrep, naturhendelser og brann.

Sårbarhet som følge av avhengighet av IKT-systemer er sentralt i prosjektet BAS 5 (BAS: Beskyttelse av samfunnet). Prosjektet ledes av FFI, med økonomisk støtte fra Norges forskningsråd og en rekke offentlige etater. Formålet med prosjektet er å bidra til å redusere sårbarheten ved samfunnskritiske IKT-systemer, og derved gjøre disse mer robuste i forhold til ulike trusler, villede handlinger og ulykker. Prosjektet skal levere sluttrapport høsten 2006.

10.1.1 Overordnet beskrivelse av infrastruktur og samfunnsfunksjon

De grunnleggende elementene som til sammen utgjør infrastrukturen er
- aksessnettet
- transportnettet
- tjenestenettet
- drifts- og støttesystemer

Aksessnettet er den delen som knytter forbindelse mellom sluttbrukerne og transport- og tjenestenettene. Det er flere former for aksessnett. Det mest omfattende består av kobberledninger som er lagt i forbindelse med utbygging av fasttelefoni innenlands. Ett (eller flere) ledningspar knytter hver enkelt husstand/bedrift til nærmeste telefonsentral.

Et annet aksessnett utgjøres av ledninger mellom sluttbrukere og leverandører av radio/TV-signaler (kabel-TV gjennom coaxialkabler). I tillegg finnes i mindre omfang aksessnett som er realisert som radioforbindelse eller fiberkabel.

Transportnettet utgjør den delen av infrastrukturen som knytter forbindelser over lange avstander. Transportnettet er en felles betegnelse for nasjonale og regionale nett. Transportnettet benytter sambandssystem med stor kapasitet over kabel eller radiolinje. Det er flere virksomheter som eier og driver transportnett på regional basis, men kun Telenor og BaneTele eier og tilbyr nasjonal transportkapasitet basert på fiberoptoiske kabler.

Det finnes et eget transportnett for kringkasting. Dette er et landsdekkende nett som eies og drives av Norkring, et heleid datterselskap av Telenor. Dette transportnettet brukes til å formidle radio og TV-signaler til TV/FM-sendere rundt om i landet, i tillegg til at det benyttes for interne forbindelser mellom NRKs regionkontorer.

Distribusjon av radio- og TV-signaler til sluttbrukerne skjer i dag på tre måter: Som radiosignaler via TF/FM-sendere, som radiosignaler via satellittsendere og som elektriske signaler via nettene for kabel-TV. (Dessuten formidles i økende utstrekning signaler via Internett). I økende grad fremover vil overføring av multimediasignaler (TV, radio, Internett, telefoni og video) til sluttbrukere skje via fiber- og radioaksesser.

Tjenestenettene utgjøres av systemer og utstyr som er nødvendig for å levere de enkelte tjenestene, som for eksempel telefoni (fast og mobil) og Internettforbindelse. Disse benytter det samme transportnettet for å formidle informasjon mellom et antall tjenestenoder. Eksempel på tjenestenoder er telefonsentraler for formidling av telefoni og noder for Internettforbindelse.

Drifts- og støttesystemene kan utgjøre en kritisk del av infrastrukturen. Det er en tendens at funksjonene sentraliseres og styres ved hjelp av elektronisk kommunikasjon. Driftssenteret for et telesystem trenger ikke å ligge i det samme landet som systemet betjener. Etter hvert som operatører vokser i markedet, vil ønsket om å redusere kostnader ved driftsfunksjonene kanskje medføre en slik utvikling. Dersom, som følge av dette, kompetanse og bemanning med nærhet til utstyret forvitrer, vil det være en potensiell fare for at operatørens evne til å opprettholde tilgjengeligheten ved større feil- eller krisesituasjoner svekkes.

10.1.2 Særskilt om Internett

Internett er et verdensomspennende offentlig tilgjengelig datanettverk som benytter et felles sett av åpne standarder. Utviklingen startet som et forskningsprosjekt for å lage robuste, pakkesvitsjete datanettverk til militær bruk. Etter hvert utviklet Internett seg til å bli et nettverk for universitets- og forskningsmiljø, først som forskningsobjekt og etter hvert som kommunikasjonsnettverk. Kom-

mersialiseringen startet i begynnelsen av 90-årene og ble kraftig drevet fram av utviklingen av *World Wide Web*. Etter hvert har Internettstandardene også utviklet seg til å bli en meget viktig bærer for all digital kommunikasjon (telefoni, radio, datakommunikasjon og tv).

To sentrale designprinsipp nevnes ofte når Internetts egenart som datanettverk skal beskrives:

- Ende til ende prinsippet. En åpen arkitektur med et nøytralt nettverk gjør at alle kan være både kunder og tilbydere, og at alle kan utvikle og tilby tjenester og innhold på nettverket. Dette har ført til en voldsom utvikling av ulike tjenestetyper, systemer og innhold.
- Protokollene er uavhengig av underliggende framføringsveier – det vil si at en kan benytte Internettprotokollene på vilkårlige digitale nettverk (fysiske framføringsveier kan være kobberkabler, koaksialkabler, optisk fiber og forskjellige radiolinker).

Globalt sett er Internett organisert som et nettverk av nettverk. De administrativt adskilte nettverkene kalles autonome system og eies typisk av Internettleverandører. Avtaler om sammenkobling og trafikktransport mellom autonome system blir gjort bilateralt. Avtalene kan enten være vederlagsfrie eller inngås mot vederlag.

Internett er løst regulert og kontrollert. De tekniske standardene utvikles av *Internet Engineering Task Force (IETF)* som er knyttet til en åpen medlemsorganisasjon *(The Internet Society - ISOC)*. Ressurser som IP-adresser og domenenavn blir forvaltet av ICANN *(Internet Corporation for Assigned Names and Numbers)* på vegne av IANA *(Internet Assigned Numbers Authority)*. Dette er en ikkekommersiell organisasjon med funksjoner utkontraktert fra *US Department of Commerce.* IP-adresser blir fordelt til 5 regionale registrarer, mens domenenavn fordeles per toppnivånavn til uavhengige foretak eller nasjonale organisasjoner. Det norske toppdomenet (.no) forvaltes av Norid, under tilsyn av Post- og teletilsynet.

Det at nettverket er internasjonalt og i liten grad offentlig regulert, gjør det vanskelig å se på Internett som en uavhengig norsk infrastruktur. Både grunnleggende nettverkstjenester og ikke minst utkontrakterte system og virksomheter er helt avhengige av kommunikasjon på tvers av landegrensene.

Norge er i verdenstoppen når det gjelder tilgang til og bruk av Internett, og samfunnet er dermed tilsvarende avhengig av at nettverket er tilgjengelig og i stand til å yte sikre tjenester. Et eksempel som ofte trekkes fram er det faktum at nettbanktransaksjoner både for private og bedrifter nesten helt har overtatt for papirbaserte transaksjoner.

Bredbåndddekningen er høy[1], og stadig nye aksessmetoder blir tatt i bruk (for eksempel via trådløse nettverk, dedikerte fiberaksesser og mobiltelefoner). Internett har blitt viktig som kommunikasjonskanal for nesten alle typer virksomhet og etter hvert foregår også mye handel via Internett og Internettbaserte transaksjonssystemer. Den økte båndbredden fører til at digitale varer (film, musikk, osv) også kan leveres over Internett. De siste årene har en også sett utbredelse av IP-telefoni, både med og uten tilknytting til det tradisjonelle telefoninettet.

Også annen kritisk infrastruktur er avhengig av Internett i større og mindre grad. Internettprotokollene brukes veldig ofte til kommunikasjon, men da i nettverk som ikke nødvendigvis er tilknyttet Internett. Protokollene benyttes også som et lukket kjernenett for andre digitale nettverk (for eksempel er store deler av norsk fasttelefoni på vei over til et slikt nettverk).

10.1.2.1 Sårbarheter

I utgangspunktet er Internett-protokollene godt egnet for å lage redundante nettverk med høy tilgjengelighet. Dette er likevel helt avhengig av hvordan de enkelte leverandørene planlegger og konstruerer sine egne nettverk og tilkoblinger mot andre leverandører.

Internettprotokollene har i dag ingen funksjoner for å tilby autentisering, integritet eller konfidensialitet, og dette kan heller ikke enkelt implementeres i selve protokollene. I stedet legges slike sikkerhetsmekanismer inn på et høyere lag, alt etter behov. For eksempel vil en kanskje ikke ha brukerautentisering for åpent tilgjengelige nettaviser, mens det for nettbanker er meget viktig. Tekniske standarder for slike sikkerhetsmekanismer er forholdsvis modne og vidt tilgjengelige, men de blir på flere områder ikke tatt i bruk.

En hovedutfordring er programvaresikkerhet. Sårbarheter som oppdages i programvare som benyttes på Internett blir etter kort tid utnyttet til innbrudd i datasystemer eller til spredning av ondsinnet programvare. Mens slike angrep tidligere som regel var motivert av ren nysgjerrighet eller økt status i spesielle miljø, ser en nå at mer og mer av angrepene har økonomisk gevinst som mål. Foruten den stadig økende viktigheten av systemene

[1] 91 % av norske husstander hadde tilbud om bredbånd per august 2005.

og informasjonen de inneholder, har denne type kriminalitet flere spesielle aspekt ved seg. Angrepsmetodene er kopierbare, de spres fort og kan enkelt brukes mot mange mål samtidig. Videre har aktørene universell tilgang fra hele verden og har i tillegg en viss grad av anonymitet, gjerne oppnådd ved å gå via andre kompromitterte system.

Det finnes flere angrepsformer for å utnytte sårbarheter på Internett. En stor gruppe utgjøres av ondsinnet kode (virus, ormer, trojanere, spionprogrammer osv.). Tjenestenektangrep er en annen form som innebærer at offer-maskinen utsettes for så stor trafikk at kapasiteten blir brukt opp og det ikke lenger blir mulig å utføre normale oppgaver. Søppelpost («Spam») fremstår først og fremst som irriterende, men man skal ikke ignorere de mer alvorlige effektene dette kan ha om mengden blir stor.

Den tradisjonelle sikkerhetsmekanismen mot trusler fra Internett har vært fysisk eller logisk separasjon av nettverk, men en ser en tydelig utvikling mot lavere grad av separasjon. Fysiske skiller byttes ut med logiske skiller og logiske skiller åpnes. Begge deler er et resultat av økte krav til tjenester på tvers av skillene. Et forsterkende problem her er en utvikling mot bruk av hyllevareprodukter i system som tidligere ikke har vært utsatt for tilfeldige angrep fra ondsinnet programvare.

10.1.3 Beskrivelse av eierforhold og organisering

Etter at det norske telemarkedet ble åpnet for konkurranse 1. januar 1998 har det vært en akselererende utvikling i antall nye operatører og nye typer aktører. Ved utgangen av 2005 var det 156 operative aktører innenfor områdene fasttelefoni, mobiltelefoni, Internett og leide linjer. Til sammenlikning var det ved utgangen av 2003 101 aktive aktører[2]. Det har særlig vært en økning av tilbydere av tilgang til Internett (ISPer).

I forhold til behovet for å sikre den kritiske infrastrukturen er det mest interessant å se på de dominerende tilbyderne/operatørene innenfor denne sektoren.

Som nevnt er transportnettet den viktigste bærebjelken for et fungerende telekommunikasjonssystem. Her er Telenor helt dominerende med sitt transportnett som er bygget ut over mange år. Andre operatører som leverer transporttjenester er i stor grad avhengig av Telenor som underleverandør.

Telenor er stadig den dominerende leverandør av teletjenester i Norge, både innenfor fasttelefoni, mobiltelefoni og Internett. Telenor er i dag et allmennaksjeselskap hvor staten har en eierandel på om lag 54 %.

En annen stor operatør i transportmarkedet er BaneTele AS, et heleid statlig aksjeselskap under Nærings- og handelsdepartementet. BaneTele AS har sitt utspring fra Jernbaneverket, og har senere kjøpt opp det konkursrammede selskapet Enitel. BaneTele eier ikke selv infrastrukturen som utgjør transportnettet, men har langsiktige leieavtaler med hhv. Jernbaneverket og de ulike eierne av nettet som Enitel også leide (av om lag 40 kraftselskaper). BaneTeles transportnett er et landsdekkende nett, og utgjøres hovedsakelig av fiberoptiske kabler. BaneTele og Telenor har en del felles infrastruktur i transportnettet ved en kombinasjon av felles fiberkabler og fremføringsveier. Bredbåndsnettene til Telenor og BaneTele er de to eneste kommersielle nettene som er landsdekkende, og disse nettene bærer det meste av kapasiteten for andre bredbåndsaktører.

I tillegg finnes et landsdekkende ikke-kommersielt transportnett som utgjøres av Forsvarets Digitale Nett (FDN). FDN er et telenett som er etablert for å dekke Forsvarets behov for teletjenester. FDN dekker i dag alle Forsvarets installasjoner over hele landet samt enkelte deler av offentlig forvaltning, og totalt antall brukere i FDN er om lag 50 000.

FDN har innebygde egenskaper som er viktige for å oppnå høy tilgjengelighet for brukerne, selv i situasjoner med betydelig degradering av transportnettet. De viktigste av disse egenskapene finner en i funksjoner for oppsetting og ruting av samband og i prioritetsfunksjonen. FDN har, som andre nett, automatisk omruting av trafikk ved brudd, i tillegg til at rutingsfunksjonen sørger for at det kan settes opp samband så lenge det er mulige veier igjen i et degradert transportnett.

Forsvaret har i en utredning nylig drøftet spørsmålet om bortsetting og/eller salg av deler av FDN til andre offentlige etater eller til private selskaper. Eventuelle beslutninger om dette er foreløpig utsatt.

Mobiltjenesteleverandøren NetCom AS er en stor og viktig aktør. Selskapet har et godt utbygd nett av base-stasjoner for GSM («tjenestenoder»), og en meget stor kundebase. NetCom er Norges nest største mobiloperatør, og tilbyr mobile kommunikasjonsløsninger. Selskapet eies av det svensk-finske konsernet TeliaSonera.

[2] Post- og teletilsynet

10.1.4 Utvalgets vurderinger og anbefalinger knyttet til virkemidlene

10.1.4.1 Eierskap som virkemiddel

Fra å bestå av et statlig forvaltningsorgan med ansvar for alle deler av telesektoren, har det skjedd en gradvis liberalisering og fristilling fra midten av 1980-tallet. I desember 2000 ble Telenor børsnotert og delprivatisert. I dag en det en lang rekke større og mindre aktører som betjener ulike deler av telemarkedet.

Problemstillinger knyttet til sikkerhet og beredskap var ikke de mest sentrale i forbindelse med fristillingen. Likevel ble det i flere stortingsmeldinger og proposisjoner på 90-tallet trukket frem en rekke oppgaver på teleområdet som er viktige ut fra spesielle samfunnshensyn. Slike oppgaver ble i telepolitikken omtalt som «spesielle samfunnspålagte oppgaver». Dette omfattet blant annet tjenester til totalforsvaret, nød- og sikkerhetstjenesten langs kysten og i nære havområder og ytelser til Svalbard.

St.prp. nr. 43 (1993-94) Om tilknytningsform for samferdselsbedriftene, behandlet spørsmålet om tilknytningsform for NSB, Postverket og Televerket. Sikkerhetsmessige hensyn ble trukket frem som ett av flere statlige mål på teleområdet. Samferdselsdepartementet foreslo i proposisjonen at det i stiftelsesdokumentet for Telenor skulle tas inn en spesiell bestemmelse om samfunnspålagte oppgaver.

De samfunnspålagte tjenestene hadde vært pålagt Telenor i konsesjon. Dette ble endret i lov av 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven). Målsettingen var blant annet å gi myndighetene virkemidler for å kunne styrke konkurransen, jf. Ot.prp. nr. 58 (2002-2003). Etter dette vil de samfunnspålagte oppgavene bli ivaretatt på annen måte enn gjennom konsesjon, enten som følge av avtale eller pålegg.

Eierskap har i varierende grad vært sett som et virkemiddel av skiftende regjeringer til å ivareta sikkerhet og beredskap.

Vurderinger og anbefalinger

Det er liten tvil om at transportnettet som eies og drives av Telenor utgjør en kritisk del av infrastrukturen i telesektoren. Utvalget mener at det i prinsippet ville være mest logisk med skille mellom nettverksfasiliteten og den nettbaserte produksjonsvirksomheten. På den måten ville en fått et klarere skille mellom samfunnsoppdraget knyttet til infrastrukturen på den ene siden og den kommersielle nettbaserte tjenesteproduksjonen (nedstrømsvirksomheten) på den andre.

Standardmodellen i den vestlige verden var å organisere telesektoren i vertikalt integrerte monopoler. Det som taler mot vertikalt skille mellom nett og nettbasert tjenesteproduksjon i dag, er tap av synergigevinster mellom oppstrøms- og nedstrømsvirksomheten. I telesektoren er dette blitt fremholdt som et avgjørende argument mot å skille ut fastnettet som en egen, offentlig eiet, eller regulert privat eiet nettverksvirksomhet.

I Norge skjedde det en gradvis omorganisering av telesektoren, som startet på slutten av 1980-tallet. I 1988 ble Televerkets monopol på terminalutstyr opphevet. En annen viktig milepæl var innføringen av konkurranse innen mobiltelefoni i 1991, da NetCom fikk konsesjon til å levere mobiltelefonitjenester. I 1995 ble Televerket omdannet til et statlig aksjeseslskap, Telenor, og i 1998 ble Telenors monopol på fasttelefoni opphevet.

Ikke i noen land det er naturlig å sammenligne seg med har det gamle «stamnettet», som utgjør kjernen i telesystemene mange steder, blitt løftet ut og organisert som statlig foretak i løpet av omorganiseringsprosessen. En kan derfor snakke om «stiavhengighet» på dette området. Også for Norges del er utviklingen kommet så langt at den i praksis må betraktes som irreversibel. I de aller fleste land finner en derfor at de tidligere offentlige telemonopolene driver tjenesteproduksjon i konkurranse med private operatører samtidig som de fortsatt kontrollerer de deler av nettet som antas å være naturlig monopol, og som konkurrerende aktører er avhengige av tilgang til.

Det har vært en rivende teknologisk utvikling innenfor IKT-sektoren i det siste tiåret. I denne perioden har det også vært en voksende erkjennelse av at de gamle statsmonopolene er for lite tilpasningsdyktige til å kunne følge med på denne utviklingen. Samtidig er det å være i front av utviklingen innenfor IKT-sektoren ansett for å være avgjørende for et lands teknologiutvikling og konkurranseevne.

Når vertikal integrasjon er mest hensiktsmessig og nedstrømsmarkedet i tillegg er et konkurransemarked (slik som telesektoren), taler regulatorisk ryddighet for privat eierskap til den integrerte virksomheten. Ved dette unngår en mistanke om at myndighetene ikke klarer å etablere tilstrekkelig armlengde mellom sin eierrolle og regulatørrollen.

Utvalget mener det er viktig at eierskap til infrastruktur som er kritisk for landet bør være under kontroll av norske eiere. Dette vil gjøre at norske interesser i størst mulig grad ligger til grunn for

strategiske beslutninger. Om nødvendig bør dette sikres ved at det offentlige har tilstrekkelig eierandeler i de aktuelle selskapene.

10.1.4.2 Regulatoriske virkemidler

Lovverket overfor telesektoren og andre former for elektronisk kommunikasjon har vært gjenstand for betydelige endringer i løpet av de siste 10-15 årene. Et hovedmål med det regulatoriske rammeverket har vært å legge til rette for overgangen fra monopol til konkurranse i telesektoren.

I 2003 ble teleloven opphevet og erstattet av en egen lov om elektronisk kommunikasjon, *ekomloven*. Den dekker alle former for elektronisk kommunikasjon, ikke bare den tradisjonelle mobil- og fasttelefonivirksomheten. Loven omfatter både regulering av priser og tilgang og sikkerhets- og beredskapshensyn. I tilknytning til loven er det også utarbeidet et sett av forskrifter, hvor den såkalte *ekomforskriften* er den sentrale. Ekomloven og -forskriften gir Samferdselsdepartementet og Post- og teletilsynet sentrale roller i reguleringen av sektoren, også ivaretakelse av sikkerhets- og beredskapshensyn.

Lovens *formål* er å sikre brukerne i hele landet gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester. Det overordnede virkemidlet er konkurranse i alle ledd i sektoren.

Tilbydere med *sterk markedsstilling* kan pålegges særskilte forpliktelser. Begrepet sterk markedsstilling er definert i loven ved at tilbyderen «alene eller sammen med andre har økonomisk styrke i et relevant marked som gjør at tilbyder i stor grad kan opptre uavhengig av konkurrenter, kunder og forbrukere». Den aktuelle tilsynsmyndigheten kan benytte en rekke forskjellige virkemidler som pålegg om tilgang, krav om offentliggjøring av leveringsvilkår og regulering av priser for ulike tjenester. Eksempler på slike krav finnes i ekomforskriftens § 2-3, § 2-5 og § 2-6, hvor tilbyder med sterk markedsstilling pålegges å tilby overføringskapasitet til andre tilbydere og øvrige brukere, tilgang til fast aksessnett og samlokalisering.

Post- og teletilsynet og Samferdselsdepartementet har et særlig ansvar for beredskap og sikkerhet i ekomsektoren gjennom bestemmelsene i ekomloven og -forskriften. I tillegg finnes det flere andre myndighetsorganer med ansvar for beredskap og sikkerhet som også har oppgaver innen elektronisk kommunikasjon, som Nasjonal Sikkerhetsmyndighet og Forsvaret.

Bestemmelsene i ekomloven bygger på den tidligere reguleringen av beredskap og sikkerhet i telesektoren slik den er blitt utviklet i årene etter dereguleringen, men er også betydelig videreutviklet for å tilpasses den nye markedssituasjonen. St.meld. nr. 47 (2000-2001) inneholder en analyse av situasjonen etter dereguleringen og forslag til tiltak. De sentrale trekkene i regelverket er følgende:

- Regelverket omfatter i prinsippet samtlige tilbydere og ikke bare Telenor, noe som åpenbart er nødvendig i lys av at mange brukere, også viktige samfunnsaktører, kjøper tjenester og tilgang til kommunikasjonsnett fra andre aktører enn Telenor.
- Telenor har tidligere hatt vilkår i sin konsesjon om å utføre spesielle samfunnspålagte oppgaver (SSO). Disse er ikke lenger en del av Telenors konsesjon, men ivaretas gjennom det generelle regelverket, som altså kan gjøres gjeldende overfor alle tilbydere av ekomtjenester. Post- og teletilsynet har inngått avtale med Telenor for 2005 om videreføring av tiltak i den tidligere SSO-avtalen, og har planer om å inngå tilsvarende avtaler med andre tilbydere som skal gjelde fra 2006.

Ekomlovens § 2-10 stiller krav til tilbydere av elektroniske kommunikasjons- og nettjenester om at de skal opprettholde nødvendig sikkerhet og beredskap, herunder prioritere viktige samfunnsaktører ved behov. Myndighetene kan stille detaljerte krav om tiltak for å ivareta beredskaps- og sikkerhetshensyn gjennom forskrifter, enkeltvedtak eller avtaler. Tiltakene kan omfatte alt fra beredskapsplanlegging, øvelser, fysisk sikring av viktige installasjoner, formidling av informasjon fra statlige myndigheter til innføring av spesielle funksjoner og tjenester i kommunikasjonsnett, driftssystemer og driftsorganisasjoner. Kapittel 8 i ekomforskriften inneholder en rekke slike krav:

- Alle tilbydere som leverer elektroniske kommunikasjonstjenester direkte, eller som leverer overføringskapasitet og samtrafikk til leverandører, til brukere med samfunnskritisk funksjon skal ha oversikt over slike brukere og hvilke tjenester som er nødvendige for at brukeren skal kunne utføre sine funksjoner (§ 8-1).
- Alle tilbydere av ekomtjenester til brukere med samfunnskritisk funksjon skal lage planer og gjennomføre tiltak som er nødvendige for å opprettholde egen beredskap og for at brukere med samfunnskritisk funksjon skal kunne ivareta sine beredskapsoppgaver.
- Det kan stilles krav om at tilbydere skal kunne opprettholde nødvendig tjenestetilbud for brukere med samfunnskritiske funksjoner uten driftsstøtte og elektroniske kommunikasjons-

tjenester lokalisert i andre land (dette kravet omtales gjerne som krav om nasjonal autonomi).
– Tilbydere av ekomtjenester skal gi prioritet til brukere med samfunnskritiske funksjoner i krise- og beredskapssituasjoner.

Tiltakene nevnt ovenfor er primært rettet inn mot ekstraordinære hendelser. Lovverket inneholder i tillegg en rekke bestemmelser for å ivareta hensyn til tilgjengelighet, konfidensialitet og integritet også i normale driftssituasjoner.[3]

Det finnes ennå ingen komplett landsomfattende statistikk over tilgjengeligheten og kvaliteten på infrastrukturene for elektronisk kommunikasjon. Det har vært enkeltepisoder hvor omfattende avbrudd har funnet sted som følge av tekniske feil, tredjepartsaktivitet i form av gravearbeider eller lignende, både i mobilnett og fasttelefoninett. Disse avbruddene har imidlertid ikke ført til omfattende kriser eller truet nasjonal sikkerhet (men har åpenbart gitt samfunnsøkonomiske tap i form av tapt arbeidstid og lignende). Datavirus, hackerangrep og lignende tredjepartsaktivitet skaper også utfordringer, men har så langt ikke gitt vedvarende problemer (utover de samfunnsøkonomiske kostnadene som påløper ved beskyttelsestiltak).

Vurderinger og anbefalinger knyttet til nasjonal autonomi for elektroniske kommunikasjons- og nettjenester

Tilgjengelig kommunikasjon er en forutsetning for normal drift av samfunnet og en forutsetning for krisehåndtering.[4] Elektroniske kommunikasjonsnett og -tjenester inngår i det som omtales som kritisk infrastruktur. I denne sammenheng er utfordringen i hvilken grad norske myndigheter skal ha nasjonal kontroll for å sikre dette. Er det markedsutviklingen eller myndighetenes beredskapshensyn som skal være premissgiver for sikker elektronisk kommunikasjon under nasjonale kriser?

Nasjonal autonomi for elektroniske kommunikasjons- og nettjenester betyr at transport- og tjenestenett er lokalisert nasjonalt, at trafikk og signalering skjer innen landets grenser og at produksjon av ulike elektroniske kommunikasjonstjenester skjer nasjonalt. Det innebærer også at drift og styrefunksjoner skjer innen landets grenser. Nasjonal autonomi omhandler også nasjonal tilgjenglighet til reservedeler og kompetanse til å håndtere feil.

Ekomforskriftens § 8-3 sier dette om nasjonal autonomi:

> Tilbyder etter § 8-1 første ledd skal i krise- og beredskapssituasjon kunne opprettholde nødvendig tjenestetilbud for brukere med samfunnskritisk funksjon uten driftsstøtte og elektroniske kommunikasjonstjenester lokalisert i andre land.
>
> Post- og teletilsynet kan i krise- og beredskapssituasjon pålegge tilbyder å utføre drift og vedlikehold av tjenestetilbudet med personell og tekniske løsninger som er lokalisert på norsk territorium.
>
> I kraft når departementet bestemmer.

Bestemmelsen om utsatt ikraftsetting var blant annet resultat av høringsrunden høsten 2003, hvor flere operatører var kritiske. Resten av kapittel 8 trådte i kraft 16.2.2004.[5]

Utvalget har hentet inn argumenter for og i mot nasjonal autonomi. Disse kan summeres opp slik:

[3] I § 2-11 stilles det krav til tilbydere om at de skal utarbeide planer for å sikre leveransene til egne kunder i minimum to uker i tilfelle konkurs, åpning av gjeldsforhandlinger eller betalingsinnstilling.

[4] Dette gjelder fastnett, mobilnett, nødnett, Internett (og IP-telefoni), Forsvarets digitale nett og kraftsektorens nett.

[5] Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften). http://www.lovdata.no/for/sf/sd/sd-20040216-0401.html

Tabell 10.1 Tabell med argumenter for og i mot nasjonal autonomi for elektroniske kommunikasjonsnett og -tjenester.

For	Mot
– Kommunikasjonstjenester i Norge opprettholdes dersom alle forbindelser i utlandet blir kuttet. – Beredskapsarbeidet kan i større grad håndteres nasjonalt. – Det er større nærhet mellom kritisk infrastruktur og de som håndterer nasjonale kriser, noe som kan gi raskere reetablering av tjenester og en mer effektiv nasjonal krisehåndtering. – Autonomi fører til en enklere og mer oversiktelig situasjon med færre aktører som er tilgjengelig nasjonalt ved kriser. – Norske myndigheter trenger kun å forholde seg til det nasjonale lovverket. – Det kan være vanskelig å involvere utenlandsk personell i kriseøvelser (pga. forskjellig språk og kultur, manglende sikkerhetsklarering, fysisk plassering osv.). – Norske myndigheter har ikke mulighet til å pålegge beredskapstiltak for infrastruktur utenfor landets grenser. – Norske myndigheter får ikke anledning til å pålegge prioriteringer ut fra norske interesser for infrastruktur utenfor landets grenser. – En operatør vil ha egeninteresse i å beskytte sine egne systemer slik at de har en konkurransedyktig oppetid. Samfunnet vil ofte ha strengere krav enn dette for å beskytte seg mot ekstraordinære hendelser. – Land som fysisk innehar infrastruktur som er kritisk for Norge kan ha et for lavt beredskaps- og sikkerhetsregime sett med norske øyne. – Per i dag er det nesten full autonomi. Det vil være vanskeligere (umulig?) å pålegge operatørene krav til autonomi på et senere tidspunkt. – Kompetanse knyttet til drift og reetablering vil i større grad befinne seg utenfor landets grenser. – Det er større sannsynlighet for at ulike trusler og påkjenninger (eks. terror, politisk uro, krig, naturkatastrofer) skjer i utlandet enn i Norge. Norge er politisk stabilt og er lite utsatt for større naturkatastrofer.	– Trusselen som krig og nasjonal isolasjon som autonomikravet i utgangspunktet var ment å ta høyde for, samsvarer ikke med dagens trusselbilde. – Tilbydermangfold og stadig flere transmisjonsforbindelser til utlandet reduserer muligheten for at det kommer scenarioer hvor det oppstår total isolasjon fra utlandet. – Bredbåndstelefoni har en stigende markedsandel i Norge med mange internasjonale operatører. Tjenesten er hos mange operatører helt avhengig av det globale Internett. – Effektivisering fordrer at aktørene forholder seg til et internasjonalt marked og kjøper tjenester der de er best og billigst (for eksempel ruting gjennom andres nett i utlandet, sentralisering av driftsfunksjoner osv.). – Krav om autonomi kan gjøre det mindre interessant for utenlandske investorer å investere i norske teleselskaper. – Autonomi kan hindre fri konkurranse ved at små teleaktører blir pålagt så store økonomiske byrder at de ikke overlever. – Hvis kun noen få, store operatører blir pålagt krav om autonomi, må alle samfunnskritiske brukere pålegges å benytte disse. Det vil virke konkurransevridene. På sikt kan det gi monopollignende situasjoner og høyere priser. Det kan også tenkes at de få, store aktørene som blir pålagt autonomi vil få mindre handlingsrom internasjonalt, og at de blir mindre interessant for utenlandske investorer. – Kan gjøre det umulig å være avhengig av driftsstøtte eller kommunikasjonstjenester i utlandet, selv i en normal driftssituasjon. – Begrenser muligheten for norske selskaper å konkurrere i utlandet. – Vil medføre mindre effektiv drift. – Økte kostnader: Ved innføring av full autonomi er kostnadene per i dag beregnet av FFI til noen hundre mill. kroner (gjelder kun Tele2 og Bane Tele). Investeringskostnadene ved innføring av autonomi er per i dag overkommelige, men fremtidens mulige kostnader kan være av en helt annen karakter.

Tabell 10.1 Tabell med argumenter for og i mot nasjonal autonomi for elektroniske kommunikasjonsnett og -tjenester.

For	Mot
– Norske myndigheter kan ikke leve med en situasjon der infrastruktur som er kritisk for Norge kan skrus av fra en driftssentral lokalisert i utlandet. – Det vil bli vanskeligere å innføre andre sikkerhets- og beredskapstiltak uten krav til autonomi. For eksempel vil krav om lokalisering av driftsentraler i fjell være vanskelig å gjennomføre hvis operatøren i neste omgang kan flytte sentralen utenlands. – Kravet om nasjonal autonomi er langt på vei en forutsetning for et nasjonalt beredskapsregime slik det er skissert i St.meld. nr. 47 (2000-2001). – Myndighetene blir i større grad tvunget til å rette fokus mot å håndtere skaden etter at den har skjedd, enn på forebyggende tiltak. – Studier om samfunnets sårbarhet ved FFI har påpekt det faktum at en utvikling der markedshensyn alene får råde vil øke sårbarheten i samfunnskritisk infrastruktur, inkludert infrastruktur for elektronisk kommunikasjon. FFI hevder derfor at det er viktig å ta beredskapshensyn utover det markedsutviklingen medfører.	– Flere av aktørene opererer i dag internasjonalt (Tele 2 driver virksomheter i 24 land, Telenor er inne på eiersiden i en rekke internasjonale selskaper, Netcom er en del av Telia Sonera) – Logiske angrep mot infrastruktur som er kritisk kan skje uavhengig av om den er plassert i Norge eller utenlands. – I noen tilfeller vil tilgang til ressurser utenfor landets grenser redusere den nasjonale sårbarhet.

Forsvarets forskningsinstitutt fikk i 2005 et oppdrag fra Post- og teletilsynet om å utrede behovet for nasjonal autonomi.[6] Utredningen angir fire alternative måter å forholde seg til et eventuelt krav om autonomi på:

1. Ingen autonomi: § 8-3 i ekomforskriften strykes, og det vurderes alternative sikkerhetstiltak i stedet.
2. Regional begrensing: Ingen nasjonal autonomi, men operatørene i det norske telemarkedet får regionale begrensninger på hvilke områder de kan etablere infrastruktur som er viktig for levering av teletjenester i Norge.
3. Nasjonal backup: Opprettholdelse av nasjonale backupløsninger på driftssiden for noen operatører.
4. Full autonomi: Alle nett og tjenester må kunne driftes og opprettholdes fra Norge i sanntid.

FFI anbefaler alternativ 3 ut fra begrunnelsen om å kombinere markeds- og beredskapshensyn med en viss pragmatisme.

På bakgrunn av organisatoriske og teknologiske endringer i elektroniske kommunikasjons- og nett-tjenester anbefaler Post- og teletilsynet at ekomforskriftens § 8-3 ikke bør iverksettes, men at ansvarlige myndigheter i stedet inngår avtaler med sentrale aktører om opprettholdelse av en viss beredskap i Norge.[7] Dette samsvarer i hovedsak med FFIs alternativ 1. For budsjettåret 2006 er Post- og teletilsynet tildelt om lag 21 mill. kr over statsbudsjettet til dette. Avtaler som inngås vil inneholde krav til sikringstiltak som for eksempel lokalisering, sikring av og tilgang til fysisk infrastruktur, sikkerhetsklarering av personell[8] og krav til hvilke tjenester som skal prioriteres i krise- og beredskapssituasjoner. Hjemmel for å inngå avtaler ligger allerede i eksisterende regelverk.

[6] Fridheim, Håvard et.al. 2005. *Nasjonal autonomi for elektroniske kommunikasjonsnett og -tjenester*. Forsvarets forskningsinstitutt. FFI/Rapport-2005/00175 (BEGRENSET)

[7] PT-notat til utvalget 5.9.2005, ref. 2005009009-3. *Nasjonal autonomi i elektroniske kommunikasjonsnett*

[8] Dette vil forutsette at sikkerhetsloven er gjort gjeldende for avtaleparten

Ideelt sett burde teletjenester i Norge kunne drives upåvirket av forhold utenfor landet. Utvalget innser imidlertid at både den teknologiske utviklingen og det faktum at bransjen er preget av sterk internasjonal konkurranse vil kunne gjøre det vanskelig å stille krav om autonom drift. På den annen side er drift av de elektroniske kommunikasjonstjenestene så viktige for samfunnet at det må finnes løsninger som ivaretar en nødvendig grad av sikkerhet og beredskap.

Det er åpenbart at dersom utviklingen i telemarkedet fortsetter uten at nasjonale reserveløsninger etableres, vil avhengigheten av utlandet øke. Det vil bli både ressurskrevende og vanskelig å etablere de beredskapsløsninger som er beskrevet ovenfor, dersom dette utsettes ytterligere.

Dersom bestemmelsen i forskriften om krav til autonomi ikke skal gjøres gjeldende, må det finnes løsninger og gjøres avtaler som er slik at kommunikasjonssystemene likevel gjøres så lite sårbare som mulig overfor forhold utenfor landets grenser. Dette vil stille store krav til telemyndigheten når de skal inngå avtaler med operatører om beredskap og tekniske løsninger som sikrer drift i nødvendig utstrekning i krisesituasjoner. Det er viktig at telemyndigheten tilføres nødvendig kompetanse og kapasitet til å spesifisere og evaluere krav og løsninger overfor teleoperatørene.

Beredskapsmessige og tekniske løsninger vil med stor sannsynlighet medføre etablering av reserveløsninger på noen områder. De ekstra kostnadene ved dette vil måtte dekkes av staten. I dag kjøper staten tjenester av beredskapsmessige karakter fra Telenor i noen utstrekning. For å sikre tilgjengelighet til teletjenester i størst mulig grad uavhengig av hendelser utenfor Norge vil rammene for kjøp av slike tjenester nok måtte økes betraktelig.

Utvalget mener at dersom avtaler om nasjonale reserveløsninger er etablert, kan kravet om autonom drift av telesystemer slik det er utformet i forskriften i dag frafalles. Nødvendige lovhjemler som sikrer slike reserveløsninger må være på plass.

Vurderinger og anbefalinger knyttet til regulering av brukere av Internett

Som tidligere vist er et fungerende Internett en forutsetning for en lang rekke kritiske samfunnsfunksjoner. Internett har innslag av egne infrastrukturelementer, samtidig som store deler av Internett er basert på teleinfrastrukturen. Internettaksess som tjeneste har likhetstrekk med telefonitjenesten, og helheten kan derfor omtales som en kritisk infrastruktur. Virkemidler for å sikre infrastrukturen må vurderes med dette for øye.

Internetts egenart og struktur skiller den fra andre kritiske infrastrukturer, blant annet ved at et stort antall privatpersoner og virksomheter har logisk tilgang gjennom bredbåndstilknytning. Dette gir seg utslag i at også virkemidler og tiltak for sikker drift skiller seg fra andre kritiske infrastrukturer. Selv om utvalgets anbefalinger om virkemidler og tiltak primært er ment å omfatte private og offentlige virksomheter, er forskjellene av en slik karakter at utvalget mener at også privatpersoner burde omfattes av reguleringer som bidrar til et sikrere Internett. Privatpersoner og mange bedrifter med bredbåndstilknytning utgjør en potensiell trussel mot viktige samfunnsinteresser blant annet ved at de uforvarende kan bli utnyttet av personer med ondsinnede hensikter. Forebyggende tiltak overfor *alle* brukere fremstår derfor som viktig for at Internett også fremover kan utgjøre en trygg kanal for elektroniske tjenester.

Utvalget anbefaler følgende:

1. At alle Internettilbydere blir pålagt å levere sikkerhetsprogramvare som en del av Internettabonnementet til privatpersoner.
2. At alle utstyrsleverandører av trådløse nett plikter å levere utstyret med tilfredsstillende sikkerhetsinnstillinger og gode veiledninger på norsk.
3. At det i regi av Samferdselsdepartementet utredes nærmere om:
   a) alle, både privatpersoner og virksomheter, skal være pliktige til å benytte oppdatert sikkerhetsprogramvare når de kobler seg til Internett.
   b) Internettilbydere skal bli pålagt å kontrollere at alle deres kunder benytter seg av oppdatert sikkerhetsprogramvare, og hvilke inspeksjons- og sanksjonsmuligheter som er teknisk og økonomisk realistiske.
   c) det kan utarbeides IKT-sikkerhetsstandarder som alle virksomheter som knytter seg til Internett blir pålagt å følge.

Forslagene understreker egenansvaret til den enkelte bruker.

Utvalget er inneforstått med at trusler i stor grad vil kunne komme fra utlandet. Således kan det hevdes at rene nasjonale tiltak vil kunne få begrenset effekt. Utvalget mener likevel at dette ikke er til hinder for at Norge kan fremstå som et foregangsland og bidra til at Internett er en trygg kanal for elektroniske tjenester.

Vurderinger og anbefalinger knyttet til organiseringen av IT-sikkerhetsarbeidet

Utvalget viser til Dokument nr. 3:4 (2005–2006) Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur. Riksrevisjonen mener blant annet at det er viktig å avklare ansvarsforhold knyttet til IT-sikkerhetsarbeidet, herunder å avklare ansvarsforhold på departementalt nivå.

Utvalget er kjent med at det er nedsatt en arbeidsgruppe under ledelse av Fornyings- og administrasjonsdepartementet for å følge opp Riksrevisjonens vurderinger knyttet til organiseringen av arbeidet med IT-sikkerhet. Etter det utvalget kjenner til skal dette arbeidet være ferdig våren 2006.

Utvalget mener det er nødvendig med organisatoriske endringer på departementalt nivå for at ansvarsforhold knyttet til IT-sikkerhet skal bli tydeligere. Dagens organisering og ansvarsdeling synes å medføre både mangler og overlapping i de ansvarlige fagdepartementenes myndighetsutøvelse. I Nasjonal strategi for informasjonssikkerhet fremgår det at koordineringsansvaret for IT-sikkerhet er delt mellom Justis- og politidepartementet, Forsvarsdepartementet, Moderniseringsdepartementet og Samferdselsdepartementet. Ansvaret er delt mellom disse departementene ut fra fagansvar i medhold av lov- og forskriftsverk samt kongelige resolusjoner.

Det er påvist uklarheter i ansvarsforholdene mellom Fornyings- og administrasjonsdepartementet, Samferdselsdepartementet og Justis- og politidepartementet. Det er uomtvistet at Fornyings- og administrasjonsdepartementet er gitt koordineringsansvaret for regjeringens IT-politikk. Samtidig utformes en stor del av IT-politikken av Samferdselsdepartementet, i og med at departementet er gitt det faglige ansvaret for forvaltningen av «overføring av elektronisk kommunikasjon med tilhørende infrastruktur, tjenester, utstyr og installasjoner», jf. ekomlovens § 1-2. I tillegg er det ikke tydelig nok hva Justis- og politidepartementets koordinerende rolle innen samfunnssikkerhet og beredskap omfatter.

Utvalget anbefaler at antall fagdepartementer med overordnet ansvar for IT-sikkerhet bør reduseres, og ideelt sett mener utvalget at dette ansvaret bør ligge til ett departement. Utvalget vil foreslå en samordning av Samferdselsdepartementets og Fornyings- og administrasjonsdepartementets ansvar på dette fagområdet. Det vises for øvrig til forslaget i kapittel 5.4.1 om å tydeliggjøre Justis- og politidepartementets ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner.

10.1.4.3 Økonomiske virkemidler

Tilskudd eller kjøp av tjenester benyttes i noen grad for å ivareta sikkerhets- og beredskapshensyn. Spesielle samfunnspålagte oppgaver (herunder beredskap og sikkerhet) ble de første årene etter selskapsdannelsen utført av Telenor etter pålegg fra Samferdselsdepartementet. Fra og med 1998 er disse oppgavene blitt finansiert ved at staten kjøper tjenestene av Telenor. Det vil si at staten gjør avtaler med Telenor om å levere spesifiserte tjenester, mot dekning av merkostnader[9]. Forvaltningen av dette tilskuddet er nå overført til Post- og teletilsynet. Til kjøp av slike tjenester ble det for 2005 bevilget 14 millioner kroner.

Telenor er forpliktet til fortsatt å videreføre nød- og sikkerhetstjenesten via kystradionettverket for å ivareta nødkommunikasjon i redningstjenesten. Justis- og politidepartementet dekker kostnadene knyttet for denne tjenesten.

Bruk av anbudskonkurranser for å ivareta sikkerhets- og beredskapsoppgaver ble vurdert i St.meld. nr. 47 (2000-2001). Samferdselsdepartementet skrev blant annet følgende:

> Prinsipielt er det intet til hinder for at andre aktører (enn Telenor) kan konkurrere om å levere de tjenestene som omfattes av USO-forpliktelsen[10], eller utføre spesielle samfunnspålagte oppgaver. I et etablert og velfungerende marked kan det være hensiktsmessig og effektivitetsfremmende å la flere aktører konkurrere om samfunnsoppgavene. En forutsetning for å innføre konkurranse om disse oppgavene vil imidlertid være at flere aktører har opparbeidet betryggende evne til å ivareta oppgavene på en tilfredsstillende og kontinuerlig måte i hele eller deler av landet.

Vurderinger og anbefalinger

Utvalget mener kjøp av tjenester og tilskudd til spesielle oppgaver for sikring av kritisk infrastruktur vil være et nødvendig virkemiddel sammen med regulatoriske bestemmelser. Det vises i denne sammenheng også til utvalgets forslag om en tilskuddsordning, jf. kapittel 6.6.3.

10.1.5 Nødnettet

Nødetatene brann, politi og helse har i dag separate sambandssystemer, mens de i fremtiden vil bli brukere av et felles, mobilt nødnett. Det forutsettes at nødnettet også tas i bruk av andre bruker-

[9] Jf. St.prp. nr. 1 Tillegg nr. 1 (1997-98) Om endringer av proposisjonen om statsbudsjettet for 1998 som følge av opphevelse av eksisterende eneretter i telesektoren

[10] USO: Universal Service Obligation

grupper, eksempelvis forsvaret, tollvesenet, fengselsvesenet, sivilforsvaret og frivillige organisasjoner.[11] Offentlige myndigheter og beredskapsenheter vil også være aktuelle brukere. Med utbyggingen av det nye nødnettet tar staten ansvar for infrastruktur av stor samfunnsmessig betydning. Stortinget har uttalt at nødnettet vil fremstå som en av grunnpilarene i landets fremtidige totalforsvar. Landsomfattende dekning for nødnettet er planlagt ferdigstilt innen utgangen av 2009.

Nødnettet - kritisk for samfunnet

Effektiv og livreddende innsats i alle situasjoner krever et forutsigbart og moderne kommunikasjonssystem med hensiktsmessig funksjonalitet, dekning og tilstrekkelig kapasitet. Situasjoner som oppfattes som kriser for de involverte, eksempelvis branner, tyverier og ulykker, er nødetatenes hverdag. Befolkningen forventer at det i slike situasjoner skal være enkelt å komme i kontakt med nødetatene. Det må være rask, avlyttingssikker og pålitelig kommunikasjon mellom alle involverte i krisehåndteringen.

Dårlig kvalitet eller brudd i nødsambandet kan føre til farlige misforståelser med store konsekvenser for liv og helse. Eksempelvis vil god kommunikasjon mellom nødmeldesentral og ambulanse være livsviktig når nødnummer 113 blir oppringt med melding om hjertestans. Radiokommunikasjon er en helt nødvendig innsatsfaktor i møte med tyngre, organisert kriminalitet og mulige terroranslag. Samtidig er avlyttingssikkert samband helt nødvendig i kriminalforebyggende arbeid. Politiet vurderer sambandet som sitt viktigste verneutstyr.

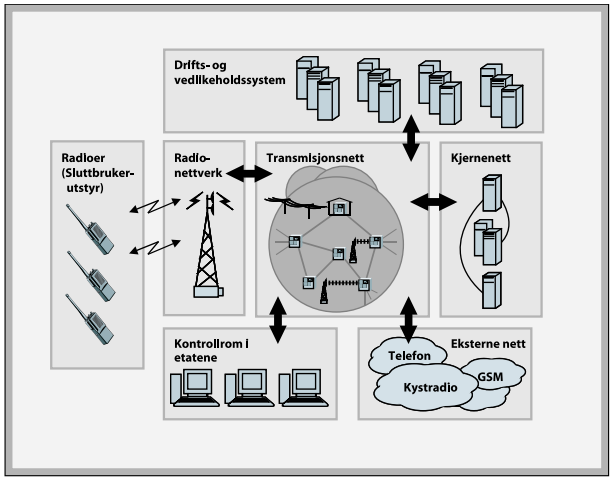
I en krise der offentlig infrastruktur er rammet, er det vesentlig at innsatsstyrkene kan stole på et robust og avlyttingssikkert radiosamband som er uavhengig av offentlige telefoni- og datatjenester.

Beskrivelse av nødnettet

Nødnettet består på et overordnet nivå av tre hoveddeler:

- Et kjernenett som utgjør «intelligensen» i nettverket.
- Et radionettverk med svært høy dekningsgrad for radioterminaler innendørs og utendørs.
- Et transmisjonsnett som transporterer data fra kjernenettet ut til radionettverket og til andre punkter som er tilkoblet nødnettet. Dette nettet vil hovedsakelig utgjøres av det transportnettet som er felles for offentlige telefontjenester og andre tilgjengelige nett.

[11] Jf. St.prp. nr. 1 Tillegg nr. 3 (2004-2005). jf. Budsjett-Innst. S. nr. 4 (2004-2005).



Figur 10.2 Illustrasjon av oppbyggingen av det fremtidige nødnettet.

Kilde: Nødnett

For å sikre høy tilgjengelighet i nødnettet vil det implementeres omfattende sikkerhets- og reserveløsninger på flere nivåer.

Nødetatene vil ha tilgang til nødnettet fra sine «kontrollrom» (politiets operasjonssentraler, branns nødalarmeringssentraler og helses akuttmedisisnke kommunikasjonssentraler, akuttmottak og legevaktsentraler) og fra håndholdte og kjøretøymonterte radioterminaler.

Mulighetene for samhandling mellom politiet, brannvesenet og helsevesenet vil med et utbygd nødnett være til stede i en helt annen form enn i dag. Ved behov kan de tre nødetatene samsnakke i grupper og hver for seg – alt i det samme felles nettet. Gruppene kan med letthet endres og defineres i forhold til det behovet som følger av den enkelte hendelse. I tillegg er det mulig å operere ut i fra det lukkede nødnettet til fast- og mobilnettet, til GSM Rail (jernbanens nye sikkerhetsnett), Kystradioen (til skip) og til andre nett.

Det må være et klart fokus å samle aktuelle beredskapsaktører innenfor det nye nettet. Nødnettet må ha prioritet på kommunikasjonstjenester med høy kvalitet til lavest mulig kostnader for brukerne. Det er viktig å få med så mange brukere med felles kommunikasjonsbehov som mulig.

Utbygging av et nytt nødnett er en meget stor teknisk oppgave og et enormt økonomisk løft for samfunnet. Det vil gå flere år før nettet er ferdig utbygd over hele landet. I statsbudsjettet for 2006 ble det bevilget omlag 400 millioner kroner til utbygging av nettet. Dette er tilstrekkelig for planlagt utbygging i 2006. Den totale utbyggingen er anslått til å koste 3,6 milliarder kroner.

Utvalget er sterkt opptatt av at utbyggingen av nødnettet må fullføres slik det er planlagt. Det vil fylle en svært viktig og kritisk samfunnsfunksjon, og nettverket av basestasjoner vil i seg selv utgjøre en viktig infrastruktur. Det er derfor avgjørende at de bevilgninger som er nødvendig for å fullføre utbyggingen blir gjort i årene fremover.

10.2 Satellittbasert kritisk infrastruktur[12]

Data fra satellitter i bane rundt jorden er i økende grad tatt i bruk innen mange viktige samfunnssektorer. Mange tjenester i et moderne samfunn baserer seg på bruk av rombaserte informasjonskilder. Navigasjon, meteorologi, overvåking og nødvarsling er eksempler på informasjon som ikke bare spiller en viktig rolle, men i noen sammenhenger en avgjørende rolle for samfunnskritiske tjenester. En utfordring i forbindelse med rombasert informasjon er systemenes internasjonale og globale karakter. Sikkerhetsmessige virkemidler på nasjonalt plan er begrenset, men må ses i et internasjonalt samarbeid.

Navigasjonssystemenes leveranser av tids- og posisjoneringsdata underbygger de gjensidige avhengighetsforhold som preger moderne infrastruktur. Med andre ord vil fravær, eller manipulering av navigasjonsdata, påvirke funksjonaliteten i andre infrastrukturer. Akkumulert vil funksjonssvikt i navigasjonssystemene kunne ha betydning både for samfunnssikkerheten og den nasjonale sikkerheten. Siden mange kritiske samfunnsfunksjoner har gjort seg avhengige av GPS, utgjør dette en sårbarhet. Sårbarheten vil imidlertid fra omkring 2010 reduseres ettersom det europeiske navigasjonssystemet Galileo, se kapittel 10.2.1, da vil være operativt.

Medlemslandene i EU har erkjent at Galileo innebærer store sikkerhetsmessige utfordringer på ulike plan. Av den grunn legger medlemslandene ned betydelige ressurser for at Galileo skal bli et sikkert og pålitelig system. Innsatsen som legges ned på sikkerhetssiden viser med tydelighet at EU-landene anser Galileo som en særlig vital del av den samlede kritiske infrastrukturen i Europa.

Utvalget er enig med de som hevder at dette området vil bli stadig viktigere for mange funksjoner i samfunnet. Anvendelser av teknologier som er avhengig av satellitter er etter hvert blitt ganske omfattende, selv om det nok kan sies at de er i et gryende stadium.

Nettopp derfor er det grunn til å se nærmere på satellittbasert infrastruktur (også kalt rombasert infrastruktur). Det er flere spesielle forhold knyttet til dette området både når det gjelder lokalisering, eierskap og sikringstiltak.

10.2.1 Overordnet beskrivelse av infrastruktur og samfunnsfunksjon

Navigasjonssystemer

Frem til i dag er det særlig det amerikanske satellittbaserte *Global Positioning System (GPS)* som har vært tilgjengelig for sivilt bruk.

Gjennom 24 operative (og 6 operative reserve) satellitter og ulike bakkeinstallasjoner betjener GPS en rekke samfunnsfunksjoner med navigasjonsinformasjon. Navigasjonssystemene er først og fremst en understøttende infrastruktur til en rekke andre infrastrukturer og aktiviteter i samfunnet. Understøttelsen skjer i form av tids- og posisjoneringsinformasjon. Eksempler på bruksområder for navigasjonssystemene er innen alle deler av transportsektoren, kraftforsyning, offshoresektoren, landbrukssektoren, telekommunikasjon, finanssektoren, fiskerisektoren, miljøsektoren, nødetatene og militærvesen.

Særskilt om Galileo

Galileo er et europeisk initiativ for å opprette et sivilt globalt system for satellittnavigasjon. Systemet kommer i tillegg til GPS og planlegges å være i operativ drift fra tidligst 2010. Galileo er et egenkontrollert navigasjonssystem som vil gjøre Europa mer uavhengig av USA. GPS og Galileo vil være interoperable, dvs. at fra et brukerperspektiv kan begge systemene benyttes. Galileo vil bestå av rundt 30 satellitter og vil bli et EU-kontrollert og drevet system. To kontrollsentre skal opprettes i Europa. Andre deler av bakkesegmentet vil plasseres rundt om på kloden. Svalbard fremstår som et alternativ for utplassering av en del av Galileo bakkesegment. En slik stasjon vil bli samlokalisert med Svalbard Satellittstasjon som eies og drives av Kongsberg Satellite Services (KSAT). KSAT eies 50 % av Norsk Romsenter via Norsk Romsenter Eiendom og 50 % av Kongsberg Gruppen via Kongsberg Defence and Aerospace

Galileos betydning for samfunnssikkerheten illustreres gjennom systemets ulike brukernivåer. Tjenester vil bli levert på flere nivåer med hensyn

[12] Temaet er nærmere berørt i Synstnes, Hans M. 2005. *Navigasjonssystemer og samfunnssikkerheten. Arbeidsnotat til Infrastrukturutvalget*. Nasjonal sikkerhetsmyndighet – i del 2, vedlegg 11.

til signalenes konfidensialitet, integritet og tilgjengelighet. For det øverste nivået, *Public Regulated Service (PRS)*, vil tilgangen være strengt myndighetskontrollert, og begrenset til applikasjoner ment for mellom annet politiet, øvrige nødetater, drift av annen særlig kritisk infrastruktur. Nasjonene innen EU står fritt til å inngå i PRS delen av Galileo. De som ønsker å delta må imidlertid delta med å finansiere og utvikle PRS. Det antas at Norge kan få delta i PRS dersom det er ønskelig. De nasjoner som velger å involvere seg i PRS vil være i en teknologisk frontposisjon, og vil kunne utnytte dette til fordel for den nasjonale samfunnssikkerheten, samt til utvikling av relaterte tjenester.

En sikkerhetsmessig målsetning med Galileo er å fjerne eller redusere sårbarheter vi i dag kjenner fra GPS og skape økt redundans og dermed redusert samfunnsårbarhet.

I motsetning til slik det er for GPS åpnes det i Galileo-prosjektet for at Norge kan delta i både utforming og driften av systemet, selv om vi ikke er en del av EU.

Kunnskap gjennom forskning og utvikling samt oppbygging av nasjonal industri og kompetanse vil være viktige virkemidler for å forstå hvordan man best kan motstå trusler mot systemet og iverksette mottiltak. Galileo PRS-signalene vil være robuste mot forstyrrelser. Kryptering av navigasjonssignalene fra satellittene vil gi en bedre beskyttelse mot villedning.

Satellittfjernmåling

Satellittfjernmåling er datakilde for mange samfunnsviktige oppgaver, eksempelvis meteorologi.

Norge har hatt bakkestasjoner for mottak av slike data helt siden midten av 1960-årene. I dag eier og opererer Kongsberg Satellite Services (KSAT) bakkestasjoner i Tromsø og i Longyearbyen, Svalbard og i Grimstad. I tillegg er bakkestasjonen Trollsat under etablering i Antarktis. Ved KSATs stasjoner leses det ned data for nær sann tids anvendelse innen blant annet meteorlogi, miljøovervåking og skipsdeteksjon. I tillegg mottas optiske satellittbilder fra en rekke satellitter. Meteorologisk institutt (MI) har sin egen nedlesestasjon for meteorologiske data fra satellitter i både polare og geostasjonære baner på Blindern i Oslo.

Samfunnskritiske tjenester

På Svalbard opererer KSAT hovedstasjonen for mottak av data fra og kontroll av polarbanesatellittene til viktige meteorologiske organisasjoner som europeiske EUMETSAT og amerikanske NOAA. Svalbard-stasjonen er kritisk viktig siden dette er den eneste kontrollstasjonen organisasjonene har for sine polarbanesatellitter. Gode og pålitelige værprognoser er avhengig av hyppig oppdatering av satellittobservasjoner og minimal forsinkelse i overføring av data til prosesseringssentrene. Data fra stasjonen i Longyearbyen distribueres via en fiberoptisk kabel som er lagt mellom Svalbard og fastlandet. Kabelen er en viktig forutsetning for å overholde krav til hurtig, kostnadseffektiv og pålitelig dataoverføring. Før fiberkabelen ble lagt ble satellittkommunikasjon benyttet. Dette er like raskt, men langt dyrere, noe som hindret utviklingen av viktige tjenester fra stasjonen. Pålitelige værvarsler er en kritisk tjeneste for næringsvirksomhet generelt og i spesielle situasjoner som for eksempel ekstremvær og for å kunne styre innsats i katastrofer, ras, flom osv., som følge av slikt vær. Svalbard-stasjonens beliggenhet på høy breddegrad sammen med pålitelig og rask dataoverføring gjør den til en nøkkelstasjon for både nasjonal og internasjonal meteorologitjeneste.

Satellittdata er en viktig informasjonskilde for å oppdage og overvåke miljøkatastrofer som for eksempel oljesøl på havet og brukes både nasjonalt og internasjonalt. Skipsdeteksjon via satellitt inngår i nasjonal suverenitetshevdelse over vårt territorialfarvann og fiskevernsonen rundt Svalbard. Data fra KSATs stasjon i Tromsø benyttes av Forsvaret for dette formålet.

Nødvarsling via satellitter

Norge deltar i et internasjonalt samarbeid for å kunne oppdage og posisjonsbestemme aktiverte nødpeilesendere via satellitt, det såkalte COSPAS/SARSAT programmet. Systemet består av en konstellasjon med flere satellitter som gir en global dekning med rask varsling og posisjonsbestemmelse av nødpeilesendere. En viktig fordel med systemet er at det overvåker nødfrekvensene også over områder som har liten eller ingen dekning for øvrig. For Norge, med redningsansvar for blant annet store havområder i nord, er systemet av stor betydning for sikkerheten til næringsvirksomhet og annen aktivitet i disse områdene.

COSPAS/SARSAT benytter i dag satellitter i både polare og geostasjonære baner. Der verdt å merke seg at det i fremtiden planlegges å utstyre Galileo- og GPS-satellitter med instrumenter for COSPAS/SARSAT systemet.

10.2.2 Utvalgets vurderinger knyttet til virkemidlene

Det er særegent for den satellittbaserte infrastrukturen at den i all hovedsak er lokalisert utenfor Norge. Dette gjelder selvfølgelig satellittene, men også kontrollsentra og andre bakkesegmenter. Viktige bakkestasjoner er imidlertid og vil også i fremtiden kunne bli lokalisert på norsk jord.

Norge har også liten eller ingen innflytelse på eierskapsspørsmålet. GPS er et rendyrket amerikansk system, og Galileo vil bli et EU-kontrollert og drevet system. Selve utbyggingen, driften og fornyelsen av det operative Galileosystemet vil bli gjennomført av en privat aktør.

I motsetning til GPS åpnes det i Galileoprosjektet for at Norge kan delta både i utforming og drift av systemet. Følgelig foreligger det både politiske og faglige muligheter for Norge, selv om vi ikke er en del av EU. Nedenfor skisseres noen utfordringer og mulige virkemidler for å ivareta nasjonale interesser i forhold til navigasjonssystemet Galileo.

Innsikt i utvikling og drift av Galileosystemet oppnås best gjennom aktiv og målrettet deltakelse i nedsatte komiteer og arbeidsgrupper samt faste staber innen EU og *European Space Agency (ESA)*. Med innsikt menes her eksempelvis førstehåndskunnskap om styrker og svakheter ved systemet, innsikt i krisehåndteringsprosesser, bedre forutsetning for norsk deltakelse i felles reaksjonsmønster mot uønskede hendelser. Deltakelse gir dessuten mulighet til å påvirke løsninger.

Norge bør vurdere å slutte seg til PRS-delen av Galileo-systemet, siden sivile offentlige brukere ikke vil få tilgang til tilsvarende informasjon fra GPS i fremtiden, og fordi Galileo PRS vil ha mer robuste signaler. Deltakelse i Galileo PRS krever statlige kontrollmekanismer.

Dersom Norge skulle få tildelt Galileo bakkeinfrastruktur (på Svalbard) vil det være viktig å fastsette hvilke lokale sikringstiltak som er nødvendig for å beskytte nettopp bakkeinfrastrukturen.

10.3 Kraft

Stabil tilgang til elektrisk kraft er et grunnvilkår for moderne, komplekse samfunn. Et sentralt trekk i utviklingen på dette området er en sterkt økende IKT-avhengighet etter hvert som en går over fra å betjene anlegg til å overvåke produksjons- og distribusjonssystemene fra et fåtall driftssentraler.

For et velutviklet land som Norge vil det være åpenbart at en stabil og effektiv kraftforsyning er en forutsetning for at samfunnsmaskineriet ikke skal bryte sammen.

Velstandsutviklingen i Norge er i stor grad bygget på den spesielle mulighet landet har hatt for produksjon av elektrisk kraft med fornybar energikilde. Kraftkrevende industri var kanskje i starten den mest sårbare delen for vårt land i forhold til mulig bortfall av elektrisk kraft. I tiden like etter andre verdenskrig kunne store deler av samfunnet fortsatt tåle forholdsvis lange utfall av kraftleveranser. Det var mulig å gjennomføre rasjonering av kraft med tidvis utkobling uten at samfunnet av den grunn stoppet opp.

I takt med den teknologiske utviklingen, og spesielt på grunn av den eksplosive utvikling av informasjons- og kommunikasjonsteknologien har samfunnets avhengighet av stabil og sikker levering av elektrisitet blitt stadig større.

I dag er denne avhengigheten total, i den forstand at vi opplever en spontan stans innenfor de fleste sektorer i det øyeblikk elektrisiteten forsvinner. Avhengigheten på tvers av samfunnssektorer har vært kjent lenge, og Forsvarets forskningsinstitutt (FFI) har redegjort for dette blant annet i tidligere BAS-utredninger[13].

Innen kraftsektoren har sentralnettet karakter av kritisk infrastruktur i egenskap av å utgjøre det landsdekkende transportnettet som binder alle kraftprodusentene og sluttbrukerne sammen. Svikt i nettet vil raskt kunne forplante seg og utvikles til å ramme store deler av samfunnet. Det er med andre ord riktig å betegne det samlede nettet som et tett koblet system.

Forstyrrelser i sentralnettet kan skape problemer for hele landet, men forstyrrelser i regionalnettet og distribusjonsnettet kan skape like store problemer for dem som blir rammet, for eksempel en by (regionalnett) eller en bygd (distribusjonsnett). Sammenbrudd i regionalnettet vil kunne sammenliknes med tap av/sammenbrudd i vannforsyningen til en by. Også distribusjonsnettet i de større byene kan utgjøre en meget kritisk del av strømforsyningen.

Hvert enkelt produksjonsanlegg utgjør imidlertid ikke på samme måte en kritisk fasilitet. Et utfall av ett enkelt anlegg (eller noen flere) vil i mange tilfeller kunne kompenseres ved økt produksjon (og eventuell import) fra andre steder inntil normal driftssituasjon kan opprettes. Det er likevel ikke tvil om at produksjonsanleggene samlet sett utgjør en kritisk infrastruktur.

Norge er de siste årene blitt en nettoimportør av kraft, og forbruket av elektrisitet forventes å øke

[13] BAS: Forskningsserie «Beskyttelse av samfunnet»

i tiden fremover. Vi er dermed i mangel av innenlands produksjonskapasitet mer avhengige av utveksling av kraft med utlandet, og denne avhengigheten vil med stor sannsynlighet øke i tiden fremover. Det blir derfor også planlagt med en tettere sammenkopling med resten av Europa i form av bygging av nye overføringskabler.

Med dagens forbruksutvikling er økt utvekslingskapasitet med utlandet ikke tilstrekkelig for å unngå kraftunderskudd, selv om det i noen grad kan bidra til å redusere risiko for store prisøkninger i perioder.

Det er verdt å merke seg at sårbarhetsutvalget pekte på de samme problemstillingene, i tillegg til å påpeke at markedsfokuset hindrer investeringer som ikke raskt kan gi tilfredsstillende avkastning.

Det fremstår derfor som en presserende oppgave for myndighetene å utrede og se til at nødvendige tiltak blir gjort for å forbedre markedsbalansen i kraftmarkedet både på kort og langt sikt. Dette gjelder så vel tiltak med sikte på økning av kapasiteten for kraftutveksling med utlandet, eliminering av flaskehalser i det innenlandske overføringsnettet, som tiltak både på produksjons- og etterspørselssiden i det innenlandske kraftmarkedet.

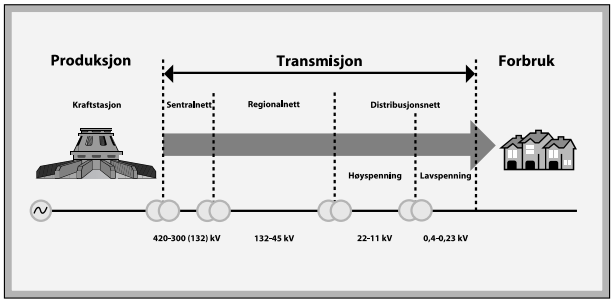
10.3.1 Overordnet beskrivelse av infrastruktur og samfunnsfunksjon

Produksjon av elektrisk kraft i Norge er tilnærmet synonymt med vannkraft. Vannkraftverkene står for nesten 99 % av innenlands energiproduksjon. Midlere produksjonsevne i det norske vannkraftsystemet er 199 TWh. Dette kan variere med ± 30 TWh avhengig av nedbørsforholdene.

Det foreligger i dag flere planer for bygging av gasskraftverk i Norge. Hittil er det gitt konsesjoner til fire prosjekter. Naturkraft AS har fått konsesjon for to gasskraftverk, Industrikraft Midt-Norge AS har fått konsesjon for ett gasskraftverk og Statoil har fått konsesjon til ett integrert gasskraftverk ved Snøhvit LNG[14]. Det er kun det siste anlegget som er utbygget, mens Kårstø er under bygging.

Norsk kraftforsyning er i stor grad basert på vannkraft fra produksjonsanlegg distribuert over hele landet. Et omfattende kraftnett er bygget opp for å overføre og fordele kraften fra produksjonsstedene til forbrukssentrene. Drifts- og styringssystemer for den grunnleggende infrastrukturen er viktige, slik at kraftoverføringen blir mest mulig sikker og effektiv. Videre er handelssystemet for elektrisk kraft avhengig av en tett kobling mot både driftssystemet og mot driftsdata fra kraftinfrastrukturen.

[14] LNG: *liquified natural gas*



Figur 10.3 Prinsippskisse kraftinfrastrukturen.[1]

Kilde: NVE.

[1] Figuren er en gjentegning. I tillegg er det gjort noen mindre endringer i forhold til den originale.

De enkelte elementer som utgjør infrastrukturen for kraftforsyning i Norge

Produksjon, overføring og omsetning er de tre grunnleggende funksjonene i kraftforsyningen.

Figur 10.3 viser en enkel modell over hvilke hovedelementer som inngår i den infrastrukturen som utgjør kraftproduksjon, distribusjon, og omsetning.

Det nederste nivået i modellen viser den fysiske kraftinfrastrukturen som sørger for produksjon, overføring og distribusjon av elektrisk kraft. Dette inkluderer alle fysiske installasjoner, anlegg og komponenter som bringer kraften fra produksjonsstedet til forbrukeren. Eksempler på komponenter på dette nivået er demninger, kraftstasjoner, transformatorer og kraftlinjer.

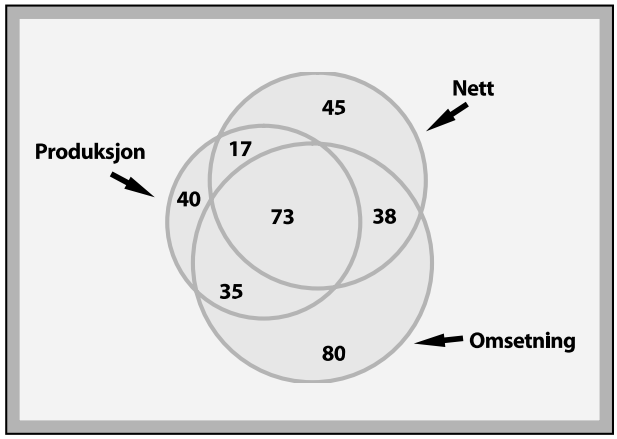
For å styre dette har vi drifts- og støttesystemet, som sørger for sikker og effektiv drift av kraftinfrastrukturen. Handel av kraft er avhengig av en intakt infrastruktur og en tett kopling til drifts- og styringssystemet. Handels- og drifts-/styringssystemet har et felles behov for informasjon og koordinering, siden elektrisitetsproduksjon er et *just-in-time* system. Forbrukere utfordrer systemet ved å bruke lys, varmeovner, motorer og annet elektrisk utstyr. Den øyeblikkelige tilkoplingen av elektrisk utstyr krever en umiddelbar reaksjon fra aggregater og brytere i nettet for å opprettholde frekvensen, spenningsnivået og stabiliteten i leveransene.

Det at produksjonen til enhver tid skal være lik forbruket, krever derfor rask kommunikasjon og informasjonsutveksling mellom en rekke aktører. Som følge av dette er kraftforsyningen en kommunikasjonsintensiv bransje. Moderne informasjons- og kommunikasjonsteknologi er blitt tatt i bruk for drift av de ulike delene av kraftforsyningen. Der det tidligere var ansatte på hvert eneste kraftforsyningsanlegg som styrte den aktuelle installasjonen

manuelt, fjernstyres nå anleggene fra et fåtall driftssentraler. Dette gjøres ved hjelp av kompliserte IT-systemer og et velfungerende samband.

Utveksling av informasjon på og mellom de ulike nivåene i figuren skjer via en grunnleggende elektronisk kommunikasjonsinfrastruktur. Denne er dels eid av kraftforsyningen selv, og dels leid som tjenester i det offentlige telemarkedet.

Kraftsektoren er organisert på ulike måter rundt aktivitetene produksjon, omsetning og overføring av kraft. Avhengig av hvilken virksomhet som drives, betegnes ofte selskapene som produksjonsselskap, nettselskap, omsetningsselskap, vertikalt integrerte selskap eller industriverk, i noen tilfeller omtalt under samlebetegnelsen energiverk. I tillegg er det etablert selskaper som kun driver megling og formidling av kraftkontrakter.



Figur 10.4 Omsetningskonsesjonærer etter virksomhet.

Kilde: OED Faktahefte 2005.

10.3.2 Beskrivelse av eierforhold og organisering

Alle som skal levere og omsette elektrisk energi må ha omsetningskonsesjon. 1. januar 2005 var det til sammen 328 selskaper med omsetningskonsesjon i Norge. Figur 10.4 viser hvordan disse selskapene fordeler seg på ulike former for virksomhet i sektoren.

228 selskaper er helt eller delvis kommunalt eid, og 137 av disse har kun kommunale eiere. Et selskap som bare har kommunale eiere kan likevel ha flere kommuner som eiere.

Mange selskaper har flere eiere og det er stor grad av krysseierskap i sektoren. Kommunene og fylkeskommunene eier om lag 50 prosent av produksjonskapasiteten i landet. Staten, gjennom Statkraft AS, eier om lag 37 prosent og private selskaper om lag 13 prosent.

Dersom det tas hensyn til Statkrafts eierandeler i selskaper som også har kommunale eiere, vil den statlige andelen være om lag 40 prosent. Staten eier store deler av sentralnettet. I tillegg eier private selskaper, fylkeskommuner og kommuner noe av sentralnettet.

10.3.2.1 Produksjon (kraftverkene)

I 2004 var det totalt 165 selskaper som produserte kraft i Norge. Av disse var 115 organiserte som aksjeselskaper. De fleste produsentene er eid av fylkeskommuner og kommuner. Ofte eier flere kommuner kraftselskaper i fellesskap.

Tabell 10.2 De 10 største kraftprodusentene i Norge pr. 1.januar 2005.

Produksjonsselskap	Midlere årsproduksjon		Installert effekt	
	TWh	Markedsandel (prosent)	MW	Prosent
Statkraft AS	35,8	31,2	8644	31,3
BKK AS	6,8	5,7	1541	5,6
E-CO Vannkraft AS	6,8	5,7	1887	6,8
Norsk Hydro ASA	6,6	5,5	1339	4,8
Lyse Produksjon AS	5,9	5,0	1544	5,6
Agder Energi AS	5,6	4,7	1188	4,3
Skagerak Kraft AS	4,0	3,4	1056	3,8
Nord-Trøndelag Elektrisitetsverk FKF	3,2	2,7	802	2,9
Trondheim Energiverk Krafs AS	3,2	2,7	746	2,7
Hafslund ASA – Sarpsborg	2,6	2,3	504	1,8

Kilde: NVE.

De 10 største kraftprodusentene i Norge disponerer om lag 70 prosent av total midlere produksjonskapasitet i landet, og har installert omtrent den samme andelen av total effekt. Statkraft har en dominerende andel innen kraftproduksjonen i Norge.

Mange av de privateide produksjonsselskapene er industriverk som i all hovedsak produserer kraft til egen industrivirksomhet.

10.3.2.2 Distribusjon

Et nettselskap kan eie lokalnett, regionalnett og/eller sentralnett. Totalt er det 173 selskaper som har nettvirksomhet på ett eller flere nivåer. 45 av selskapene er rene nettselskaper. De øvrige driver i tillegg også med produksjon og/eller omsetningsvirksomhet.

De fleste nettselskapene er helt eller delvis eid av en eller flere kommuner. Kommuner og fylkeskommuner eier det meste av regionalnettene og de lokale distribusjonsnettene. Statnett SF, som eier om lag 87 prosent av sentralnettet, er eid av staten.

Rundt 60 % av selskapene som driver nettvirksomhet er organisert som aksjeselskap, mens andre er organiserte som andelslag eller som kommunale, fylkeskommunale eller interkommunale bedrifter.

10.3.2.3 Omsetning

Omsetningsselskap kjøper kraft i markedet for videresalg, i all hovedsak til sluttbrukere. Dette tilsvarer i stor grad omsetningsvirksomheten i de tradisjonelle distribusjonsselskapene.

Totalt er det 226 selskaper som driver kraftomsetning. Av disse er det 80 selskaper med omsetning som eneste virksomhet. De fleste omsetningsselskapene er organisert som aksjeselskap.

10.3.2.4 Privat eierskap

Det er private eierinteresser innenfor alle virksomhetsområdene (produksjon, omsetning og overføring). Om lag 42 prosent av selskapene der det kun er private eierinteresser er rene omsetningsselskaper.

Utenlandske eierinteresser er relativt begrensede i norsk kraftforsyning, men det er enkelte utenlandske selskap som har fått omsetningskonsesjon i Norge. Disse driver i all hovedsak handel i engrosmarkedet/spotmarkedet. I tillegg har utenlandske foretak kjøpt eierandeler i norske selskaper som har omsetningskonsesjon eller opprettet egne norskregistrerte datterselskaper. De utenlandske eierinteressene er i stor grad konsentrert om selskaper som driver omsetning, men også eierandeler i produksjons og nettvirksomhet forekommer.

10.3.2.5 Vertikal integrering

Vertikal integrering ble diskutert i den Odelstingsproposisjon som ligger til grunn for energiloven av 1990. Hensyn som taler for og imot slik organisering ble drøftet. Det endte med å ikke oppstille krav om selskapsmessig skille i loven. Den har kun krav om regnskapsmessig skille. Loven er uendret på dette punkt i dag.

I forbindelse med tildeling av omsetningskonsesjoner, sier NVE om nettselskap i konsern: «Ved sammenslåinger, kjøp/oppkjøp, annen ervervelse eller etablering hvor både nettvirksomhet og konkurranseutsatt virksomhet er involvert, kan NVE stille krav til organisering. En løsning som NVE har akseptert er en konsernorganisering hvor monopolvirksomheten organiseres i et eget datterselskap.»

Tabell 10.3 De 10 største nettselskapene (distribusjonsnett pr. 1.1.2004).

Nettselskap	Antall abonnenter	Overført mengde (GWh/år)
Viken Nett AS	466 423	10 006
Skagerak Nett AS	174 901	4 382
BKK Nett AS	171 156	4 276
Agder Energinett AS	154 438	3 260
Lyse Nett AS	111 030	3 366
Eidsiva Energinett AS	102 182	2 379
Fortum Distribusjon AS	95 021	2 108
Trondheim Energiverk Nett AS	89 088	2 135
Nord-Trøndelag Elektrisitetsverk, FKF	76 463	1 853
Troms Kraft Nett AS	62 605	1 862

Kilde: NVE (Viken Nett AS har senere skiftet navn til Hafslund Nett AS).

10.3.3 Utvalgets vurderinger og anbefalinger knyttet til virkemidlene

10.3.3.1 Eierskap som virkemiddel

Et særtrekk ved den norske kraftreformen sammenlignet med for eksempel Storbritannia, var at det ikke skjedde noen privatisering samtidig med at markedsbasert kraftomsetning ble innført. I St.prp. nr. 100 (1990-1991), jf. Innst.S. nr. 28 (1991-1992), argumenterer Olje- og energidepartementet for at «kraftproduksjonsanlegg [...] er verdier av nasjonal betydning som staten må ha et særlig ansvar for. Det er ikke ønskelig at staten gir fra seg en direkte og nær kontroll med betydelige deler av disse ressursene.» Tilsvarende heter det at «det sentrale overføringsnett vil ha en funksjon som instrument i den statlige sektorpolitikk på energiområdet.»

Det heter videre om Statnett at selskapet bør kunne oppnå en rimelig avkastning på investert kapital. Samtidig må kravene til den tekniske standarden og beredskapen i sentralnettet fastsettes «ut fra en vurdering av de samfunnsmessige kostnadene ved strømbrudd ved en gitt driftssikkerhet samt kostnader ved tap i overføringsnettet». Alt i alt legges det opp til en balanse mellom et variert offentlig virkemiddelsett og desentraliserte beslutninger på forretningsmessig basis både for Statkraft og Statnett, men den samfunnsøkonomiske målfunksjonen er klarere uttrykt for Statnetts vedkommende.

Sentralnettet har karakter av kritisk infrastruktur i egenskap av å utgjøre et landsdekkende transportnett. Statnett er et resultat av at den tidligere statlige forvaltningsbedriften Statkraftverkene ble delt opp i de to selskapene Statkraft AS og Statnett SF. Statkraft AS ivaretar den konkurransebaserte produksjonen av kraft (kraftverk), mens Statnett SF har ansvaret for sentralnettet som har karakter av naturlig monopol, og har dessuten det nasjonale systemansvaret. En kan derfor si at vi her har vertikal separasjon mellom enerettsvirksomheten som består i å forvalte det landsdekkende overføringsnettet og konkurransevirksomheten i kraftproduksjon og -distribusjon til sluttbrukere.

Selv om selskapsformene i sektoren for øvrig i stor grad er endret fra kommunale bedrifter til aksjeselskaper, er andelen av offentlig eierskap til disse fremdeles dominerende. Spørsmålet er da hvorvidt dette eierskapet i seg selv er et nødvendig og viktig virkemiddel for å ivareta rikets sikkerhet og nasjonale interesser.

Vurderinger og anbefalinger

Beredskapshensyn kan i prinsippet ivaretas gjennom forskjellige typer offentlige pålegg, jf. forskrift om beredskap i kraftforsyningen. Slike pålegg medfører kostnader, som kan dekkes via statsbudsjettet eller andre finansieringsordninger i den grad tiltakene ikke er bedriftsøkonomisk lønnsomme. Her er det heller ingen prinsipielle forskjeller mellom private og offentlige aktører med bedriftsøkonomiske målfunksjoner.

I nettet er det mye som tyder på at visse typer investeringer vil være vanskelige å gjennomføre på bedriftsøkonomisk grunnlag. Det gjelder særlig i sentralnettet og i noen grad også regional- og distribusjonsnettet, hvor investeringer kan ha en rekke nyttevirkninger som er vanskelige å måle og dermed prissette i et marked eller gjennom et nettreguleringsregime bare basert på bedriftsøkonomiske incentiver. Det skyldes ikke minst at bidraget til leveringssikkerheten fra en investering kan være svært vanskelig å beregne og verdsette. Ulike prosjekter i nett, produksjon og forbruk kan dessuten være gjensidig avhengige. Skjev fordeling av informasjon mellom aktører og asymmetri i virkemidler mellom nettselskaper, andre infrastrukturselskaper og konkurranseutsatte aktører skaper dessuten rom for strategisk atferd, som kan resultere i så vel over- som underinvesteringer. Mange av de samme problemstillingene er relevante også på lavere nettnivåer, ikke minst når utbygging av lokal kraftproduksjon får et visst omfang. Erfaringer gjort av DSB gjennom deres tilsynsvirksomhet tyder på at nettselskapene tilpasser seg – og sine investeringer/disposisjoner – ut fra rene økonomiske vurderinger som til tider er meget kortsiktige, men som kan få uheldige langsiktige virkninger på sårbarheten og dermed leveringssikkerheten. Det er stedvis også et problem at nettselskapene i stor grad har satt ut («*outsourcet*») sine entreprenør- og vedlikeholdstjenester med den følge at den lokale kunnskapen om deres eget nett har forsvunnet. Dette ville i seg selv ikke være kritisk dersom denne lokalkunnskapen hadde blitt dokumentert før den forsvant, men det har stedvis ikke skjedd.

I fravær av tilfredstillende økonomiske og juridiske reguleringsmekanismer for samfunnsøkonomisk riktige nettinvesteringer er eierskapet til Statnett SF sannsynligvis et egnet virkemiddel for å ivareta sikkerhetshensyn i kraftsystemet på lang sikt. De viktigste funksjonene i Statnett i det henseende er selve systemansvaret (den løpende systemdriften) og muligheten til både å fatte beslutninger om hvilke investeringer som skal gjøres og finansiere investeringene selv. Det betyr likevel ikke at private (eller for den saks skyld kommunale) investeringer i overføringskapasitet i sentral-

nettet bør utelukkes, men Statnett bør ha et helhetsansvar.

Statnett sitter med det overordnede systemansvaret og ansvaret for å holde oppe et landsdekkende nett uten flaskehalser. Dette er oppgaver som ikke uten videre materialiserer seg i inntekter til enhver tid. Utvalget er kjent med at et annet utvalg arbeider med dette spørsmålet og skal avlevere sin innstilling om kort tid. Utvalget påpeker viktigheten av at det ved vurdering av de økomiske virkemidlene innen kraftsektoren, tas høyde for å ha et landsdekkende nett uten flaskehalser.

Ut fra sikkerhets- og beredskapshensyn er det vanskelig å se at det vil være noe å vinne på privatisering av sentralnettet, siden det er mulig å konkurranseutsette enkeltfunksjoner om det skulle være ønskelig.

I og med at utvalget ikke anser distribusjonsnettet som fullt så kritisk som sentralnettet, er det grunn til å anta at argumentet for offentlig eierskap er svakere, men det er behov for supplerende virkemidler i form av kvalitetskrav, leverings- og tilknytningskrav, oppføling av forskrifter, osv. Eventuelt kan staten definere beredskapsbehov og sørge for tilstrekkelig finansiering via inntektsrammene eller statlige overføringer (i noen grad skjer dette allerede i dag gjennom beredskapsforskriften og inntektsrammereguleringen).

Særskilt om hjemfall

Det er foretatt en offentlig utredning om hvordan hjemfallsinstituttet kan videreføres under nye rammebetingelser som følger av EØS.[15] Dagens hjemfallsordning innebærer at private eiere av kraftverk har konsesjoner som utløper etter 60 år. Offentlige eiere og private som har eid kraftverket fra tiden før hjemfall ble innført har evigvarende konsesjoner.

Hjemfallsutvalget ble delt i synet på hvordan konsesjonsbestemmelsene skal videreføres. Flertallet foreslår at alle eiere gis en konsesjonstid på 75 år fra det tidspunkt ny lov trer i kraft. Det foreslås videre at konsesjonæren får beholde 1/3 av kraftverket for evig tid etter konsesjonstidens utløp. Dette innebærer foruten at offentlige eiere får tidsbegrenset konsesjon, at private eiere som i dag har konsesjoner som utløper i tidsrommet 2010 til 2050 får forlenget konsesjonstiden frem til 2080.

Mindretallet i hjemfallsutvalget foreslår primært hjemfall 60 år etter et eventuelt salg kun for de kraftverk som blir solgt. Det vil si at offentlige eiere som sitter på evigvarende konsesjoner vil beholde disse så lenge de ikke selger (omtalt som transaksjonsmodellen). Sekundært foreslår mindretallet hjemfall for alle etter 60 år fra lovendringsdato, med kompensasjon på 45 % av verdien for tapt evigvarende konsesjon, dersom dette faktisk er en tapt rettighet for opprinnelig eier.

Spørsmålet om hjemfall har betydning for kraftforsyningen også i det perspektiv utvalgets mandat har. Spesielt er utvalget opptatt av muligheten for at eierskap til store deler av kraftverkene kan bli overført til utenlandske kraftselskap. Dette vil kunne føre til en svekkelse av kontrollen med beredskapssystemet i kraftsektoren, som blant annet består av og er avhengig av sikkerhetsklarerte personer fra kraftselskapene med helt nødvendig kompetanse.

Utvalget vil derfor sterkt anbefale at hjemfallsinstituttet videreføres på en slik måte at dagens offentlige, nasjonale eierskap til kraftressursene på sikt ikke svekkes.

Strømrasjonering

Situasjoner med begrenset kapasitet i strømnettet kan oppstå både som følge av naturkatastrofer og terror- eller sabotasjehandlinger. Det er en kjent problemstilling at distribusjonsnettet i Norge (og i de fleste andre land) har en slik nettstruktur at det er svært vanskelig å prioritere levering av strøm til enkeltvirksomheter under slike forhold.

Utvalget mener likevel at myndighetene må arbeide for å finne frem til løsninger som kan ivareta dette behovet så langt som mulig. På bakgrunn av de alvorlige konsekvenser langvarige strømutfall kan få, må kanskje samfunnet akseptere relativt høye kostnader dersom det finnes teknologiske løsninger på dette problemet.

I Karlskrona kommune i Sverige drives et forsøksprosjekt med radiostyring av transformatorstasjoner ved hjelp av datamaskiner som tar beslutninger om utkopling av soner så å si i det øyeblikk det skjer en hendelse i strømnettet. Norske myndigheter bør følge med på de erfaringer man gjør i dette prosjektet, og for øvrig bruke ressurser på vurdering og eventuell utprøving av andre løsninger.

Samtidig bør det vurderes hvordan det kan sikres at kritiske samfunnsfunksjoner blir understøttet av reserveaggregater i større utstrekning enn hva som er tilfelle i dag. Utvalget har pekt på at en tilskuddsordning blant annet kan være incitament til økte investeringer for dette formålet. Det må muligens også vurderes å stille krav om etablering av nødstrømsaggregater for enkelte spesielt kritiske samfunnsfunksjoner.

[15] NOU 2004:26 *Hjemfall*.

10.3.3.2 Regulatoriske virkemidler

I kjølvannet av energiloven er det utviklet et omfattende og sammensatt virkemiddelapparat for å ivareta sikkerhetshensyn. Virkemidlene er dels økonomiske, for eksempel ved å inkludere kundenes kostnader ved avbrudd som en del av reguleringen av nettselskapene. Dels består virkemidlene i forskrifter, påbud og retningslinjer som fordeler ansvar og plikter for beredskap og sikkerhet mellom myndigheter og selskaper.

Kraftsektoren reguleres først og fremst gjennom energiloven og vassdragsloven med tilhørende forskrifter og retningslinjer. Selv om markedskreftene har fått mer innpass i kraftsektoren, reguleres virksomheten fortsatt gjennom konsesjoner:

- Anleggskonsesjon – anlegg for produksjon, omforming, overføring og fordeling av elektrisk energi med høy spenning, kan ikke bygges eller drives uten konsesjon.
- Områdekonsesjon – gis for bygging og drift av anlegg for fordeling av elektrisk energi med spenning opp til et nivå som fastsettes av departementet.
- Omsetningskonsesjon – gjelder andre aktører enn staten. Det kan knyttes ulike vilkår til konsesjonen.

Beredskapstankegangen har vært – og er – basert på et regelstyrt regime med beredskapsforpliktelser pålagt alle virksomheter. Beredskap innenfor kraftforsyningssektoren er først og fremst regulert gjennom lov og regelverk.

De viktigste reguleringene finner vi følgende steder:

- Energilovens beredskapskapittel (kapittel 6) inneholder bestemmelser om kraftforsyningens beredskapsorganisasjon (KBO), vedtaksmyndighet, pålegg om sikringstiltak, fordeling av utgifter og vedrelag ved gjennomføring av sikringstiltak, meldeplikt ved bygging eller endring av kraftforsyningsanlegg og gebyr til dekning av utgifter ved beredskapsarbeidet.
- Energilovforskriftens beredskapskapittel (kapittel 6) inneholder blant annet utfyllende bestemmelser om KBO, sikringstiltak, forebyggende sikkerhet, økonomiske rammer og statlig tilskudd, gebyr og gjennomføring og tilsyn.
- NVE vedtok 16. desember 2002 en ny forskrift om beredskap i kraftforsyningen som inneholder ulike typer krav knyttet til beredskap i kraftforsyningen, herunder om ulike aktørers oppgaver, plikter, ansvar m.m. Det er også utarbeidet en veiledning til denne forskriften.
- Lov om tilsyn med elektriske anlegg og elektrisk utstyr

Kraftforsyningens beredskapsorganisasjon (KBO) er en landsomfattende organisasjon bestående av NVE og de virksomhetene som står for kraftforsyningen, dvs. alle enheter som eier eller driver kraftproduksjon med tilhørende vassdragsregulering, overføring og distribusjon av elektrisk kraft og fjernvarme.

Ved krigsberedskap overtar KBO ansvaret for landets kraftforsyning. Alle kraftforsyningsenheter plikter å rette seg etter direktiver fra overordnet myndighet i KBO. KBO skal i tillegg kunne løse oppgaver i fred ved skade på kraftanlegg som følge av naturgitte forhold, teknisk svikt, terror- eller sabotasjeaksjoner samt i forbindelse med rasjonering etter energiloven. Etter energikrisen vinteren 2002-2003 har KBO fått utvidede fullmakter knyttet til rasjonering.

Tilsynsvirksomhet innen sektoren

Det er særlig to tilsynsmyndigheter som er inne i bildet i forhold til sikkerhet og beredskap. (Virksomhetene må likevel forholde seg til en lang rekke andre offentlige tilsyn på andre områder som også kan virke inn på sikkerhet og beredskap).

NVE kontrollerer at kraftselskapene har beredskap mot havarier og sikrer at kraftforsyningens rolle i den sivile beredskapen blir ivaretatt. NVE fører også tilsyn med at eierne av dammer og andre anlegg i vassdragene ivaretar det ansvaret de har for å være forberedt mot unormale hendelser, og at de overholder konsesjonsvilkår, manøvreringsreglement og andre regler med hensyn på natur og miljø.

DSB driver tilsyn etter lov om tilsyn med elektriske anlegg og elektrisk utstyr og selv om deres regelverk i hovedsak er rettet mot tekniske forhold er det knapt en paragraf i DSBs regleverk som ikke virker inn på beredskapen og sikkerheten.

I den utstrekning virksomheter kommer inn under sikkerhetsloven vil de også måtte være forberedt på tilsyn fra NSM.

Vurderinger og anbefaling

Kraftsektoren er den sektoren som kanskje har kommet lengst med hensyn til innføring av reguleringsmekanismer for sikring av den kritiske infrastrukturen. Utvalget mener at hensynet til sikkerhet og nasjonale interesser i forbindelse med dereguleringsprosessen innenfor denne sektoren er ivaretatt på en god måte.

Utvalget har imidlertid registrert at forholdet til sikkerhetsloven ikke er tilstrekkelig avklart hos flere av de store aktørene. Dette gjelder også for Statkraft og Statnett. Heller ikke kommunalt eide aksjeselskaper er omfattet av sikkerhetsloven, og kan dermed ikke skjerme informasjon eller objekter med hjemmel i loven. De har heller ikke hjemmel til å foreta sikkerhetsklarering av nøkkelpersonell i den utstrekning det anses formålstjenlig.

10.3.3.3 Økonomiske virkemidler

For å stimulere til reinvesteringer og ivareta kvalitetshensyn ble den såkalte KILE-ordningen (Kvalitetsjusterte inntektsrammer ved ikke levert energi) innført fra 2001. Nettselskapene påføres en økonomisk straff ved avbrudd som varer mer enn 3 minutter. Avbrudd gir opphav til en inntektsreduksjon basert på mengden ikke-levert energi og avbruddssatser pr. kWh. Avbruddssatsene varierer fra 7 kr/kWh til 99 kr/kWh avhengig av kundetype og hvorvidt avbruddet er varslet eller ikke.

Fra 2007 skal nettreguleringen revideres. I henhold til NVEs forslag skal ordningen med kvalitetsincentiver videreføres og utvides til å omfatte kortvarige avbrudd. I tillegg skal nettselskapene betale direkte kompensasjon til de berørte kundene ved avbrudd som varer mer enn 12 timer. Samtidig kan oppdateringsreglene for inntektsrammene og valg av parametere som referanserente bidra til lønnsomhet i forskjellige typer investeringer. I distribusjonsnettet har dessuten selskapene tilknytnings- og leveringsplikt, som også har konsekvenser for investeringene.

Vurderinger og anbefalinger

Analyser av nettselskapenes tilpasning til KILE-ordningen tyder på at ordningen gir signaler som tas hensyn til i selskapenes beslutninger om investeringer og vedlikehold[16]. Det er ikke gitt at ordningen gir tilstrekkelige virkemidler til at leveringskvaliteten og beredskapen holdes på et akseptabelt nivå. KILE er primært et *langsiktig* virkemiddel for å stimulere til investeringer og vedlikehold, og kan ha gode samfunnsøkonomiske egenskaper med hensyn til leveringssikkerheten hvis ordningen er hensiktsmessig utformet. I denne sammenheng bør det vurderes hvorvidt inntektsrammereguleringen også kan brukes som middel for å sikre vedlikehold av nødvendig kompetanse og til å pålegge selskapene til enhver tid å holde oppdaterte kartdata over sine nett.

[16] Omtalt i ECON-notat nr. 2005-056. *Kritisk infrastruktur og offentlig eierskap* - i del 2, vedlegg 12.

At reinvesterings- og vedlikeholdstakten i nettselskapene har falt sterkt de senere årene – til et nivå som forutsetter en levetid på mer enn hundre år for komponenter i nettene – er sentrale forhold som bør vies oppmerksomhet fra myndighetenes side.

10.4 Vann og avløp (VA)

En tilfredsstillende vannforsyning og avløpshåndtering er en forutsetning for det moderne samfunnet, og VA-infrastrukturen scorer høyt på de fleste kriteriene for utvelgelse av kritisk infrastruktur, jf. kapittel 3.1:

- *Avhengighet:* Både husstander, institusjoner, arbeidsplasser, skoler/barnehager, industrivirksomheter m.m. er avhengige av at VA-tjenestene fungerer og vil raskt bli berørt ved bortfall av tjenesten.
- *Alternativer:* I og med at VA-infrastrukturen er et naturlig monopol, er det ingen konkurrerende, overlappende systemer for innbyggere og næringsliv dersom tjenesten svikter.
- *Tett kobling:* En styrke ved VA-infrastrukturen, i motsetning til eksempelvis kraftforsyningens landsdekkende samkjøring, er at svikt ved ett vannverk normalt ikke vil påvirke driften av andre vannverk. Imidlertid vil svikt i en del av systemet, for eksempel forurensning av vannkilde, kunne få store konsekvenser for resten av systemet. Av den grunn er det viktig at det enkelte vannforsyningssystem er bygget opp med en tilstrekkelig robusthet, eksemplvis med reservevannkilder, høydebassenger osv.

Vannverkene har som oppgave å sørge for både nok vann, godt vann og sikker forsyning. Erfaringer fra hendelser der vannforsyningen har sviktet, viser at de største problemene oppstår som følge av vannmangel til hygieniske formål. Dersom man ikke lenger har vann til å skylle ned i toalettene, vil både byer/tettsteder og de enkelte virksomheter lammes. Det blir også raskt kritisk dersom man ikke har vann til kroppsvask, særlig for pleietrengende. Sykehus er eksempel på virksomheter som er avhengige av kontinuerlige tilførsler av rent vann.

Næringsmiddelindustrien er avhengig av rent vann og nok vann i sin produksjon. Hotell- og utelivsbransjen vil måtte stenge etter kort tid som følge av stans i vannforsyningen. Brannvesenet og virksomheter som baserer sitt brannvern på sprinkling, vil få åpenbare problemer dersom vannleveransene svikter under en brann, særlig ved større branner der det ikke foreligger naturlige vannkilder rett i nærheten.

Hvis drikkevannet er forurenset og når ut til abonnentene før man er klar over situasjonen, vil utbrudd av vannbårne sykdommer kunne ramme enkeltindivider og samfunnet tungt. Et nylig eksempel på det er parasittutbruddet i Bergen høsten 2004 med 1400 syke, som følge av at drikkevannet en periode var forurenset med parasitten *Giardia,* og vannbehandlingen på vannverket på det tidspunkt ikke var egnet til å uskadeliggjøre parasitter.

Konsekvensene ved svikt i vannforsyningen påvirkes av en rekke faktorer. For det første er det tidsfaktoren. En utredning fra 2003, om sårbarhet i vannforsyningen, viser til at svikt i vannforsyningen noen få timer neppe gir store samfunnsmessige konsekvenser, men konsekvensene vil øke sterkt utover i det første døgnet. Også det geografiske omfanget av hendelsen vil ha betydning, for eksempel vil svikt i vannforsyningen til de større bysentraene få større konsekvenser enn svikt i vannforsyningen til mindre tettbygde strøk, fordi det vil være lettere å finne alternative måter å skaffe seg vann på i bygdesamfunn. Hvor god beredskap vannverkene og kommunene har, herunder informasjonsberedskap, vil også påvirke hvor store konsekvensene blir[17].

Det mest kritiske scenariet med tanke på avløpssektorens funksjonsdyktighet, er at vannforsyningen svikter slik at man ikke får spylt ned i toalettene. En annen form for kritisk situasjon kan oppstå dersom avløpssystemet skulle bli fylt med eksplosive eller giftige gasser, med risiko for eksplosjoner, branner eller forgiftning i bygningene som er tilknyttet avløpssystemet. Et tredje tenkelig scenario er at større transportsystemer eller renseanlegg for avløpsvann blir satt ut av funksjon, noe som vil kunne føre til forurensede drikkevannskilder og uakseptable hygieniske tilstander i nærområdet for utslippet. I og med at vann- og avløpsledninger av praktiske og økonomiske grunner ligger i samme grøft, vil dessuten hendelser på avløpsnettet eller generelt forfall med forurensning som resultat, kunne påvirke drikkevannskvaliteten ved reparasjoner eller ved kortvarige trykkfall i vannledningene.

10.4.1 Overordnet beskrivelse av infrastruktur og samfunnsfunksjon

Norge har store mengder vann og bedre kvalitet på vannet i naturen enn de fleste andre land. Årlige tilgjengelige ferskvannsressurser i Norge er på om lag 381 milliarder kubikkmeter i et normalår[18]. Det tilsvarer et forbruk på 175 liter per person per døgn for verdens om lag 6 milliarder mennesker. Det er et naturgitt godt utgangspunkt for vannforsyningstjenesten til innbyggere og næringsliv. Kvalitetskrav til drikkevann er regulert i drikkevannsforskriften, men det er også en rekke andre forskrifter som regulerer vannforsyningstjenesten, herunder regler knyttet til beredskapsplanlegging, damsikkerhet, brannvannforsyning m.v.

Om lag 40 % av vannproduksjonen ved norske vannverk går til husholdningene, 9 % til næringsmiddelindustrien, 9 % til annen industri, 11 % til jordbruk og andre formål, mens 31 % av vannproduksjonen går tapt som lekkasjer på ledningsnettet[19]. Hver dag bruker norske husholdninger om lag 200 liter vann per person. Rundt 10 liter går til drikke og matlaging, mens det øvrige primært går til andre formål, som renhold, hygiene, klesvask, toalettspyling m.m. Vann er menneskets viktigste næringsmiddel, og et voksent menneske trenger rundt 2-3 liter væske per dag.

Avløpsvann er vann som er brukt i husholdninger, industri og annen virksomhet, og som må borttransporteres og renses forsvarlig før utslipp til naturen igjen. Kravene til rensing er hjemlet i forurensningsforskriften og varierer avhengig av blant annet størrelsen på utslippet og følsomheten/tilstanden til resipienten der renset avløpsvann skal slippes ut.

Slammet fra renseprosessen gjenbrukes i stor grad som gjødsel- og jordforbedringsmiddel i jordbruket og på grøntarealer, etter å ha gjennomgått behandling for å fjerne lukt og smittestoffer og etter en kontroll av at miljøgiftinnholdet er tilfredsstillende lavt, jf. krav i gjødselvareforskriften.

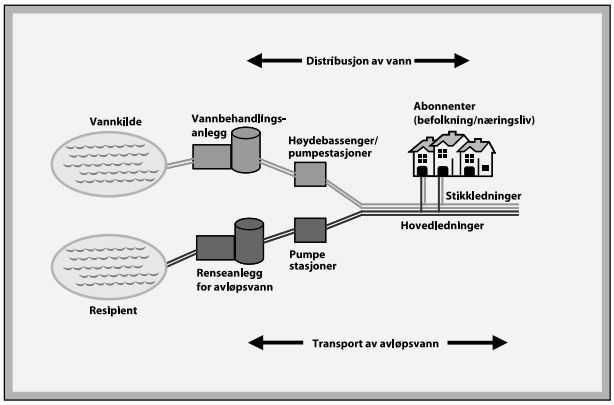
Skjematisk kan VA-infrastrukturen grovt inndeles i disse enhetene, se figur 10.5:

- Vannkilde (grunnvann eller overflatevann) og tilhørende nedbørfelt
- Vanninntak
- Vannbehandlingsanlegg
- Distribusjonssystem for vann (ledningsnett, tunneler, høydebasseng, pumpestasjoner)
- Transportsystem for avløpsvann (ledningsnett, tunneler, pumpestasjoner)
- Avløpsrenseanlegg, inkludert slambehandlingsanlegg
- Utslippsledning
- Resipient for renset avløpsvann

[17] Scandpower Risk Management, Forsvarets forskningsinstitutt, Aquateam, Hjellnes-COWI 2003. *Sårbarhet i vannforsyningen*

[18] Statistisk sentralbyrå 2005. *Naturressurser og miljø 2005.*

[19] Statistisk sentralbyrå 2005. *Naturressurser og miljø 2005.*



Figur 10.5 Prinsippskisse VA-infrastruktur.

Vann- og avløpsverkene varierer mye i størrelse, fra de helt minste som betjener en mindre gruppe hus, til de store som sørger for vann- og avløpstjenester til store byer/regioner. I følge offisiell statistikk fra SSB er det 1727 vannverk som leverer vann til 50 personer eller mer, og disse sørger for vannforsyning til 90 % av landets befolkning. Tilsvarende er det 2597 avløpsanlegg som tar hånd om avløpet fra mer enn 50 PE (personenheter, målt som hydraulisk kapasitet), og disse dekker behovet for 80 % av befolkningen. Den resterende del av befolkningen får dekket sitt behov med mindre anlegg eller separate løsninger[20].

90 % av befolkningen som er tilknyttet et vannverk, får sin vannforsyning fra overflatevannkilder, som innsjøer/tjern og elver/bekker, mens 10 % får vann fra grunnvannskilder[21].

For distribusjon av vann og borttransport av avløp er det lagt om lag 46 000 km hovedvannledninger og om lag 40 000 km hovedavløpsledninger (inkludert overvannsledninger). I tillegg er det private stikkledningsnettet til/fra bygningene estimert å være om lag 22 000 km. Det innebærer at total lengde av vann- og avløpsledninger i Norge tilsvarer nesten tre ganger avstanden rundt ekvator.

Stipulert gjenanskaffelsesverdi for vann- og avløpsinfrastrukturen er på over 430 milliarder kroner, hvorav transportsystemene for vann og avløp utgjør hele 90 %.[22] Årlig omsetning i vann- og avløpssektoren er omlag åtte milliarder kroner. Det er vel 6000 ansatte innenfor vann- og avløpssektoren, i tillegg jobber flere tusen innenfor entreprenørbransjen periodevis med bygging av VA-anlegg.

[20] Statistisk sentralbyrå 2005. *Naturressurser og miljø 2005.*
[21] Statistisk sentralbyrå 2005. *Naturressurser og miljø 2005.*
[22] NORVAR-rapport 130/2003. *Gjenanskaffelseskostnader for norske vann- og avløpsanlegg.*

10.4.2 Beskrivelse av eierforhold og organisering

Det er i hovedsak kommunene som sørger for vann- og avløpstjenester i Norge i dag, selv om det ikke er en direkte lovpålagt oppgave for kommunene. Blant de 90 % av befolkningen som er tilknyttet et vannverk, får hele 95 % av disse sitt drikkevann fra vannverk som er eid av en eller flere kommuner. De resterende 5 % får vann fra vannverk som normalt er organisert som private andelslag, der abonnentene har gått sammen om å lage en felles vannforsyningsløsning. Det er om lag tilsvarende eierstruktur i avløpssektoren.

Flere kommuner har etter hvert endret organiseringsform for sin VA-virksomhet, fra å være en integrert del av den kommunaltekniske virksomheten til å være organisert som et interkommunalt selskap, kommunalt foretak eller kommunalt aksjeselskap:

- Det er en rekke interkommunale VA-selskaper, i hovedsak organisert med hjemmel i lov om interkommunale selskaper. Selskapene er engros-selskaper som leverer renset drikkevann til kommunene og/eller tar imot avløpsvann fra kommunene for rensing.
- En del kommuner har skilt VA-virksomheten sin i en bestillerdel og en utførerdel. Utførerdelen gjelder driftsoppgaver og i noen tilfeller også anleggsvirksomhet. Ofte er da utførerenheten organisert som kommunalt foretak iht. kapittel 11 i kommuneloven.
- I noen få tilfeller er VA-virksomheten skilt ut som kommunalt eide aksjeselskap, men med kommunal styring av budsjetter for utvidelser og fornyelser.

Utbyggingsoppgaver blir i stor grad utført på anbud av private aktører, mens forvaltningsoppgaver og driftsoppgaver normalt skjer i regi av kommunene og VA-virksomhetene selv. Det kan også forekomme at drift av vannbehandlingsanlegg/ renseanlegg settes ut på anbud, men dette har ikke vært vanlig i Norge frem til i dag.

10.4.3 Utvalgets vurderinger og anbefalinger knyttet til virkemidlene

10.4.3.1 Eierskap som virkemiddel

Som drøftet i kapittel 9 er VA-sektoren karakterisert ved at det er sterk synergi mellom selve infrastrukturvirksomheten (tekniske anlegg) og konkurransevirksomheten (leveranse av vann og borttransportering av avløp), noe som taler for vertikal integrasjon av disse virksomhetene. Samtidig er det av kvalitetsmessige, sikkerhetsmessige og

kostnadsmessige hensyn lite aktuelt å åpne opp for konkurrerende vannleverandører inn på samme forsyningsnett, utover de avtaleregulerte forsyningsmuligheter enkelte vannverk har etablert med nabovannverk for blant annet å ha økt leveringssikkerhet ved vannknapphet.

Av kostnadsmessige grunner vil det videre være uaktuelt å bygge ut konkurrerende infrastruktur for vann og avløp i den enkelte kommune/forsyningsområde. VA-tjenestene fremstår derfor som naturlige monopolvirksomheter, og man vil ikke kunne oppnå reell konkurranse om slike tjenester, som normalt er det viktigste argumentet for privatisering. I valget mellom offentlig monopol og privat monopol er det således mye som taler for offentlig eierskap til VA-infrastrukturen.

Det er vanskelig å spå om det på noe tidspunkt kan komme overnasjonale føringer når det gjelder spørsmålet om liberalisering av norsk VA-sektor. I en SINTEF-rapport fra 2005, utført på oppdrag fra Kommunenes Sentralforbund, er dette spørsmålet drøftet nærmere. Konklusjonen er at det på kort sikt ikke forventes noe vedtak fra EUs side om liberalisering av VA-sektoren, blant annet som følge av at VA-tjenestene er organisert forskjellig fra land til land. På lengre sikt er det mer usikkert, men det antas at et eventuelt liberaliseringstrykk i første rekke vil komme fra det enkelte land. Ulike scenarier peker uansett i retning av et moderniseringspress mot sektoren. SINTEF stiller også spørsmål ved om påtrykk om liberalisering fra WTO-land gjennom GATS-avtalen kan bli vel så sterkt som påtrykk fra EU[23].

Vurderinger og anbefalinger

Manglende ivaretakelse av sikkerheten i VA-sektoren vil kunne ha store konsekvenser for andre samfunnssektorer, innbyggere og næringsliv, som er avhengig av en velfungerende VA-tjeneste. Sikkerhetsutfordringene gjelder både i et kortsiktig perspektiv (tilstrekkelige sikkerhetsmarginer teknisk og organisatorisk til enhver tid) og i et langsiktig perspektiv (tilstrekkelige fornyelser for å ivareta sikkerheten for kommende generasjoner).

Som nevnt i kapittel 9 er det mye som taler for at VA-infrastrukturen bør være offentlig eid. Utvalget ønsker å peke på følgende sikkerhetsmessige aspekter, som trekker i retning av samme konklusjon:

- Norsk VA-sektor består av svært mange enheter og er lite homogen, til forskjell fra eksempelvis engelske vannselskaper. Statlig kontroll for å påse at eventuelle private eiere ivaretar kvalitet, sikkerhet og langsiktighet, vil betinge oppbygging av et stort statlig kontrollorgan, og det er usikkert om det i det hele tatt er mulig å regulere disse aspektene godt nok i en desentralisert og lite homogen bransje med store variasjoner i naturgitte rammebetingelser.
- Dagens fornyelsestakt på vann- og avløpsledningsnettet tilsier en levetid på om lag 200 år, men det er nødvendig med en raskere utskifting for å holde tritt med forfallsutviklingen. Dersom man får private monopoleiere, som alltid vil måtte veie investeringshensyn opp mot behovet for avkastning, vil det være regulatoriske utfordringer med hensyn til å pålegge et 100 års perspektiv på investeringene, jf. argumentasjonen over.
- Det er behov for kvalitetsforbedringer og økt sikkerhetsnivå innen VA-sektoren, og det er forventinger til at Mattilsynet vil påvirke til en positiv utvikling som ny tilsyns- og godkjenningsmyndighet for vannverk. Det vil derfor være nødvendig å øke brukerbetalingen for VA-tjenestene i mange kommuner i årene fremover. Med et offentlig eierskap, og forutsatt et fortsatt selvkostregime, vil abonnentene ha visshet om at prisøkningen går til kvalitetsforbedringer og sikkerhetstiltak.

Utvalget vil på denne bakgrunn anbefale at VA-virksomhetene skal være i offentlig eie. Det hersker noe usikkerhet med hensyn til om det kan komme overnasjonale føringer når det gjelder liberalisering av VA-tjenestene. Utvalget vil derfor anbefale at offentlig eierskap til VA-infrastrukturen blir regulert gjennom lov i Norge.

I Nederland ble det fra 2004 innført lovforbud mot at andre enn offentlige vannselskaper får produsere og distribuere drikkevann. I Sverige er det i skrivende stund til behandling i Riksdagen et forslag til ny svensk VA-lov, som blant annet regulerer offentlig eierskap. Det vil være hensiktsmessig å dra nytte av erfaringene fra Sverige og Nederland i arbeidet med å få på plass en norsk lovbestemmelse.

Det er viktig å presisere skillet mellom eierskap og drift. Forutsatt at man kan lykkes i å avtaleregulere tjenestekvalitet, sikkerhet og beredskap tilfredsstillende, vil det ikke være noe prinsipielt i veien for at konkurranseutsetting av driftsoppgaver fortsatt skal være tillatt.

[23] SINTEF-rapport 2005. *Brytningstider for vann- og avløpssektoren? Om konsekvenser for kommunene av en eventuell liberalisering.*

Det er også viktig å presisere at organisering i private andelslag, eid av abonnentene selv, fortsatt må være tillatt.

Utvalget er inneforstått med at anbefalingen vedrørende offentlig eierskap som virkemiddel i VA-sektoren er forskjellig fra utvalgets anbefalinger for nettselskapene i kraftsektoren, på tross av at de to sektorene har mye til felles, som for eksempel:

- Naturlige monopol kjennetegner begge virksomhetene.
- Begge bransjer er meget kapitalintensive – kostnadene er primært knyttet til investering i og forvaltning av kapitalvarer.
- De tekniske levetidene til primæranleggene er meget lange, typisk 30-50 år i kraftsektoren og 50-100 år for VA-ledningsanlegg.
- Begge nettvirksomheter står overfor en utfordring knyttet til aldring i infrastruktur – hvor vedlikehold og fornyelse er sentrale tema.

Det er imidlertid også viktige forhold som skiller de to sektorene:

- Kraftsektoren er omregulert med vertikalt skille mellom det sentrale overføringsnettet og produksjon og distribusjon. I VA-sektoren er produksjon, distribusjon og omsetning vertikalt integrert.
- Kraft produseres til et fritt marked, mens VA-tjenestene er naturlige monopoler. Årsaken til denne forskjellen er at det er mulig å overføre strøm over lange avstander, men det vil være umulig å gjøre det samme kostnadsmessig og kvalitetsmessig når det gjelder vann. Det betyr i praksis at der er konkurranse om sluttbrukerne i el-markedet, mens sluttbrukerne av VA-tjenester er uløselig knyttet til den lokale vann- og avløpsvirksomheten.
- Det er nødvendig med en lengre investeringshorisont for VA enn for kraft, da kostnadene per meter distribusjonssystem er mye høyere.
- VA-sektoren har et særskilt kvalitetsaspekt knyttet til rensing av drikkevann og avløpsvann, der behovet vil variere fra sted til sted avhengig av lokale forhold.
- VA-sektoren består av atskillig flere enheter enn kraftsektoren, hvorav en rekke små, som ville gi særskilte utfordringer i en deregulert modell.

10.4.3.2 Regulatoriske virkemidler

VA-sektoren skiller seg fra de andre kritiske infrastruktursektorene i den henseende at myndighetsansvaret og lovreguleringen er fordelt på en rekke departementer, blant annet Miljøverndepartementet, Helse- og omsorgsdepartementet, Landbruks- og matdepartementet, Kommunal- og regionaldepartementet, Olje- og energidepartementet og Justis- og politidepartementet. Ingen av departementene har et helhetlig eller koordinerende sektoransvar, og som følge av myndighetsorganiseringen er bransjen underlagt et fragmentert lov- og forskriftsverk.

I forbindelse med etableringen av det statlige Mattilsynet 1. januar 2004 ble ansvaret for godkjenning av vannverk og tilsyn med vannforsyningen overført fra kommunene til Mattilsynet, derunder også tilsynet med vannverksberedskapen. Kommunene har imidlertid fortsatt et visst tilsynsansvar etter drikkevannsforskriften. Det utøvende myndighetsansvaret for avløpsanlegg er delt mellom fylkesmannen og kommunene.

Når det gjelder gjennomføring av analyser av vann, avløp og slam, har dette i stor grad blitt overlatt til det private laboratoriemarkedet etter opprettelsen av det statlige Mattilsynet. Tidligere ble slike analyser vanligvis gjennomført av kommunalt eide laboratorier tilknyttet det lokale næringsmiddeltilsynet.

Vurderinger og anbefalinger – myndighetsoppfølging og -koordinering

Den fragmenterte myndighets- og regelverksstrukturen på vann- og avløpsfeltet gir utfordringer når man skal vurdere hvorvidt sikkerhets- og beredskapsaspektet er godt nok ivaretatt i de regulatoriske rammebetingelsene. Den fragmenterte styringen av vannsektoren var bakgrunnen for ett av tiltakene som ble foreslått i handlingsplan for oppfølging av utredningen «Sårbarhet i vannforsyningen»:

> Det foreslås vurdert opprettet en nasjonal samordningsgruppe for vannforsyningen som kan bidra til en helhetlig styring av vannforsyningen. Erfaringen med en slik sentral samordningsgruppe i Sverige er gode. Før det eventuelt besluttes å opprette en slik gruppe, bør det vurderes å se nærmere på de erfaringene som er gjort i Sverige. Mandatet for en sentral samordningsgruppe bør blant annet være å se på behovet for samordning av regelverk og ansvar, samt koordinering og samordning av tilsyn.

Utvalget anbefaler på denne bakgrunn at det etableres en samordningsgruppe for vannsektoren, med en representativ sammensetning, med tilstrekkelige ressurser og med mandat til blant annet å samordne arbeidet med regelverk og til-

syn, gjennomføre risikovurderinger, vurdere sikkerhetsnivå og kartlegge behovet for nødvendige tiltak.

Utvalget anser det ikke nødvendig å etablere en egen samordningsgruppe på avløpsområdet.

Sårbarhetsutvalget foreslo at det måtte settes større kraft bak arbeidet for å sikre at kravene i drikkevannsforskriften blir oppfylt, og betydningen av gode beredskapsplaner ble understreket. Kommunens dobbeltrolle som vannverkseier og myndighet innen drikkevann ble pekt på som prinsipielt betenkelig. Dette ble løst da Mattilsynet overtok som tilsyns- og godkjenningsmyndighet for vannverkene 1. januar 2004, og det var forventet at den nye statlige drikkevannsmyndigheten ville sørge for at kvalitet og sikkerhet ved vannforsyningen ble bedre ivaretatt. Drikkevann har imidlertid ikke vært prioritert høyt nok fra det nye Mattilsynets side disse første to årene til at man kan se noen umiddelbar effekt av myndighetsoverføringen.

I etterkant av utredningsarbeidet «Sårbarhet i vannforsyningen» ble det utarbeidet forslag til en handlingsplan for en sikrere vannforsyning i Norge. Mattilsynet ble pekt på som ansvarlig myndighet for nærmere vurdering og oppfølging av en rekke tiltak. Blant annet ble det pekt på behovet for en svartjeneste som umiddelbart kan bistå det enkelte vannverk dersom det skulle oppstå mistanke om forurensning av drikkevannet, for eksempel i form av en telefontrussel. Videre ble det pekt på behovet for å sikre et visst analysetilbud for biologiske og kjemiske agens i vann, som ikke tilbys av det ordinære laboratoriemarkedet.

Utvalget mener at Mattilsynet må trappe opp sitt arbeid som tilsyns- og godkjenningsmyndighet innen vannforsyning, for å sikre etterlevelse av kvalitets- og sikkerhetskrav. Mattilsynet må også sørge for en snarlig oppfølging av prioriterte tiltak i handlingsplanen for en sikrere vannforsyning.

Utviklingen i laboratoriemarkedet den senere tiden tyder på at det skjer en omstrukturering og sentralisering som følge av priskonkurranse, som gjør at det er grunn til å frykte at de beredskapsmessige aspektene ikke blir godt nok ivaretatt. Dette vil kunne ha konsekvenser i forhold til lokal kapasitet og kompetanse ved blant annet mistanke eller trusler om forurenset drikkevann. I høringsnotat om fremtidig organisering av laboratorietjenester på matområdet var det foreslått ulike virkemidler som staten kunne gå inn med dersom beredskapsmessige hensyn ikke ble godt nok ivaretatt i et fristilt laboratoriemarked[24].

Utvalget mener det er viktig at Mattilsynet følger nøye med på utviklingen på laboratorieområdet og går inn med statlige virkemidler dersom de beredskapsmessige hensyn innen vannforsyningssektoren ikke blir godt nok ivaretatt i et fullt ut konkurranseeksponert marked.

Vurderinger og anbefalinger – VA-organisering og kompetanse

Fundamentet for en sikker VA-tjeneste ligger i de personellressurser den enkelte VA-virksomhet disponerer. Det er av avgjørende betydning at det finnes tilfredsstillende kompetanse og tilstrekkelige personellressurser under drift og i beredskapssituasjoner. Samtidig viser undersøkelser at man risikerer å få en halvering av antall personer med relevant VA-faglig bakgrunn innen 2020, dersom man ikke lykkes med å opprettholde utdanningstilbudene og få en kraftig økning i antall studenter som uteksamineres. Sårbarhetsutvalget pekte særlig på de utfordringer mindre vannverk kan ha med ressurser og kompetanse og anbefalte at aktuelle fagmyndigheter vurderte forslaget om større grad av interkommunalt samarbeid.

Utvalget mener at det bør gjennomføres en utredning om aktuelle incitamenter for å stimulere til mer robuste enheter innen VA-sektoren, herunder tiltak for å sikre nødvendig kompetanse. Utvalget foreslår at det som del av utredningen vurderes behovet for en veiledende bransjestandard for kompetanse- og bemanningsbehov i VA-sektoren. Det er også viktig å følge med på rekrutteringssituasjonen og løpende vurdere behovet for tiltak.

Vurderinger og anbefalinger – Beredskapsevne

Kriser i vannforsyningssektoren vil av natur normalt ha lokale virkninger og må håndteres av lokal kriseledelse i kommuner, vannverk og Mattilsyn, eventuelt i samarbeid med andre aktører som politi, sivilforsvar og fylkesmann avhengig av krisens karakter og omfang. I og med at det normalt vil gå mange år mellom hver gang et vannverk vil oppleve en reell krisesituasjon, vil det være en fordel om man lokalt kan få støtte fra personell med erfaring fra tilsvarende kriser. I Sverige har man opprettet en sentral krisestøtteenhet på initiativ fra Livsmedelsverket. Enheten består av et begrenset antall personer som til daglig arbeider ved vannverk, men som rykker ut når andre vannverk har behov for støtte og ekstern kompetanse i en krisesituasjon.

[24] Høringsnotat om framtidig organisering av laboratorietjenestene på matområdet mv. Fiskeridepartementet, Helsedepartementet og Landbruksdepartementet februar 2003.

Utvalget mener at en tilsvarende krisestøtteenhet vil være vel så nyttig å få etablert i Norge, der gjennomsnittsstørrelsen på en vannverksorganisasjon er mindre enn i Sverige og kapasiteten til å håndtere kriser tilsvarende vil være mindre.

Det har vært lite fokus på risiko og sårbarhet og behovet for beredskap innen avløpssektoren. Noen avløpsverk/kommuner har utarbeidet egne beredskapsplaner for avløp, men det vanligste er at slike situasjoner er ment å skulle håndteres innenfor den kommunale beredskapsplanen.

Utvalget mener at det bør gjøres en kartlegging av beredskapsevne og -behov innen avløpssektoren for å se om dagens håndtering er tilfredsstillende, eller om det er behov for å styrke innsatsen.

10.4.3.3 Økonomiske virkemidler

Offentlig eide VA-verk finansierer sin virksomhet gjennom kommunale gebyrer, med hjemmel i lov om kommunale vass- og kloakkavgifter. Vann- og avløpsgebyrene skal ikke overstige kommunenes nødvendige kostnader på henholdsvis vann- og avløpssektoren (selvkostprinsippet). Det har den senere tid vært en viss diskusjon om det bør være anledning for eiere av VA-anlegg til å ta ut avkastning, jf. blant annet KOU 2005:1 Egne inntekter for kommunene.

I og med at VA-virksomhetene er naturlige monopoler med mangel på konkurranse, vil en avvikling av selvkostprinsippet betinge en form for statlig inntektsrammeregulering, for å ivareta abonnentenes rettigheter. ECON har utredet mulighetene for inntektsrammestyring på oppdrag for KS og konkludert med at:

> Det er ikke mulig å nå mål om effektivitet, kvalitet og riktige incentiver til investeringer samtidig ved en enkel reguleringsmodell. Regulering av VA-sektoren i Norge kan bli mer krevende enn regulering av nettsektoren, fordi VA-sektoren består av en rekke små aktører som til dels har svært ulike rammebetingelser for sin virksomhet.[25]

Som del av debatten om liberalisering av VA-tjenester og valg av inntektsregime, virker det å være enighet i de fleste europeiske land om behovet for effektivisering og modernisering av VA-sektoren. I St.prp. nr. 64 (2003-2004) Om lokaldemokrati, velferd og økonomi i kommunesektoren 2005 foreslås flere tiltak for å effektivisere sektoren, herunder utvikle et nasjonalt informasjonssystem for sammenlikning av virksomheter (benchmarking). NORVAR har gjennom flere år arbeidet med utvikling av et benchmarkingssystem for VA-sektoren, og erfaringene er at det er vanskelig å få til en reell sammenlikning mellom virksomheter, men at systemet gir et godt grunnlag for «benchlearning» for den enkelte VA-virksomhet med hensyn til å lære av egne og andres erfaringer. Kommunal- og regionaldepartementet har i skrivende stund til vurdering forslag til alternative modeller for benchmarking innen VA-sektoren.

Vurderinger og anbefalinger

Den forfallsutvikling man ser på VA-ledningsnettet i mange kommuner vil i lang tid fremover betinge økte investeringsbudsjetter for å kunne ivareta sikkerhet og kvalitet på VA-tjenestene på både kort og lang sikt. Utvalget mener at et fokus på effektivisering av VA-tjenestene, herunder benchmarking, kan bidra positivt, ved at det kan frigjøre ressurser som kan brukes til å redusere aldringstendensene i VA-infrastrukturen.

Utvalget vil imidlertid advare mot at man forlater dagens selvkostregime for VA-sektoren til fordel for en inntektsrammestyring, uten en grundig vurdering av hvilke konsekvenser det kan få for den langsiktige sikkerheten ved VA-tjenestene. Hvis man forlater selvkostprinsippet vil man raskt komme opp i dilemmaet mellom kvalitets- og sikkerhetsforbedringer versus avkastning. Det er dessuten ikke sannsynliggjort at det er mulig å utvikle en egnet statlig reguleringsmodell som kan gjenspeile den diversitet og de ulike naturgitte rammebetingelser som vann- og avløpsvirksomhetene er prisgitt[26].

10.5 Olje og gass

Olje- og gassvirksomheten har hatt og har svært mye å si for den økonomiske veksten i Norge og finansieringen av det norske velferdssamfunnet. Gjennom mer enn 30 års virksomhet har næringen skapt verdier for godt over 4000 milliarder kroner, målt i pengeverdien i dag[27]. Sektoren bidro med 21 prosent av Norges BNP i 2004.

Ettersom norsk økonomi i stor grad påvirkes direkte av svikt eller bortfall i vår produksjons- og forsyningskapasitet knyttet til olje og gass, har Norge en sterk økonomisk interesse av at produksjon og leveranse av olje og gass kan opprettholdes under alle former for påkjenninger. Bortfall av pro-

[25] ECON-rapport nr. 2004-005. Konsekvenser av ny regulering i VA-sektoren i kommunene

[26] ECON-rapport 2004-005. *Konsekvenser av ny regulering i VA-sektoren i kommunene*.

[27] Fakta Olje- og energidepartementet og Oljedirektoratet 2005. *Norsk petroleumsverksemd.*

duksjonskapasitet betyr likevel ikke at verdiene blir borte. Råvarene blir liggende til produksjonskapasiteten er tilbake. Olje og gass er også strategiske råvarer. Et bortfall vil få store konsekvenser for blant annet samfunnets evne til å transportere personer og gods. Den økende bruken av gass innenlands er med på å understreke betydningen av gass som en strategisk råvare, også i Norge. Dette bildet nyanseres noe ved at oljeproduksjon i stor grad kan reguleres gjennom internasjonalt samarbeid, og bortfall ett sted vil søkes kompensert med internasjonale reguleringer. Olje- og gassindustrien fremstår også som sterke symboler på økonomisk makt, noe som bidrar til å gjøre industriens installasjoner til potensielle mål.

Andre land er i stadig større grad avhengig av selve olje- og gassproduktene for sin industri og sine husholdninger. I ytterste konsekvens kan vår nasjonale handlefrihet bli utfordret i forholdet til andre stater som er kritisk avhengige av norsk leveranse. Dette gjelder spesielt innenfor gassforsyningen, som har landingspunkter i Tyskland, Belgia, Frankrike og Storbritannia. Norge dekker om lag 14 % av gassforbruket i Europa, og er således den neste største gasseksportør til Europa og for øvrig den tredje største gasseksportør på verdensbasis. Storbritannia vil om kort tid få dekket om lag 20 % av landets gassbehov gjennom norske leveranser.[28]

Med Norges plass blant verdens største olje- og gassprodusenter vil verdensøkonomien ikke være upåvirket av en eventuell katastrofal hendelse som kan forstyrre eller sette ut av spill deler av virksomheten på norsk sokkel. Dette legger et særlig ansvar på norske myndigheter i forhold til å ta sikkerhet på alvor i denne sektoren. Ved omfattende svikt i olje- og gassproduksjon vil konsekvensene på kort sikt bli meget alvorlige. Om konsekvensene på lengre sikt vil være like alvorlige avhenger blant annet av i hvilken grad samfunnet er i stand til å beskytte infrastrukturen med synlige sikringstiltak. Slike sikringstiltak vil være nødvendige hvis virksomheten skal kunne drives videre ved et vedvarende økt trusselnivå.

Man står nå foran en vesentlig endring i produksjonsvirksomheten ved overgangen til drifts- og kontrollsystemer som styres fra land, såkalt e-drift. Dette gjør at virksomheten utsettes for nye IT-relaterte trusler på lik linje med annen kritisk infrastruktur som er avhengig av elektronisk kommunikasjon for å fungere. Karakteren av et tett koblet system blir på denne måten enda mer fremtredende.

[28] Opplyst av Statoil til utvalget, februar 2006.

10.5.1 Overordnet beskrivelse av infrastruktur og samfunnsfunksjon

Olje- og gassvirksomheten er basert på en komplisert infrastruktur bestående av faste og flytende produksjonsinnretninger, flyttbare boreinnretninger, undervannsinstallasjoner, rørtransportsystemer, mottaks- og prosessanlegg, raffinerier, kontrollsentraler, forsyningsbaser, lagre, forsyningsfartøy, helikoptre og helikopterterminaler.

Petroleumsvirksomheten omfatter 29 operatørselskap, 72 felt, hvorav 50 felt i produksjon, 125 faste plattformer, 239 faste undervannsinstallasjoner, 55 registrerte flyttbare innretninger, 22 rørtransportsystemer og 8 landanlegg.[29] Det er i dag 9 operatører som opererer infrastrukturen. I alt sysselsetter næringen om lag 76 000 personer. Hydro og Statoil har nærmere 53 % av operatørskapene på norsk kontinentalsokkel.[30]

10.5.2 Beskrivelse av eierforhold og organisering

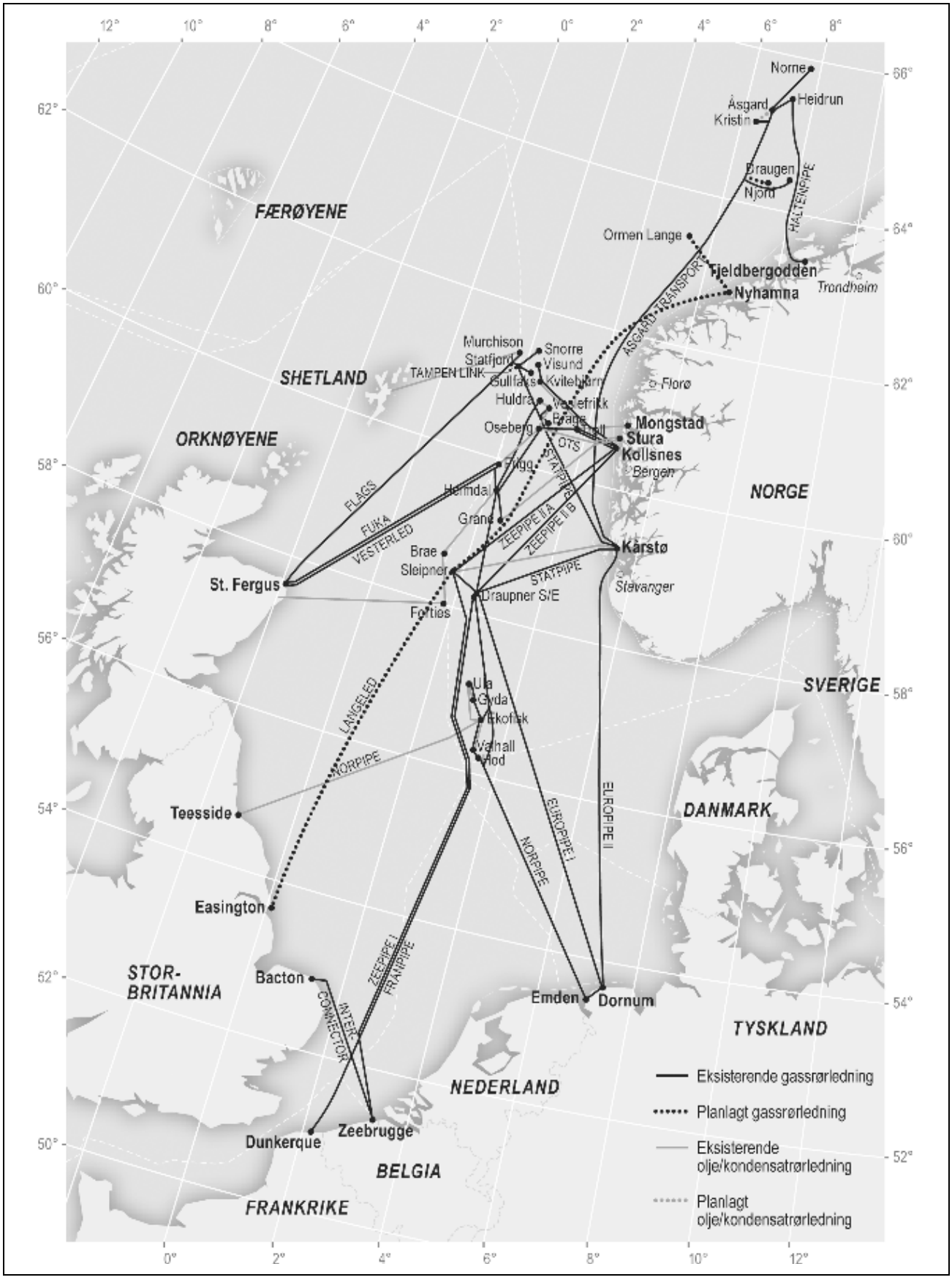
10.5.2.1 Produksjon og omsetning

Da petroleumsepoken startet for Norge valgte myndighetene i starten en modell med utenlandske selskap til å drive denne virksomheten. I dag er det både nasjonale og internasjonale selskaper som står for produksjon og omsetning på den norske kontinentalsokkelen. Det kan også nevnes at største helikopteroperatør og flere rederier i forsyningsvirksomheten er utenlandsregistrerte foretak.[31]

Statoil ble dannet i 1972, og har siden vært en sentral offentlig aktør i norsk petroleumsvirksomhet. Statoil eier både oljeinstallasjoner og deler av infrastrukturen for gasstransport. Selskapet har også vært operatør for store deler av gasstransportsystemet. Det overordnede målet med organiseringen og eierskapet var å sikre en samfunnsøkonomisk effektiv utbygging av de norske petroleumsressursene og sikre at en størst mulig andel av grunnrenten i sektoren tilfaller det norske samfunnet. I tillegg var det en rekke andre politiske mål knyttet til blant annet næringsutvikling og lokaliseringen av petroleumsvirksomheten på land. Statoil var et viktig instrument også i disse sammenhengene.

Samfunnsøkonomisk ligner deler av petroleumsinfrastrukturen på andre infrastrukturer som elektrisitetsnettet. Det gjelder særlig infrastruktu-

[29] Oljedirektoratets database, søk utført 17. februar 2006.
[30] St.meld. nr. 38 (2003-2004). *Om petroleumsvirksomheten*; Oljedirektoratets database, søk utført 17. februar 2006.
[31] Opplyst av Statoil, februar 2006.



Figur 10.6 Eksisterende og planlagte rørledninger.

Kilde: Oljedirektoratet.

ren for transport av gass, som kan betegnes som et naturlig monopol. Det har derfor ikke vært samfunnsøkonomisk ønskelig å etablere parallelle infrastrukturer for gasstransport. I motsetning til for eksempel kraftsektoren har imidlertid eierskapet til gassinfrastrukturen ligget hos oppstrømsaktørene (produsentene av gassen) separat. Den tradisjonelle modellen for driften av systemet var at en av eierne av hvert enkelt gassrørledningsnett hadde operatøransvar.

Eierskapet til størstedelen av gasstransportsystemet ble senere overført til et nytt interessentskap, Gassled, hvor de tidligere eierne av gassinfrastrukturen er representert som eiere (med enkelte unntak). Kapasiteten i Gassled disponeres av det statseide Gassco, en uavhengig operatør som ble etablert i 2001. Gassco tildeler også kapasiteten i transportsystemet til skipere av gass i henhold til definerte regler, og opererer også et annenhåndsmarked for transportkapasitet.

Statoil er operatør for 60 % av den norske olje- og gassproduksjonen. Staten har en eierandel på om lag 71 % i Statoil. Det nest største operatørselskapet er Hydro som er operatør for om lag 30 % av olje- og gassproduksjonen. Statens eierandel er på om lag 44 % i Hydro.

10.5.2.2 Transmisjon

Gassco er operatør for størstedelen av transportsystemet og behandlingsanleggende for gass. Rørledningene og anleggene er etablert i en samlet eierstruktur (Gassled), med Gassco som operatør. Staten er eneeier av Gassco. Etter opprettelsen av Gassled i 2002, ble en ny arbeidsprosess etablert for infrastrukturutvikling med etablering av en årlig 10 års transportplan. Alle ressurseiere, eiere av infrastrukturen og myndighetene er involvert.

Gassco er ansvarlig for å samordne videreutviklingen av gasstransportsystemet, i tillegg til å selv vurdere behovet for videreutvikling. Målet er at Norge skal ha et integrert og veldrevet system til beste for utnyttelsen av olje og gass også i framtiden.

10.5.3 Nye bruksområder for gass i Norge

Norge har tradisjonelt eksportert det meste av gassproduksjonen utenlands. Konsekvensene av bortfall av gass har derfor frem til nå hovedsakelig vært av økonomisk karakter. Innenlands bruk av gass er i ferd med å øke, og med det endrer også konsekvensene av bortfall seg. I Rogaland ble gassnett tatt i bruk i mars 2004 som kraftkilde til blant annet gartnerier, meierier og forprodusenter. Gasskraftverk ved Kårstø er i ferd med å bli realisert, og planer foreligger for bygging av andre gasskraftverk. Det foreligger også planer om en gassledning fra Rogalandsregionen til Grenland som kraftkilde til industrien. Videre foreligger det planer om å forsyne industri i Østfold med gass. Denne gassen vil bli skipet inn og lagret og videredistribuert i Østfold.

Ved økt bruk av gass i Norge vil leveringssikkerheten være et kritisk punkt. Etter som mottager-/brukergrupper vokser, vil avhengigheten til en viss grad kunne sammenlignes med tradisjonell strømforsyning, med de sårbarhetsperspektiver det medfører.

10.5.4 Utvalgets vurderinger og anbefalinger knyttet til virkemidlene

10.5.4.1 Eierskap som virkemiddel

Staten har et betydelig eiermessig engasjement i norsk petroleumsvirksomhet gjennom Statens direkte økonomiske engasjement (SDØE), som eier av statsaksjeselskapene Petoro og Gassco, som majoritetseier av Statoil og som minoritetseier i Norsk Hydro. Olje- og energidepartementet er ansvarlig eierdepartement for SDØE, Petoro, Gassco og Statoil. Nærings- og handelsdepartementet er ansvarlig eierdepartement for Norsk Hydro.[32]

Det overordnede målet med organiseringen og eierskapet var å sikre en samfunnsøkonomisk effektiv utbygging av de norske petroleumsressursene og sikre at en størst mulig andel av grunnrenten i sektoren tilfaller det norske samfunnet. I tillegg var det en rekke andre politiske mål knyttet til blant annet næringsutvikling og lokaliseringen av petroleumsvirksomheten på land.

Behovet for, og kontroll med sikring av den kritiske infrastrukturen i denne sektoren ser ikke ut til å ha vært en særskilt begrunnelse for offentlig eierskap.

Vurderinger og anbefalinger

En betydelig del av petroleumsvirksomheten på den norske kontinentalsokkelen skjer i regi av aktører med privat og/eller utenlandsk eierskap. Det er derfor uansett behov for et effektivt sikkerhetsregelverk med tilstrekkelige sanksjonsmuligheter. En rekke slike virkemidler er tilgjengelige i dagens lovverk og forskrifter. Offentlig eierskap er i beste fall et partielt virkemiddel for å ivareta sik-

[32] St.meld. nr. 38 (2003-2004) *Om petroleumsvirksomheten.*

kerhetshensyn, og vil være mindre viktig som virkemiddel dersom det generelle sikkerhetsregelverket og håndhevingen av det fungerer godt nok.

10.5.4.2 Regulatoriske virkemidler

Olje- og energidepartementet har som overordnet sektormyndighet ansvar for sikrings- og beredskapsarbeidet. Petroleumsloven med tilhørende forskrifter er det sentrale styringsverktøyet. For eksempel inneholder petroleumsloven bestemmelser om levering til nasjonalt behov og levering i tilfelle krig, krigsfare eller andre ekstraordinære situasjoner. Den norske staten kan med hjemmel i disse bestemmelsene pålegge rettighetshavere å levere petroleum til utvalgte mottakere innenlands til dekning av nasjonalt behov (mot vederlag beregnet etter bestemte regler). I tilfelle krig og lignende situasjoner kan rettighetshavere pålegges å stille petroleum til disposisjon for norske myndigheter.

1. januar 2004 ble Oljedirektoratet delt i to nye selvstendige enheter, Oljedirektoratet og Petroleumstilsynet. Oljedirektoratet hører administrativt inn under Olje- og energidepartementet, mens Petroleumstilsynet hører administrativt inn under Arbeids- og sosialdepartementet. Etter St.meld. nr. 17 (2002-2003) om statlige tilsyn, ble Petroleumstilsynet etablert 1. januar 2004. Petroleumstilsynet har ansvaret for sikkerhet, beredskap og arbeidsmiljø i petroleumssektoren.

Når det gjelder ansvar for sikring av den kritiske infrastruktur innenfor petroleumsvirksomheten ligger dette først og fremst hos eieren av infrastrukturen. Rettighetshavere på norsk kontinentalsokkel har plikt til å iverksette og opprettholde sikringstiltak, plikt til å ha beredskapsplaner for bevisste anslag og plikt til å stille innretningen til disposisjon for øvelser og til å delta i slike øvelser.[33] Plikten til beredskapsplanlegging omfatter også plikt til å planlegge tiltak som skal iverksettes for å bidra til å hindre drifts- og leveranseavbrudd. Operatørene har dessuten plikt til å overvåke all sikkerhetstruende aktivitet i havområdene rundt installasjoner og objekter. Overvåkningen skjer fra selve innretningene eller beredskapsfartøyer ved hjelp av radarsystemer. Ved et villet angrep mot en innretning, er det politiet, med støtte fra Forsvaret (Forsvarets jagerfly, Forsvarets spesialkommando, mv.) som responderer. I petroleumsregelverket er det gitt ytterligere bestemmelser om tiltak for å forebygge og motvirke ulovlige aktiviteter mot olje- og gassinnretninger.

Vurderinger og anbefalinger

Petroleumsloven fastslår at den norske stat har eiendomsrett til undersjøiske petroleumsforekomster og eksklusiv rett til ressursforvaltning. Loven har også bestemmelser om særskilte krav til sikkerhet, inkludert krav om beredskap mot bevisste anslag. Rettighetshaverne skal iverksette og opprettholde sikringstiltak for å bidra til å hindre bevisste anslag, og de skal ha beredskapsplaner for slike anslag.

Utvalget mener at de regulatoriske virkemidlene som er tatt i bruk er gode bidrag også i forhold til å ivareta de sikkerhetshensyn og nasjonale interesser som skal vurderes i denne sammenheng. Utvalget mener imidlertid at det er behov for å vurdere tilsynsvirksomheten på området for å avklare gråsoner.

Ved etableringen av Petroleumstilsynet (Ptil) i 2004 ble syv (nå åtte) petroleumsrelaterte anlegg på land overført fra forvaltningsområdet til Direktoratet for samfunnssikkerhet og beredskap og over til Petroleumstilsynet. Begrunnelsen var at petroleumsindustrien til havs og på land skulle underlegges et ensartet regelverks- og tilsynsregime.

I forkant av denne beslutningen ble det fra flere hold reist motforestillinger mot å underlegge de landbaserte anleggene et annet regelverks- og tilsynsregime enn det som ellers gjelder på land. Det ble pekt på at dette blant annet kunne ha sikkerhetsmessige implikasjoner. Erfaringene viser at det har oppstått uklare grenseflater mellom de berørte myndighetene, og det hevdes at industrien har problemer med å forholde seg til et sokkelrelatert regelverk i kombinasjon med det landbaserte. Det har også oppstått uklarhet om tilsyns- og regelverksregimene for nye landbaserte anlegg for håndtering av petroleum, eksempelvis nye gasskraftverk. Utvalget anser denne situasjon som uheldig, og mener at det er viktig at de berørte departementer avklarer ansvarsområdene i forhold til landbasert virksomhet som håndterer olje og gass.

Også innenfor denne sektoren vil utvalget understreke at virkemiddelsettet i forhold til informasjonssikkerhet, personellsikkerhet og objektsikkerhet som sikkerhetsloven gir, bør anvendes i større utstrekning enn hva som er tilfelle. Det er også i samsvar med synspunkter utvalget har mottatt i dialog med operatørselskaper.

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

10.5.4.3 Økonomiske virkemidler

Det kan i oppstå en konflikt mellom sikkerhetshensyn og ønsket om lavest mulige kostnader og maksimalt overskudd fra petroleumsvirksomheten. Petroleumstilsynet har likevel argumentert for at HMS-regelverket for flyttbare boreinnretninger, som har vært viet særlig oppmerksomhet, ikke er fordyrende sammenlignet med regelverket i andre land.

I et bedriftsøkonomisk perspektiv er det også klare incentiver til å gjennomføre sikkerhetstiltak som reduserer eller fjerner den mulige konflikten mellom sikkerhet og lønnsomhet. Manglende ivaretakelse av sikkerhetshensyn skaper en risiko for stans i produksjonen, som i sin tur kan gi betydelige inntektstap. På sikt kan manglende ivaretakelse av sikkerheten fra en aktørs side føre til tap av troverdighet og reduserte muligheter til å investere i nye prosjekter på norsk sokkel.

Vurderinger og anbefalinger

Utvalget ser ikke behov for at staten skal gå inn med spesielle økonomiske virkemidler i forhold til å gjennomføre konkrete sikkerhetstiltak. Rettighetshaverne bør selv bekoste det som er nødvendig for å oppfylle kravene i lover og forskrifter.

10.6 Transport

Transportsektoren knytter samfunnet sammen, og hele samfunnets funksjonsdyktighet er avhengig av tilgjengelig transport. Dette i seg selv tilsier at transportinfrastrukturen er en kritisk infrastruktur. Analyser ved Forsvarets forskningsinstitutt (FFI) viser at mange alternative fremføringsveier gjør at transportsektoren samlet sett er robust. Erfaringene fra storflommen på Østlandet i 1995, der hovedferdselsårene mellom Østlandet og Trøndelag ble brutt i mange dager når det gjelder veg- og togforbindelse, viste at gods- og passasjertransport fant alternative kjøreruter. I følge FFI skal det mange samtidige terror- eller krigsanslag til for å svekke transportkapasiteten på nasjonalt eller regionalt nivå. Senere studier viser at det flere steder i landet er mindre redundans enn først antatt. Samferdselsdepartementets SAMROS-prosjekt har tatt utgangspunkt i kritiske punkter rundt i landet hvor bortfall vil medføre svært lange omkjøringer eller ikke omkjøringsmuligheter i det hele tatt. Som vist i kapittel 4 er transportinfrastrukturen også utsatt for terrorhandlinger ved at offentlig transport skiller seg ut som terrormål.

De mest dramatiske konsekvensene av bortfall vil først oppstå etter noe tid. Etter om lag en uke vil manglende tilgjengelighet til transporttjenester på nasjonalt eller regionalt nivå blant annet føre til svikt i helsevesenet, dagligvareforsyningen og drivstofforsyningen.

Selv om større hendelser innen transportsektoren ikke setter den ut av funksjon, vil store ulykker og terrorhendelser kunne svekke den nasjonale trygghetsfølelsen. Det vil kunne reises spørsmål ved myndighetenes legitimitet og evne til å forebygge og håndtere hendelser. Erfaringsmessig er transportsektoren også den av sektorene med kritisk infrastruktur som er mest utsatt for store ulykker og terrorhandlinger.

Just-in-time prinsippet er med på å øke samfunnets avhengighet av sikre og forutsigbare transporttjenester. Eksempelvis har de store matvarekjedene sentralisert sine lagre og logistikksentre de siste årene. I tillegg er store deler av matvarelagrene til enhver tid på hjul. Med lengre transportakser, blir matvareleveransene i enda sterkere grad avhengig av en fungerende transportinfrastruktur. Økende handel mellom land bidrar også til økt avhengighet av en fungerende transportinfrastruktur.

Trafikkstyring er kritisk for de ulike transportsystemenes funksjon. Både fly- og jernbanetrafikken er helt avhengige av sentral trafikkstyring. Forstyrrelser i trafikkstyringen ved driftssentralene får umiddelbare konsekvenser for trafikkflyten, og systemene sett under ett bærer preg av å være tett koblet. Vegtrafikk og skipstrafikk er ikke like kritisk avhengig av trafikkstyring.

10.6.1 Overordnet beskrivelse av infrastruktur og samfunnsfunksjon

Transportsektoren kan deles i fire undersystemer; luftfart, sjøtrafikk, vegtrafikk og trafikk på bane. Systemene utfyller hverandre, og det er til en viss grad erstatningsmuligheter dem imellom.

Utviklingen i transportsektoren henger sammen med den økonomiske utviklingen. Økt økonomisk vekst har gitt behov for økt person- og godstransport. Dette får betydning for transportert varemengde og folks jobb- og fritidsreiser. Biltransport står for rundt 70 % av antall reiser og 60 % persontransportarbeidet.

De viktigste delene av vegnettet er riksveger og fylkesveger. Stamvegnettet omfatter de vegrutene som binder landet sammen og som derfor har særlig betydning for transporter mellom landsdeler og utlandet. Lengden på stamvegnettet er om

lag 8 600 km.[34] Dette er om lag en tredel av det totale riksvegnettet.

Maritim infrastruktur omfatter i hovedsak havner, farleder og navigasjonsinstallasjoner. Hovedled og biled er statens ansvar.

Kystverket opererer fire trafikksentraler, som driver overvåking av trafikken. De fire er lokalisert til Horten, Brevik, Kvitsøy og Fedje. I tillegg er det en trafikksentral under etablering i Vardø. Sentralene er etablert på bakgrunn av trafikktetthet eller transport av farlig gods.

Som ledd i arbeidet med forebyggende sjøsikkerhet og i oljevernberedskapssammenheng, driver Kystverket systemer for elektronisk navigasjon[35], elektroniske meldinger om transport av farlig/forurensende last og mottak av AIS-signaler[36] fra skip. Det er krav om at skip på 500 BT i innenriks skipsfart og passasjerskip uansett størrelse skal være utstyrt med AIS. AIS vil sende statisk og dynamisk fartøyinformasjon (identitet, type, posisjon, kurs, hastighet) og annen sikkerhetsrelatert informasjon (lasttype, bestemmelsessted, estimert ankomsttid).

Det er 57 havner med egen havneadministrasjon i Norge. Havnene styres av et havnestyre. Det er 10 havner som har status som nasjonale havner. Dette er Tromsø, Bodø, Trondheim, Ålesund, Bergen, Karmsund, Stavanger, Kristiansand, Grenland og Oslo. Staten oppnevner to representanter til havnestyrene i de nasjonale havnene, hvorav en representant oppnevnes fra Forsvaret og en fra Kystverket. Oslo er landets største havn for stykkgods og containere.

Avinor opererer tre flykontrollsentraler, i hhv. Bodø, Sola og Røyken. Fra 2007 er det besluttet at flykontrollsentralen i Røyken skal flyttes og oppgavene utføres fra Sola. Avinor driver 42 flyplasser og Forsvaret fire. Oslo lufthavn Gardermoen drives av et datterselskap til Avinor. Syv flyplasser har hovedandelen av flytrafikken – Gardermoen, Sola, Flesland, Værnes, Torp, Bodø, Tromsø.

Hovedelementene for jernbanetransport er jernbanenettet, det elektrotekniske anlegget (strømforsyning, signalanlegg og tele-/dataanlegg) og terminalene. Dagens jernbanenett er på i overkant av 4000 km, hvorav over halvparten er elektrifisert. Jernbanetrafikk er avhengig av sentral trafikkledelse gjennom togledersentraler. Jernbaneverket har åtte togledersentraler.

Det er veg- og sjøtransport som har de største volumene når det gjelder godstransport. I 2002 var godstransportarbeidet på 29 644 tonnkilometer. Av dette hadde sjøtransport en andel på 48 % (oljetransport fra sokkelen ikke inkludert) og vegtransport en andel på 46 %, jernbanen hadde en andel på 6 %. Luftfartens andel av godstransporten er marginal.

Logistikksentraler er helt sentrale når det gjelder effektiv vareflyt. Intermodale logistikksentraler er der hvor omlasting fra en transportform til en annen gjennomføres. Dette skjer typisk i forbindelse med havner, der det lastes over fra skip til veg- eller jernbanetransport.

Sentralt i arbeidet med ny nasjonal transportplan står utviklingen av nasjonale transportkorridorer mellom landsdeler og til utlandet. Det er viktig å knytte nettverkene for de ulike transportsystemene sammen.

10.6.2 Beskrivelse av eierforhold og organisering

I henhold til nasjonal transportplan skal staten årlig bevilge 19,25 milliarder kroner i rammebevilgninger til samferdselsformål. Staten er ansvarlig for utbygging og drift av den grunnleggende infrastrukturen innen alle de fire transportsystemene.

Når det gjelder infrastruktur for skipstrafikk, er Kystverket ansvarlig for utbygging og drift av viktig maritim infrastruktur. Fiskeri- og kystdepartementet (FKD) opplyser at fyr- og merketjenesten har en estimert gjenskaffelsesverdi på 3-4 milliarder kroner.

Kystverket får en årlig tildeling over statsbudsjettet på om lag 600 millioner kroner. I tillegg har Kystverket inntekter gjennom avgifter på 550 millioner fra gebyrer (for eksempel losgebyr, kystgebyr). Kystverkets produksjonsdel er privatisert (under navnet Secora). Utvikling og drift av havner og havneinfrastruktur er havneeiers ansvar. De viktigste havnene i Norge er hovedsakelig kommunalt eid. Noen store eksporthavner er i privat eie. Dette er typisk store bedrifters egne utskipingshavner/kaier.

Statens vegvesen/Vegdirektoratet har ansvaret for planlegging, bygging, drift og vedlikehold av riks- og fylkesvegnettet. Vegdirektoratet er et statlig forvaltningsorgan underlagt Samferdselsdepartementet. Årlig budsjett for Vegdirektoratet er på rundt 12 milliarder kroner, hvorav mesteparten går til investeringer. Statens vegvesens produksjonsdel er privatisert og skilt ut som eget selskap – Mesta. Etter privatiseringen av produksjonsdelen (Mesta), har ikke Vegdirektoratet noen egne

[34] St. meld. nr. 24 (2003-2004) *Nasjonal transportplan 2006-2015*.
[35] Differensiel GPS – DGPS
[36] AIS står for *Automatic Identification System*.

Figur 10.7 Nasjonale transportkorridorer.

Kilde: Nasjonal transportplan 2006-2015.

produksjonsressurser, men er avhengig av å kjøpe tjenester i markedet. Direktoratet har sørget for at det er en passus om beredskap i alle avtaler med leverandører av entrepenørtjenester slik at selskapene forplikter seg til å levere tjenestene også ved krisesituasjoner.

Avinor er et statlig aksjeselskap, 100 % eid av den norske staten ved Samferdselsdepartementet. Avinor eier og driver flyplasser og er ansvarlig for utøvelse av flysikringstjenester. Avinors virksomhet finansieres gjennom flyplass- og lufttrafikkavgifter samt kommersielle inntekter. Omsetning for Avinor var 5 075 millioner kroner i 2004. Staten kjøpte regionale lufthavntjenester av Avinor for om lag 300 millioner kroner i 2004. Oslo Lufthavn (OSL) er skilt ut som eget datterselskap til Avinor. Forsvaret stiller fire av sine flyplasser til disposisjon for sivil trafikk.

Jernbaneverket har ansvar for infrastruktur og trafikkstyring på det nasjonale jernbanenettet i Norge. Jernbaneverket er et statlig forvaltningsorgan underlagt Samferdselsdepartementet. Budsjett i 2004 var på 4 575 millioner kroner.

Staten har tilsyn som skal påse at sikkerhet innen transportsektorene blir ivaretatt. Statens jernbanetilsyn er et statlig tilsynsorgan med ansvar for å se til at trafikk på skinner (tog, t-bane og trikk) er trygg. Luftfartstilsynet fører tilsyn med sikkerheten i lufttrafikken. Sjøfartsdirektoratet er et statlig tilsynsorgan med ansvar for tilsyn med sikkerheten på norske skip samt havnestatskontroll. Vegdirektoratet har ansvar for å føre tilsyn med kjøre-

tøy og trafikanter. I tillegg har DSB ansvar for tilsyn med transport av farlig gods på land.

EU Kommisjonen ga i februar 2006 ut et forslag til forordning for beskyttelse av innlands godstransport mot terroristanslag og andre kriminelle handlinger. Forordningen er ment å omfatte hele verdi- og logistikkjeden, fra de som tilvirker det som skal transporteres, transportørene, speditørene, lagring og terminalhåndtering med mer.

Det skal være frivillig å implementere de tiltak som foreslås i forordningen. De som velger å tilslutte seg systemet vil bli såkalte «sikre transportører», noe som vil medføre enklere og raskere ekspedisjon ved for eksempel sikkerhetskontroller med mer. EU mener dette vil kunne bli et konkurransemessig fortrinn, som mange av de kommersielle aktørene vil benytte seg av. Det skal utpekes en myndighet i hvert land som skal koordinere og overvåke gjennomføringen av forordningen, som nå er overgitt til rådet og EU-parlamentet for videre behandling. Bruken av en slik ordning med «sikre» operatører eller underleverandører er allerede i dag et innarbeidet konsept innen deler av luftfarten.

10.6.3 Utvalgets vurderinger og anbefalinger

Tilgjengelige transportsystemer er vitalt for samfunnets normale drift. Det tilsier at det offentlige utøver stor grad av kontroll over infrastrukturen. Transportsektorens infrastruktur er videre til dels naturlige monopoler. Kostnadshensyn tilsier derfor at det i mange tilfeller ikke svarer seg å etablere konkurrerende infrastrukturer drevet etter markedsøkonomiske mekanismer. Distriktspolitiske og miljømessige hensyn er med på å understreke dette. Eksempelvis vil etablering og drift av dyre infrastrukturer i tynt befolkede områder kun svare seg samfunnsøkonomisk, ikke bedriftsøkonomisk. På samme måte kan etablering av nye og konkurrerende infrastrukturer bety så store inngrep i naturen at det er ønskelig å holde dette til et minimum.

I forhold til drift av infrastrukturen gjør trafikkompleksiteten det nødvendig med sentral styring og overvåkning fra driftsentraler. Dette gjør seg særlig gjeldende for jernbane og luft, men til dels også for sjø avhengig av trafikktettheten. I de større byene er trafikktettheten på veg så stor at driftstyring i økende grad er viktig for normal drift. Funksjonsdyktigheten til infrastrukturen er så avhengig av driftsstyring at det må sikres nasjonal kontroll gjennom offentlig eierskap. Videre er driftsentralfunksjoner i de ulike transportgrenene naturlige monopoler, og samlet tilsier dette at det offentlige i tillegg til å ha eierskapet, også opererer disse.

Når det gjelder utførelsen av nybygginger og vedlikehold av infrastrukturene ser utvalget ingen forhold av sikkerhets- og beredskapsmessig art som tilsier at det offentlige skal eie entreprenørselskapene. Utvalget ønsker likevel å peke på viktigheten av at de sikkerhets- og beredskapsmessige funksjonene ikke løsrives fra det ordinære driftsansvaret. God sikkerhet og beredskap oppnås kun ved at disse er integrert.

Luftfart

Infrastrukturen er her luftfartsnettet, og ansvaret for infrastrukturvirksomheten omfatter driftsvedlikeholds- og utbyggingsoppgaver av flyplasser og luftfartsnett og kontroll med flybevegelser i luftrommet for sivil luftfart. Disse oppgavene ivaretas av det offentlig eide selskapet Avinor. Selskapet har ingen kommersielle interesser når det gjelder trafikkvirksomheten. Det er vanskelig å se hva en ville vinne ved privatisering, siden det offentlige uansett måtte ha full innsynsrett og mulighet for pålegg om beredskaps og sikringsmessige tiltak. Vertikal separasjon og offentlig eierskap til infrastrukturfasilitetene er i tråd med drøftingen i kapittel 9, da det er vanskelig å se noen klare muligheter for synergigevinster av betydning ved integrasjon mellom infrastrukturvirksomheten og den kommersielle bruken av infrastrukturen. Integrasjon ville dessuten føre til problemer med å skille eierrollen og regulatørrollen.

Jernbanetrafikk

Forvaltning og drift av infrastrukturen er skilt ut og er delegert til den offentlige forvaltningsvirksomheten Jernbaneverket. Jernbaneverket driver ikke egen transportvirksomhet og det er vanskelig å innse hva en vil vinne ved privatisering. Kommersielle krav til inntjening kan gå på bekostning av sikkerhet.

Vegsektoren

Statens vegvesen har ansvaret for planlegging, bygging, drift og vedlikehold av riks- og fylkesvegnettet og har tilsyn med kjøretøy og trafikanter. Også her er det vertikal separasjon da forvaltningsvirksomheten ikke driver egen trafikkvirksomhet, og det synes liten grunn til å privatisere denne forvaltningsvirksomheten. Men det praktiseres konkurranseutsetting i stor skala når det gjelder vegbygging og vedlikehold.

Sjøtransport

Kystverket forvalter kystlinjen og har ansvaret for drift av fyrstasjoner, lykter, lanterner, faste og flytende merker langs kysten. Det har også ansvaret for statens beredskap mot akutt forurensning. Offentlige havner drives av egne kommunale selskaper med Kystverket som koordinerende nasjonal havnemyndighet. En har vertikal separasjon mellom havnefasiliteter og kommersiell bruk ved at verken kystverket eller de lokale havnevesen driver kommersiell sjøtransport. Sikring av terminaler og havneanlegg har vært et viktig tema i den senere tid. Sikringskravene – ISPS-kravene - kommer fra FNs sjøfartsorganisasjon IMO. Disse ble vedtatt på rekordtid etter terrorhendelsene 11. september 2001, og omfatter havner og anlegg med internasjonal trafikk. Kostnadene ved terrorsikring er det de enkelte havner som må bære. Innføringen av ISPS-kravene kan innebære en uforholdsmessig stor økonomisk belastning på den enkelte havn, noe som tilsier at utgiftene til oppfølging av disse kravene må kunne finansieres gjennom offentlig-privat samarbeid. Det vises i denne sammenheng til utvalgets forslag knyttet til innføring av en statlig tilskuddsordning, jf. kapittel 6.6.3.

Anbefalinger på tvers av transportgrenene

Utvalget vil understreke betydningen av å ha en helhetlig sikkerhetstilnærming ved valg av fremføringsvei og transportgren for transport av farlig gods. Ved valg av fremføringsvei og transportgren må samfunnet stille krav til at den sikreste og ikke den billigste fremføringsveien/transportgrenen blir valgt. Utvalget vil derfor anbefale at Samferdselsdepartementet, Nærings- og handelsdepartementet, Fiskeri- og kystdepartementet og Justis- og politidepartementet samarbeider om å tydeliggjøre behovet for å velge den sikreste fremføringsveien og transportgrenen til virksomheter som har behov av transport av farlig gods.

Kapittel 11
Kartlegging av kritiske samfunnsfunksjoner og sektorvise anbefalinger

En helhetlig tilnærming til beskyttelse av kritisk infrastruktur, omfatter også beskyttelse av kritiske samfunnsfunksjoner. I forlengelsen av kapittel 10, gis det derfor i dette kapittelet beskrivelser av enkelte kritiske samfunnsfunksjoner som dekker grunnleggende behov i samfunnet. I tillegg gis det anbefalinger. Det er gitt noe kortere beskrivelser av de samfunnskritiske funksjonene enn av de kritiske infrastrukturene. Utvalget har blant annet ikke foretatt dybdeanalyser av virkemiddelbruken innenfor de samfunnskritiske funksjonene. Det har ikke vært mulig innenfor utvalgets tids- og ressursrammer å vurdere Storting, Regjering, domstolene, forsvar, miljøovervåkning og renovasjon, men utvalget påpeker at disse er kritiske samfunnsfunksjoner.

11.1 Bank og finans

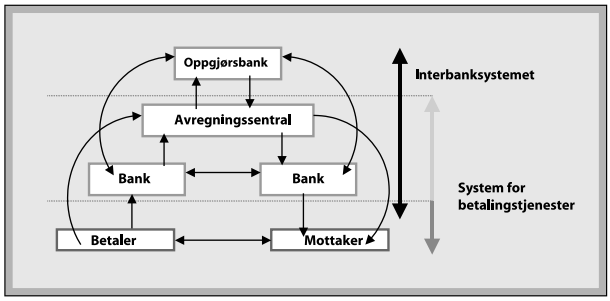
Et effektivt og robust betalingssystem og en velfungerende og stabil finansiell infrastruktur er av stor betydning for landets økonomi. Betalingssystemet og de underliggende infrastrukturene ivaretar næringslivets, publikums og offentlig forvaltnings behov for tilgang til et effektivt og sikkert system for betalingsformidling, og for overføringer og tilpasninger i finansielle fordringer og forpliktelser. Betalingssystemet og den finansielle infrastrukturen utgjør dermed en kritisk samfunnsfunksjon. Bankene og deres leverandører av elektronisk kommunikasjon-tjenester er sentrale aktører i betalingssystemet. Det er per 1. januar 2006 i alt 146 banker i Norge som deltar i interbanksystemene, herav 20 forretningsbanker og 126 sparebanker.[1] Blant forretningsbankene er det 7 filialer av utenlandske banker. Innskudd i bankene (kontopenger) benyttes som betalingsmidler ved siden av kontanter. Bankene er dessuten sentrale i å formidle oppsparte midler fra innskytere til låntakere. Hver dag utgjør overføringene mellom bankenes konti i Norges Bank i størrelsesordenen 150-200 milliarder kroner.

11.1.1 Beskrivelse av samfunnsfunksjonen

Betalingssystemet består av den kunderettede delen (systemet for betalingstjenester) og den delen som håndterer avregning og oppgjør mellom bankene (interbanksystemet). Disse systemene er teknisk og funksjonsmessig nært knyttet til hverandre. Strukturen i det norske betalingssystemet er illustrert i figur 11.1.

Systemer for betalingstjenester omfatter systemer som gjør det mulig å betale ved å belaste bankkonti, for eksempel ulike typer kort, girooverføringer og elektroniske penger (E-penger). Nettbankløsninger brukes i økende grad for å foreta betalingstransaksjoner, mens bruken av papirbaserte løsninger som brevgiro og sjekk har gått sterkt tilbake. Systemene for betalingstjenester behandler mange transaksjoner med relativt lav verdi per transaksjon. Hver dag behandles normalt 4-6 millioner slike transaksjoner med en samlet verdi på i størrelsesordenen 50 - 70 milliarder kroner.

Hvis betaler og betalingsmottaker har konto i samme bank, kan oppgjøret av betalingen utføres av denne banken ved at betalers konto belastes og betalingsmottakers konto godskrives. Hvis betaler og betalingsmottaker har konto i forskjellige banker, oppstår det et fordringsforhold mellom bankene som må gjøres opp i en oppgjørsbank. De



Figur 11.1 Det norske betalingssystemet.

Kilde: Norges Bank.

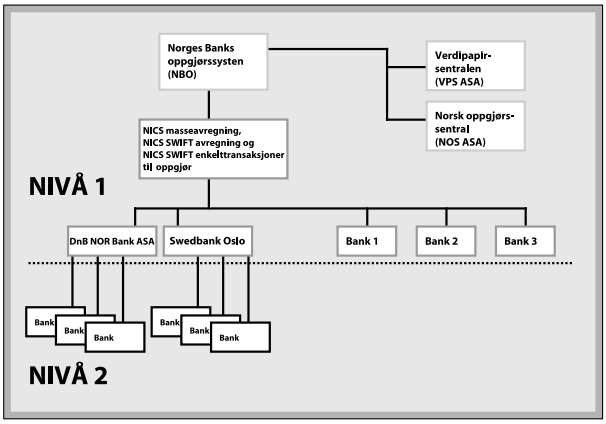
[1] Norges Bank 2004. *Årsrapport om betalingsformidling 2004,*

fleste betalingstransaksjoner mellom privatpersoner, bedrifter og offentlige virksomheter inngår i daglige avregninger mellom bankene og nettoposisjonene gjøres opp i en oppgjørsbank. Systemer for avregning og oppgjør mellom banker kalles interbanksystemer. Norges Bank er den øverste oppgjørsbanken i Norge, og betalingene mellom de største bankene gjøres opp der (24 banker). De fleste mindre bankene i Norge benytter DnB NOR Bank ASA som oppgjørsbank (107 banker), mens mange av bankene i SpareBank1-Gruppen benytter Swedbank Norge som sin oppgjørsbank (15 banker).

Oppgjør av fordringsforhold mellom bankene kan skje for hver enkelt betaling (bruttoppgjør) eller ved avregning av en rekke enkeltbetalinger (nettooppgjør). De største avregningene skjer i NICS[2] og utføres av Bankenes Betalingssentral (BBS) på oppdrag fra NICS Operatørkontor som representerer bankene. Det er to typer avregninger i NICS: Avregning to ganger daglig av betalinger som i hovedsak genereres i systemene for kunderelaterte betalingstjenester (NICS Masseavregning) og avregning tre ganger daglig av enkeltbetalinger mellom bankene på SWIFT-format[3] (SWIFT netto - transaksjoner på SWIFT-format inntil 25 millioner kroner per transaksjon). Resultatet av disse avregningene sendes til Norges Bank for oppgjør på bankenes konti i Norges Bank. De fleste bruttotransaksjonene som bankene sender til oppgjør i Norges Bank, formidles også via NICS (transaksjoner over 25 millioner kroner). Enkelttransaksjoner kan også sendes direkte fra bankene til Norges Bank.

Norges Bank er også oppgjørsbank for betalinger knyttet til handel med verdipapirer og derivater. Avregning for slike handler utføres av henholdsvis Verdipapirsentralen ASA (VPS) og Norsk Oppgjørssentral ASA (NOS). VPS er både et rettighetsregister for verdipapirer og en avregningssentral. Avregningene fra VPS og NOS oversendes til oppgjør i Norges Bank to ganger daglig.

VPS som rettighetsregister holder oversikt over hvem som eier aksjer (børsnoterte og ikke børsnoterte), rentebærende instrumenter utstedt av norske foretak i NOK og andeler i verdipapirfond. Hvis beholdninger av verdipapirer er benyttet som sikkerhet for for eksempel lån, er rettighetshaver registrert i tillegg til hvor stor andel av beholdningen som er pantsatt. I forbindelse med



Figur 11.2 Strukturen for avregning og oppgjør mellom bankene.

Kilde: Norges Bank

ulike utbetalinger fra utsteder til invester, forestår VPS beregning av utbetalingene og senter betalingsinstruksjoner direkte til BBS.

Forstyrrelser i betalingsformidlingen kan få umiddelbare og store konsekvenser for resten av økonomien. Det samme gjelder forstyrrelser knyttet til rettighetsregisteret for finansielle instrumenter. Det antas også at sikkerheten og robustheten i det finansielle systemet i Norge kan påvirke utenlandske aktørers tillit til norsk økonomi og det finansielle systemet i Norge. Det legges derfor stor vekt på at den finansielle infrastrukturen skal være robust, blant annet ved at aktørene har etablert reserveløsninger for drifts- og kommunikasjonsløsninger, herunder katastrofeberedskap, og at det generelt er stor oppmerksomhet om sikkerhet og beredskap i sektoren. Reserveløsninger og katastrofeberedskap testes periodisk, ofte i samarbeid mellom flere aktører. Dette er i tråd med Kredittilsynets IKT-forskrift der det blant annet stilles krav til etablering av reserveløsninger og gjennomføring av regelmessige, dokumenterte tester, jf. §§ 10 og 11. Dersom store deler av den finansielle infrastrukturen skulle settes ut av drift, vil det imidlertid være begrensete muligheter for å videreføre en tilnærmet normal betalingsformidling.

Den moderne finansielle infrastrukturen er basert på at flere aktørers IT-systemer er i kontinuerlig drift. Disse systemene er igjen avhengig av annen infrastruktur som telekommunikasjon og strømforsyning. De sentrale aktørene i finansiell infrastruktur har egne løsninger for nødstrøm som under visse forutsetninger kan erstatte den offentlige strømforsyningen. Avbrudd og avvik hos en aktør i finansiell sektor kan likevel lett få virkninger også for andre aktører som banker og datasen-

[2] NICS: *Norwegian Interbank Clearing System*; Banknæringens felles avregnings- og transaksjonsbehandlingssystem.

[3] SWIFT:*Society for Worldwide Interbank Financial Telecommunication*.

traler, for eksempel som følge av avbrudd i datakommunikasjon.

Finansnæringen har aktivt tatt i bruk nye teknologiske muligheter og løsninger både når det gjelder de teknologiske plattformer som den enkelte virksomhet baserer seg på, og i særlig grad når det gjelder utviklingen av produktene og tjenestene som tilbys. I tillegg har finansnæringen i all hovedsak utkontraktert IT-driften til spesialiserte leverandører av IKT-tjenester. I de siste årene har slike tjenester også blitt utkontraktert til leverandører i utlandet, i første rekke Danmark og Sverige.

Elektroniske betalingsformer, som i stadig økende omfang overtar for de tradisjonelle, papirbaserte betalingsformene, er avhengig av tilgang til elektroniske kommunikasjonsnett der infrastrukturen i økende grad kontrolleres av private aktører. Bruken av elektroniske betalingsinstrumenter har økt gjennom flere år og utgjorde i 2004 over 90 pst av det samlede antallet betalingstransaksjoner. For eksempel økte antallet betalinger ved bruk av nettbank i 2004 med 36 prosent til over 138 millioner transaksjoner. Samtidig falt bruken av brevgiro, girobetalinger via telefon og giroer innlevert på ekspedisjonssted.[4] Bankenes kapasitet til å motta og behandle papirbaserte betalingsinstrumenter er redusert tilsvarende. Denne utviklingen innebærer at sårbarheten i finansiell infrastruktur i økende grad er knyttet til IKT-systemer. Publikums tilgang til kontanter vil også i stor grad være avhengig av at de IKT-baserte løsningene i finansiell infrastruktur er tilgjengelige, blant annet minibanker og kortterminaler.

Bankenes mulighet til å gjøre opp sine fordringer og forpliktelser er viktige for å ivareta stabiliteten i det finansielle systemet. Bankenes innestående på konti i Norges Bank er en viktig kanal for å formidle rentesignalene i pengepolitikken. I forbindelse med årtusenskiftet ble likviditeten i bankene betydelig styrket for å ta høyde for mulige problemer som denne overgangen kunne føre til for IKT-systemene. Det oppsto for øvrig ingen store problemer for finansnæringen ved overgangen til år 2000.

VPS sin mulighet for å gå gjennomført verdipapiroppgjøret og nødvendige rettighetsregistreringer er viktig for å ivareta stabiliteten og tilliten til verdipapirmarkedet. Overfor utvalget er det blitt hevdet at manglende tillit til sikkerheten og robustheten i denne delen av det finansielle systemet i Norge kan føre til at utenlandske investorer flytter sine plasseringer ut av landet.

[4] Norges Bank 2004. *Årsrapport om betalingsformidling 2004.*

Tabell 11.1 De 10 største bankene i Norge.

Konsern/*group*	Mill. kr
DnB NOR	714 680
Nordea Bank Norge	265 004
Fokus Bank	79 282
Handelsbanken 1)	66 375
SpareBank 1 SR-Bank	59 198
Skandinaviska Enskilda Banken 1)	52 578
Sparebanken Vest	46 265
SpareBank 1 Nord-Norge	42 245
BNbank	39 729
SpareBank 1 Midt-Norge	38 612

Kilde: Finansnæringens hovedorganisasjon.

11.1.2 Beskrivelse av eierforhold og organisering

Bank- og finanssektoren består hovedsakelig av private finansinstitusjoner. Staten har imidlertid betydelige eierinteresser innen sektoren, blant annet eier staten 33,7 % av aksjene i Norges største bank DnB NOR ASA. Tabell 11.1 gir en oversikt over de 10 største bankene i Norge, målt ut fra forvaltningskapital i 2004.

Rammevilkårene for bank- og finanssektoren i Norge blir i all hovedsak bestemt av deltakelsen i det indre markedet for finansielle tjenester og kapitalbevegelser og reglene om dette i EØS-avtalen. Kredittilsynet har til oppgave å påse at bestemmelsene etterleves. Fra 2007 skal norske banker etter planen oppfylle et nytt internasjonalt regelverk for risikostyring og tilsynsvirksomhet i finansiell sektor, det såkalte Basel II regelverket. Kredittilsynet er ansvarlig myndighetsorgan for innføring og overvåking av dette nye regelverket.

Norges Banks virksomhet er regulert i lov om Norges Bank og pengevesenet. Norges Bank skal bidra til en balansert økonomisk utvikling og at inflasjonsmålet nås, bidra til stabile og effektive finansmarkeder og betalingssystemer, tilfredsstille samfunnets behov for pengesedler og mynt og sørge for effektiv og sikker forvaltning av statens finansielle formue. Norges Banks ansvar knyttet til betalingssystemet og den finansielle infrastrukturen er regulert i sentralbankloven. I § 1, 1. ledd, fremgår det blant annet at Norges Bank skal «[...] fremme et effektivt betalingssystem innenlands og overfor utlandet.» Betalingssystemloven av 1999 gir Norges Bank ansvar for konsesjon og tilsyn med interbanksystemer, jf. figur 11.1. Loven gir Norges Bank mulighet til å gripe direkte inn med pålegg overfor operatører av interbanksystemer

med betydning for finansiell stabilitet. I kraft av sin rolle som øverste oppgjørsbank, har Norges Bank også en viktig oppgave med å gjennomføre betalingsoppgjørene på en sikker måte. Myndighetsansvaret for å følge opp betalingssystemet er delt mellom Norges Bank og Kredittilsynet.

Etter kredittilsynsloven fører Kredittilsynet blant annet tilsyn med kredittinstitusjoner, forsikringsselskaper og verdipapirhandel m.v. I § 3 i loven heter det blant annet at:

> Tilsynet skal se til at de institusjoner det har tilsyn med, virker på hensiktsmessig og betryggende måte i samsvar med lov og bestemmelser gitt i medhold av lov samt med den hensikt som ligger til grunn for institusjonens opprettelse, dens formål og vedtekter.

I tilknytning til dette føres det tilsyn med institusjonenes bruk av datasystemer og informasjonsteknologi. Krav til bruk av IKT-systemer er regulert i IKT-forskriften. I IKT-forskriftens § 12 pålegges foretak under tilsyn å regulere, i sine avtaler med IT-leverandører, Kredittilsynets rett til å foreta gjennomgang av aktiviteter hos leverandører knyttet til leveransene. I henhold til lov om betalingssystemer godkjenner Kredittilsynet verdipapiroppgjørssystemer og har et ansvar for å følge opp systemer for betalingstjenester.

Ved finansielle kriser kan Norges Bank tilføre ekstraordinær likviditet til en enkelt bank eller banksystemet som helhet. Norges Bank har lagt til grunn at ekstraordinær tilførsel av likviditet bør forbeholdes situasjoner der den finansielle stabiliteten kan være truet uten slik støtte.

I 2003 inngikk Norges Bank en avtale med ErgoIntegration AS (nå ErgoGroup AS) om drift og forvaltning av IT-systemene knyttet til Norges Banks oppgjørssystem. Selve IT-driften ble overført i 2004. Overføringen ble gjennomført som en virksomhetsoverdragelse, slik at ErgoGroup AS også overtok medarbeidere med sentral kompetanse om den IT-faglige driften og utviklingen av systemet. ErgoGroup AS eies av Posten Norge AS som igjen eies av Samferdselsdepartementet

Etter avtale med Finansnæringens Hovedorganisasjon og Sparebankforeningen i Norge er Bankenes Betalingssentral AS driftssted for NICS, jf. figur 13. Bankenes Betalingssentral AS eies av norske banker, med DnB NOR ASA som største aksjonær.

Verdipapirsentralen (VPS) ble etablert som et særlovselskap i 1985. I perioden 1985 til 2002 var VPS en selveiende institusjon (stiftelse). Stiftelsen ble omgjort til privat aksjeselskap i 2003. Virksomheten til VPS ASA kan sammenlignes med grunnboken for fast eiendom. VPS registrerer hvem som eier verdipapirer i Norge, dvs. i hovedsak hvem som eier den delen av norsk næringsliv som er børsnotert, hvem som er långivere til rentebærende instrumenter, hvem som er eiere av verdipapirfond og hvor stor del av disse verdipapirene som er pantsatt. Den samlede verdien av de verdipapirene som er registrert i VPS er om lag 2 500 milliarder kroner. Daglig gjennomsnittlig bruttoverdi av handler som avregnes i Verdipapiroppgjøret er om lag 30 mrd. kr. og verdien av betalingsformidling som går til BBS er om lag 2,5 mrd. kr per dag. Selv om denne virksomheten er konkurranseutsatt, jf. verdipapirregisterloven, er VPS et faktisk monopol. Tilsvarende virksomheter (Central Securities Depositories) i andre land er også faktiske monopoler.

Hver enkelt aktør i finansiell sektor har et selvstendig ansvar for sikkerheten i egen virksomhet. Dette ansvaret omfatter blant annet å utvikle stabile driftsløsninger og gode reserve- og beredskapsløsninger. For å bidra til en best mulig samordning av beredskapsarbeidet mellom aktørene i finansiell sektor ble Beredskapsutvalget for finansiell infrastruktur (BFI) opprettet i 2000. BFI har ansvaret for å komme frem til og koordinere tiltak for å forebygge og å løse krisesituasjoner og andre situasjoner som kan resultere i store forstyrrelser i den finansielle infrastrukturen. Kredittilsynet, Finansnæringens Hovedorganisasjon, Sparebankforeningen, Bankenes Betalingssentral AS, EDB Business Partner ASA og Verdipapirsentralen ASA har medlemmer i dette utvalget. Finansdepartementet deltar som observatør, mens Norges Bank leder utvalget og ivaretar sekretariatsarbeidet. I tillegg har utvalget kontaktpersoner hos flere andre aktører, blant annet DnB NOR Bank ASA, Nordea Bank Norge ASA, Norges vassdrags- og energidirektorat, Post- og teletilsynet og Telenor ASA. BFI erstatter ikke den enkelte institusjons selvstendige ansvar for beredskap i egen virksomhet.

11.1.3 Utvalgets vurderinger og anbefalinger

Bank- og finanstjenester er en kritisk samfunnsfunksjon som i stor grad er avhengig av eksterne kritiske infrastrukturer for opprettholdelse av funksjonsdyktighet. Dette gjelder i særlig grad i forhold til ekstern elektronisk kommunikasjonsinfrastruktur og kraftinfrastruktur.

Utvalget har derfor sett på de tiltak som retter seg mot de kritiske infrastrukturene som de aller fleste kritiske samfunnsfunksjonene er avhengige av. Utvalget ønsker derfor å understreke viktighe-

ten av at bank- og finanssektoren i sine ROS-analyser tar høyde for at de i stor grad er avhengig av ekstern infrastruktur for opprettholdelse av funksjonsdyktighet.

11.2 Matforsyning

Norge hadde tidligere egne ordninger for beredskapslagring og rasjonering av matvarer. Bortfall av avsperringsscenariet og en generelt god forsyningssituasjon har ført til at beredskapslagringen er sterkt redusert og rasjoneringsordningen avviklet. Beredskapslagringen har dessuten gått fra å være råvarebasert til bare å omfatte matvarer som kan brukes så å si umiddelbart. Den dekker 10 dagers kaloribehov for befolkningen i Nord-Norge nord for Ofoten. I tillegg arbeides det med etablering av planer for lageroppbygging av matvarer og et opplegg for å etablere ekstra lagerkapasitet.

Landbruksbaserte matvarer utgjør en vesentlig del av norsk matvareforbruk. På 1980- og 1990-tallet har norskprodusert andel av energiforbruket ligget på mellom 40 % og 50 %. For meieriprodukter og kjøtt er andelen nær 100 % mens den for korn har variert mellom 15 % og 50 %. Norsk produksjon av matkorn dekker i normalår mellom 40 % og 50 % av landets forbruk. Bruken av norsk hvete innebærer en buffer mot endring i markedstilgangen, fordi det er mulig å justere ned kvalitetskravene for mathvete. Dette er et egnet virkemiddel i forhold til å ivareta liv og helse. 90 % av all fisk og sjømat som landes og foredles i Norge eksporteres. Dette gir en viss fleksibilitet ved svikt i tilgangen av andre varer.

Velfungerende logistikksystemer hos matvaredistributørene er avgjørende for matvareforsyningene i Norge. ECON viser til at brist i norsk logistikk kan oppstå for eksempel ved at transportruter brytes (veger, havner, jernbane) eller ved at styringssystemer for logistikken svikter, for eksempel ved bortfall av elektronisk kommunikasjon eller strømforsyning.[5] I utvalgets møter med matvaredistributørene er det orientert om at matvareforsyning som system er avhengig av en rekke andre infrastrukturer. For at matvareproduksjon og -distribusjon skal kunne foregå som normalt er man avhengig av åpne veger, tilfredsstillende vannforsyning, stabil strømforsyning, fungerende elektronisk kommunikasjonssystemer og nøkkelarbeidskraft.

[5] ECON-rapport 21/01. *Robust forsyningsevne i krig og fred.*

11.2.1 Beskrivelse av samfunnsfunksjonen

Samfunnsfunksjonen matvareforsyning omfatter en rekke næringer innenfor landbruk, fiskeri- og akvakultur, videreforedling og - omsetning. Risiko- og sårbarhetsanalyser utført siden begynnelsen av 1990-tallet har vist at alle disse elementene må være til stede for at målsettingene om tilnærmet normale matvareforsyninger også i kriser skal kunne nås. De samme analysene har imidlertid ut fra det aktuelle krisescenariet konkludert med at det må etableres et særskilt forum for matvaredistribusjon knyttet til Nærings- og handelsdepartementets kriseorganisasjon for å møte de mest aktuelle forsyningsproblemene. Det vurderes fortløpende om det er behov for å utvide dette forumet, eller om det skal inngås tilsvarende samarbeid med aktører innenfor andre deler av matvareforsyningskjeden.

Distribusjon og omsetning av dagligvarer i Norge i dag foregår for en stor del gjennom fire grossistsammenslutninger: Norgesgruppen, Coop Norge, ICA Norge AS og Rema 1000. Fra 1990 har kjedene som er tilknyttet grossistsammenslutningene økt sin markedsandel fra rundt 50 % av detaljomsetningen av matvarer til 99 %. Norges Colonialgrossisters Forbund opplyser at dagligvaremarkedet omsetter for om lag 113 milliarder kroner årlig i 2004. I tillegg omsettes det en del dagligvarer i kiosker og på bensinstasjoner. Distribusjon av landbruksbaserte ferskvarer til detaljister går i all hovedsak gjennom Landbrukets ferskvaredistribusjon. Det foregår også en del direktedistribusjon av andre varer som f eks fersk fisk og fiskeprodukter.

I etterkrigstiden har vi sett en økende grad av sentralisering og strukturkonsentrasjon innen varehandelen. Totalt har det vært en nedgang fra om lag 9 000 dagligvareforretninger på slutten av 1970-tallet til om lag 4 400 i dag.[6] Mens antallet dagligvarebutikker har minket, har butikkene også blitt større.[7] Reduksjon av antall butikker har medført økte avstander og dermed større avhengighet av transport for kundene. En annen utvikling fra 1970-tallet er etableringen av et lavprismarked.

Aktørene i dagligvaremarkedet har organisert sine logistikksystemer slik at kostnadene i logistikkjeden reduseres. Alle grossistsammenslutningene benytter samlasteterminaler i Osloområdet til omlasting av varer fra leverandørene til biler som kjører til regionale lagre, men enkelte har også sentrale lagre.

[6] Nærings- og handelsdepartementet og Landbruksdepartementet 2002. *Risiko- og sårbarhetsanalyse av dagligvareforsyningen til Nord-Norge.*

[7] Lavik, Randi 2001. *Dagligvaretilgang i ulike regioner – utvikling 1980-2000.* Statens institutt for forbruksforskning. Rapport 5-2001.

Det har vært en vertikal integrering fra produsent, grossist og detaljist, hvor produsent og detaljist inngår forpliktende kontrakter med detaljist.[8] Sammenslutningene har dessuten i større grad tatt kontroll med den fysiske varestrømmen fra produksjonssted til butikk. En stor del av varene går direkte fra fabrikk til butikk uten mellomlagring. Man forsøker å rendyrke *just-in-time* prinsippet. Det er effektivt og rasjonelt, og lageret er for en stor del på paller i butikken. Ingen av sammenslutningene sitter på spesielle beredskapslagre.

Sentralisering av lagre og produksjonsanlegg har medført økt behov for transport. Transport fungerer også som lager og sånn sett er det meste av lagerbeholdningen på hjul. Sammenslutningene kjøper for en stor del transporttjenester av tredjepartsleverandør. Dette gjelder i særlig grad transport inn til terminal og lager.

Det tilstrebes så høy punktlighet som mulig i leveransene til butikkene. Leveransene fra dagligvaregrossistene skjer etter faste ruter og kjøreplaner hvor leveransene til den enkelte butikk skjer på bestemte dager og innenfor et gitt tidsvindu. Butikkene har begrensede lagre og vil ofte kunne oppleve mangel på enkelte varer ved forsinkelser utover 1 – 2 dager. Det er på bakgrunn av dette at veginfrastrukturen er et sårbart punkt i logistikkjeden.[9] En relativt stor nedgang de siste årene i antall meierier og slakterier har økt avhengigheten av transport. Et vedvarende strømbrudd er også en situasjon som kan skape store problemer for dagligvaregrossistene.

I normalsituasjoner håndterer næringen store sesongvariasjoner i etterspørselen, for eksempel ved ferieavvikling, men dette er avvik som kjedene har kunnet planlegge for å håndtere. Forsyningssystemet er sårbart i forhold til etterspørselssjokk, som for ekempel ved hamstring. Dette har blant annet vist seg under streiker og lignende. Det tar kort tid før butikkhyllene blir tomme for enkelte varer. Dagligvarebransjen har imidlertid gitt uttrykk for at dens logistikksystemer er meget fleksible. I krisesituasjoner vil den kunne øke volumet gjennom egne systemer betraktelig.

11.2.2 Beskrivelse av eierforhold og organisering

Landbruks- og matdepartementet (LMD) (produksjon, foredling, matsikkerhet), Nærings- og handelsdepartementet (NHD) (foredling, distribusjon) og Fiskeri- og kystdepartementet (FKD) (produksjon, foredling, matsikkerhet), er departementer med ansvar for ulike deler av matvareforsyningen. NHD har koordineringsansvar for matvareberedskap og administrerer Rådet for matvareberedskap. I dette rådet er alle de fire grossistsammenslutningene og Landbrukets ferskvaredistribusjon medlemmer.

I samarbeid med LMD og FKD har NHD gjennomført flere risiko- og sårbarhetsanalyser knyttet til forsyningssituasjonen for matvarer. Det arbeides nå med oppfølging av en risiko- og sårbarhetsanalyse fra 2002 for dagligvareforsyningen til Nord-Norge.

11.2.3 Utvalgets vurderinger og anbefalinger

Det er lite sannsynlig med store avbrudd i matforsyningen. Derimot er sannsynligheten for mindre avbrudd større. I en slik sammenheng er det viktig å vise til at den enkelte av oss som forbruker har et ansvar for å tenke gjennom hvilke varer vi kan ha bruk for i den nærmeste fremtid, og eventuelt ta høyde for uforutsette hendelser. Det er rimelig å forvente en viss robusthet i den enkelte husholdning, og at den enkelte må kunne klare seg selv noen dager før myndighetene iverksetter tiltak. I forbindelse med årtusenskiftet produserte det daværende Direktoratet for sivilt beredskap en brosjyre med råd om hva husholdningene burde ha av matvarer og andre livsnødvendigheter. Med etableringen av en ny nasjonal kriseweb ser utvalget det som naturlig at spørsmålet om en slik brosjyre på nett blir vurdert.

Utvalget ønsker også å vise til at matvarer dekker helt grunnleggende behov i befolkningen. Det vil derfor ikke være heldig å sette seg i en posisjon hvor landet i utstrakt grad gjør seg avhengig av import. Selv om sannsynligheten for større avbrudd i matvareforsyningen er svært liten, er konsekvensen av et større bortfall så stor at utvalget vil understreke viktigheten av å opprettholde tilfredsstillende nasjonal matvareproduksjon ut fra et sikkerhetsperspektiv. Det vil ta svært lang tid å bygge opp en tilfredsstillende kapasitet blant annet i landbruket, hvis den først er bygget ned.

Utvalget anbefaler at det innenfor det formaliserte samarbeidet mellom Nærings- og handelsdepartementet og de største matvaredistributørene arbeides for å identifisere sårbarhet i kritisk infrastruktur som matforsyningen er avhengig av, slik at svakheter kan videreformidles til rette fagmyndighet og så langt som mulig minimaliseres.

---

[8] Lavik, Randi 2001. *Dagligvaretilgang i ulike regioner – utvikling 1980-2000.* Statens institutt for forbruksforskning. Rapport 5-2001.

[9] Nærings- og handelsdepartementet og Landbruksdepartementet 2002. *Risiko- og sårbarhetsanalyse av dagligvareforsyningen til Nord-Norge.*

11.3 Helse-, sosial- og trygdetjenester

Et robust og velfungerende helsevesen er avgjørende for liv, helse og befolkningens trygghetsfølelse. Internasjonale sikkerhetspolitiske endringer, globalisering og endrede reisemønstre innebærer nye utfordringer for samfunnet. For helsevesenet gir dette seg utslag i at de må være i stand til å yte helsetjenester ved hendelser som vil berøre og ramme svært mange, som for eksempel pandemiske infeksjonssykdommer, terrorhandlinger og naturkatastrofer.

Sosialtjenesten og trygdeetaten har stor betydning for mange enkeltmennesker. Langvarig svikt i tjenester og stønader vil føre til at store grupper vil mangle hjelp og økonomiske midler til daglige livsnødvendigheter, og vil rokke ved trygghetsfølelsen til sårbare grupper i befolkningen.

Viktigheten av helse- sosialsektoren understrekes ved at det i lov om helsemessig og sosial beredskap og i folketrygdloven er stilt krav til beredskapsplaner for å sikre tjenestetilbudet ved kriser og katastrofer i fredstid eller ved krig.

11.3.1 Beskrivelse av samfunnsfunksjonen

Helse- og sosialtjenesten og trygdeområdet omfatter mange funksjoner som må opprettholdes. Eksempler på slike er sykehus, ambulansetjeneste, blodbanker, røntgen, isolater, laboratorier, sykehusapotek, lagre med særlig viktig utstyr, vaksiner og medikamenter, sykehjem, personlig assistanse til funksjonshemmede og trygdedatabaser.

Lov om helsemessig og sosial beredskap av 1. juli 2001 har som formål at helse- og sosialtjenesten skal være best mulig forberedt på å kunne tilby tjenester også etter at en krise eller katastrofe har inntruffet. Dette innebærer at tilbydere av helse- og sosialtjenester skal utarbeide planer for hvordan de skal kunne tilby tjenester under kriser og katastrofer i fredstid og ved krig. Lovverket stiller også krav om at planverket skal samordnes på tvers av etater innen helse- og sosialsektoren.

Ved alle større kriser og katastrofer vil det være et helseaspekt. Kravet til beredskapsplaner gjelder kommunene, fylkeskommunene og staten. Loven oppstiller krav om gjennomføring av ROS-analyser for tilbydere av helse- og sosialtjenester. I tillegg til lov om helsemessig og sosial beredskap med tilhørende forskrift, finnes det viktige beredskapsbestemmelser på helseområdet i smittevernloven, strålevernloven og i annen helselovgivning.

Den alminnelige smittevernberedskapen i Norge er kjernen i beredskapen mot smittsomme sykdommer og eventuelle angrep med biologiske våpen. Leger har en umiddelbar varslingsplikt til kommunelegen og fylkesmannen ved tilfeller av smittsomme sykdommer der det er mistanke om at dette er forårsaket av biologiske midler. Meldingssystem for smittsomme sykdommer (MSIS) ved Nasjonalt folkehelseinstitutt er det offisielle norske overvåkingssystemet for smittsomme sykdommer. Folkehelseinstituttet skal varsle Sosial- og helsedirektoratet og til EUs og WHOs varslingssystemer.

Det satses målbevisst på bruk av elektronisk kommunikasjon for å effektivisere helsevesenet. De regionale helseforetakene eier Norsk Helsenett AS som er et eget nettverk for elektronisk kommunikasjon i helse- og sosialsektoren. Eksempelvis har enkelte helseforetak ordninger der et sykehus tar røntgenbilder og overfører det til et annet sykehus hvor behandlingen skal skje.[10]

Tilgang til legemidler ved større sykdomsutbrudd

Logistikken i helsesektoren blir i stor grad styrt etter *just-in-time* prinsippet. Tilstrekkelig tilgang på legemidler, vaksiner og medisiner kan bli kritiske faktorer ved håndteringen av utbrudd av epidemier eller hendelser som er forårsaket av biologiske midler.

Erfaringer fra tidligere internasjonale kriser, for eksempel Gulfkrigen i 1991, viser at det raskt kan oppstå knapphet på viktige medisiner og medisinske forbruksartikler internasjonalt. Det er ikke sikkert at internasjonale legemiddelprodusenter vil prioritere leveranser til Norge framfor andre land.

Norge har forberedt seg på et influensautbrudd (pandemi) ved å utarbeide en nasjonal beredskapsplan og ved å gjøre avtale med en utenlandsk legemiddelprodusent om tidlig leveranse av vaksiner til Norge. Det er i tillegg kjøpt inn og satt på lager i Norge influensamedisin til behandling av dem som blir syke.

Dersom det oppstår en alvorlig internasjonal smittesituasjon eller annen større krise der det er knapphet på medisiner, vil det være en mulighet for at myndighetene i det legemiddelproduserende landet vil vurdere å ta kontroll over legemiddelprodusentens leveranser og søke å prioritere egne borgere. Dette vil i verste fall kunne føre til store problemer i legemiddelmarkedet, og resultere i uakseptabelt små leveranser til Norge.

Statens legemiddelverk har opplyst at Norge i all hovedsak mangler infrastruktur for legemiddelproduksjon. Infrastrukturen i Norge er derfor nær-

[10] Opplyst under utvalgets møte med Helsetilsynet.

mest utelukkende knyttet til distribusjons- og omsetningstjenester.[11] Helsetilsynet opplyser dessuten at det er mangler i legemiddelberedskapen og i beredskapen for medisinske forbruksartikler. Det er videre opplyst at det ikke er tilfredsstillende beredskapslagre av en del legemidler og medisinske forbruksartikler i Norge, blant annet antibiotika.[12]

11.3.2 Beskrivelse av eierforhold og organisering

Helse- og omsorgsdepartementet har et overordnet ansvar for helsesektoren og for samordning av tiltak og informasjonshåndtering i forhold underliggende virksomheter og andre departementer. Under departementet er det flere fag- og myndighetsorganer, som sammen med helsetjenestene lokalt og regionalt ivaretar beredskapen innenfor sektoren. Sosial- og helsedirektoratet har et helhetlig ansvar for nasjonal koordinering av helse- og sosialsektorens beredskap, både forberedende planlegging og operativ håndtering i en krise. Statens strålevern har ansvar for tverrsektoriell koordinering av beredskap ved atomulykker. Nasjonalt folkehelseinstitutt er nasjonal faginstans for smittevernberedskap og biologiske hendelser. Statens helsetilsyn fører tilsyn med at helse- og sosialtjenesten oppfyller lovpålagte beredskapskrav, og Statens legemiddelverk har ansvar for godkjenning av legemidler og tilsyn med legemiddelforsyningskjeden. Det er utviklet beredskapsplaner på alle nivåer.

Landets kommuner har ansvar for primærhelsetjenester, pleie- og omsorgstjenester og sosiale tjenester.

I henhold til lov om sosiale tjenester og lov om statlig tilsyn med helsetjenesten, har Statens helsetilsyn det overordnede faglige tilsyn med sosialtjenesten og helsetjenesten. Det betyr at Statens helsetilsyn er overordnet myndighet for Fylkesmannen og Helsetilsynet i fylkene hva gjelder tilsyn.

Foretaksreformen innebærer at Helse- og omsorgsdepartementet, ved siden av å være øverste ansvarlige myndighet for den nasjonale helsepolitikken, også har et direkte eieransvar for den største delen av spesialisthelsetjenesten, herunder finansieringen.

Helse- og omsorgsdepartementets utarbeider årlige bestillerdokumenter til de regionale helseforetakene. Disse gis normalt ut en gang per år, like etter at beslutningen om årets statsbudsjett foreligger i Stortinget. Bestillerdokumentene inneholder krav fra Helse- og omsorgsdepartementet om hvilke oppgaver som skal utføres i det påfølgende år, og hvilke krav som settes til de regionale helseforetakene. Styringslinjen overfor helseforetakene er delt i to. Den skjer gjennom bestillerdokumentet og gjennom foretaksmøtet i januar. I bestillerdokumentet formuleres krav stilt til tjenesten og i foretaksmøtet stiller departementet krav i kraft av å være eier.

De to grunnleggende områdene som helsetjenestene i Norge består av er primærhelsetjenestene, som i hovedsak er kommunenes ansvar (for eksempel legevakt, helsestasjon, sykehjem), og spesialisthelsetjenestene (for eksempel sykehus og ambulansetjeneste) som i hovedsak er statens ansvar.

Spesialisthelsetjenesten ble fra 1. januar 2002 organisert i fem statlig heleide regionale helseforetak. De regionale helseforetakene er ved lov gitt ansvar for å sørge for spesialisthelsetjenesten til befolkningen i sin region. Spesialisthelsetjenester kan tilbys gjennom regionens helseforetak, private tilbydere av spesialisthelsetjenester og fra helseforetak i andre helseregioner. De regionale helseforetakene og helseforetakene er egne rettssubjekter med klare fullmakter og ansvar, og er også eiere av egne helseforetak.

De offentlige sykehusene og sykehusapotekene er organisert i helseforetak. Det kan være ett eller flere sykehus organisert under samme helseforetak.

Arbeids- og inkluderingsdepartementet er ansvarlig departement for Rikstrygdeverket og trygdeetaten. Folketrygdloven er styrende for Rikstrygdeverkets virksomhet og i loven finnes det også krav til beredskapsplanlegging. Trygdeetaten består av mer enn 500 enheter inkludert Rikstrygdeverket og det finnes ett trygdekontor i hver kommune. Store kommuner har flere lokale trygdekontorer.

Det er besluttet at Trygdeetaten, sosialetaten og Aetat skal slås sammen i en ny arbeids- og velferdsetat (NAV) sommeren 2006. Arbeids- og velferdsetaten skal sammen med kommunene etablere lokale arbeids- og velferdskontorer (som fra kommunesiden minimum omfatter økonomisk sosialhjelp). Til sammen utgjør dette den nye arbeids- og velferdsforvaltningen. Den nye forvaltningen vil omfatte om lag 15 000 ansatte (inkludert de kommuneansatte) og vil ha ansvar for utbetaling av om lag 250 milliarder kroner (1/3 av statsbudsjettet). Den nye Arbeids- og velferdsetaten vil ha et eget lovverk med egne beredskapsbestemmelser for å sikre at ytelser også blir utbetalt i en krisesituasjon.

[11] Jf. brev av 21.02.2005 fra Statens legemiddelverk til utvalget.
[12] Opplyst under utvalgets møte med Helsetilsynet.

11.3.3 Utvalgets vurderinger og anbefalinger

Viktige helseinstitusjoner som sykehus, er avhengig av fungerende infrastruktur som strøm, elektronisk kommunikasjon, vann og avløp for å kunne levere gode helsetjenester. Dette er i stor grad infrastruktur som helseinstitusjonene ikke har kontroll over. Det er viktig at sykehuseiere er i dialog med infrastrukturvirksomheter sykehuset er avhengig av, for å sørge for tilstrekkelig robuste leveranser og for å melde fra om at de skal være prioriterte brukere i forhold til gjenoppretting ved bortfall av tjenesten. Sykehus må for eksempel ha planer og systemer for nødvannforsyning, nødstrøm og elektronisk kommunikasjonstjenester dersom det skulle oppstå brudd i ordinær tilgang.

Vaksiner og medisiner vil være knapphetsgoder ved fare for eller utbrudd av alvorlige epidemier og pandemier. Ved slike situasjoner vil helsevesenet, i samarbeid med andre myndigheter, ha viktige oppgaver i forhold til å prioritere bruk av medisiner. I den sammenheng bør leverandører av kritiske infrastrukturtjenester (som forsyning av strøm, vann og elektronisk kommunikasjon) gis prioritet slik at andre viktige samfunnsfunksjoner som er avhengig av kritisk infrastruktur ikke stopper opp.

Det er etablert en arbeidsgruppe med representanter fra Sosial- og helsedirektoratet, Statens legemiddelverk og Nasjonalt folkehelseinstitutt som skal foreslå tiltak for å øke forsyningssikkerheten for legemidler. Dette er særlig rettet mot å redusere sårbarheten ved manglende tilgang til legemidler tilvirket utenfor Norge. Arbeidet ble bestemt ferdigstilt i løpet av 2005. Utvalget understreker viktigheten av å følge opp dette arbeidet, og viktigheten av at resultatet av arbeidet blir bredt forankret i alle sektorer med kritisk infrastruktur og kritiske samfunnsfunksjoner.

11.4 Politi

Opprettholdelse av ro og orden og kriminalitetsbekjempelse er av fundamental betydning for samfunnets funksjonsdyktighet og den enkelte borgers sikkerhet. Gjennom forebyggende, håndhevende og hjelpende virksomhet er politiet sentralt i samfunnets samlede innsats for å fremme og befeste borgernes rettssikkerhet, trygghet og alminnelige velferd for øvrig.[13] Politiets rolle og oppgaver anses som en kritisk samfunnsfunksjon.

[13] Se politiloven § 1.

11.4.1 Beskrivelse av samfunnsfunksjonen

Politiets oppgaver fremgår av politilovens § 2 der det heter:

Politiet skal:
1. beskytte person, eiendom og fellesgoder og verne om all lovlig virksomhet, opprettholde den offentlige orden og sikkerhet og enten alene eller sammen med andre myndigheter verne mot alt som truer den alminnelige tryggheten i samfunnet
2. forebygge kriminalitet og andre krenkelser av den offentlige orden og sikkerhet
3. avdekke og stanse kriminell virksomhet og forfølge straffbare forhold i samsvar med regler gitt i eller i medhold av lov
4. yte borgerne hjelp og tjenester i faresituasjoner, i lovbestemte tilfeller og ellers når forholdene tilsier at bistand er påkrevet og naturlig
5. på anmodning yte andre offentlige myndigheter vern og bistand under deres tjenesteutøvelse når dette følger av lov eller sedvane
6. samarbeide med andre myndigheter og organisasjoner tillagt oppgaver som berører politiets virkefelt så langt regler gitt i eller i medhold av lov ikke er til hinder for dette
7. utføre andre oppgaver som er fastsatt i lov eller som følger av sedvane, herunder oppgaver som i lov er lagt til lensmannen, namsfogden eller politistasjonssjef med sivile rettspleieoppgaver.

Politiets trygghetsskapende oppgaver er særlig fremhevet i loven. Publikum har forventninger om at politiet skal kunne respondere raskt ved behov for hjelp. Dersom publikum ikke er fornøyd med politiets tilgjengelighet, i alle fall i det som oppfattes som alvorlige situasjoner, kan dette medføre tap av politiets evne til å bekjempe kriminalitet og ivareta befolkningens trygghet. Et lokalt forankret politi som er i døgnkontinuerlig tjeneste, er derfor en viktig forutsetning for å kunne ivareta slike hensyn. Dette bidrar for øvrig til effektiv kriminalitetsbekjempelse, ettersom enhver kriminell handling har en lokal forankring.

Politiet utgjør en helt sentral rolle innen det sivile samfunnets beredskap og samfunnssikkerhetsarbeid, herunder i arbeidet med sikringen av kritisk infrastruktur og kritiske samfunnsfunksjoner. Politiet må være forberedt på krisesituasjoner som krever en større koordinert innsats, og har plan- og instruksverk, og utstyr og beredskapsordninger for ekstraordinære hendelser. Politiets stående styrke kan på kort varsel mobiliseres i en krisesituasjon. I politiets stående styrke inngår Beredskapstroppen som er en innsatsavdeling med høy

beredskap og kompetanse, trenet for alvorlige og kompliserte gissel- og terrorsituasjoner til lands og offshore. Særskilte uttrykningsenheter utdannet og trenet for beredskapssituasjoner er etablert i Politidistriktene. For ytterligere å styrke politiet i en krisesituasjon kan mannskaper innkalles fra Politireservestyrken.[14] Politireserven er en forsterkingsressurs bestående av vernepliktige som har avtjent førstegangstjeneste, og som er overført til politireserven for den resterende plikttjenestetiden.

De metodene som politiet tar i bruk må være så effektive at alvorlig kriminalitet og samfunnstruende aktiviteter kan avdekkes og stanses. Lovfestede etterforskningsmetoder som politiet har til rådighet ble endret for å ivareta samfunnets sikkerhetsinteresser og borgernes trygghetsbehov, jf. Ot.prp. nr. 60 (2004-2005) *Om endringer i straffeprosessloven og politiloven* (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet), jf. Innst. O. nr. 113 (2004-2005). Endringene har gitt politiet bedre muligheter til å avverge og forebygge alvorlig og samfunnstruende kriminalitet.

Politiets sikkerhetstjeneste har som oppgave å forebygge og etterforske terrorvirksomhet, ulovlig etterretningsvirksomhet, spredning av masseødeleggelsesvåpen og av utstyr, materiale og teknologi for produksjon og bruk av slike våpen, og voldelig ekstremisme. Tjenesten har også et ansvar for å forebygge trusler mot statsledelsen, samt rådgivende oppgaver.

Politiets roller og oppgaver er grundig redegjort for i St.meld. nr. 42 (2004-2005) *Politiets rolle og oppgaver*.

11.4.2 Organisering

Det er staten som skal sørge for den polititjeneste som samfunnet har behov for, jf. politiloven § 1, 1. ledd. Justis- og politidepartementet og Politidirektoratet utgjør den sentrale politiledelsen.

Politidirektoratet har ansvaret for ledelse og oppfølging av politidistriktene og politi- og lensmannsetatens særorgan. Ansvaret er knyttet til den overordnede faglige ledelsen av politi- og lensmannsetatens virksomhet, herunder fordeling av ressurser og resultatoppfølging. Direktoratets oppgaver er blant annet etatsledelse, personal- og organisasjonsutvikling, støtte- og tilsynsoppgaver, forvaltningsoppgaver, beredskap, fag- og metodeutvikling samt behandling av klagesaker.[15]

Politiet er inndelt i 27 politidistrikter med en politimester som leder for hvert distrikt. Distriktene er igjen inndelt i funksjonelle og geografiske driftsenheter. Hovedredningssentralene ledes av politimestrene i Rogaland og Salten politidistrikter. Se for øvrig omtale i kapittel 11.5 om Nød- og redningstjenester.

Det er følgende særorganer i politiet:
- Kripos
- Utrykningspolitiet (UP)
- Den sentrale enhet for etterforsking og påtale av økonomisk kriminalitet og miljøkriminalitet (ØKOKRIM)
- Politiets data- og materielltjeneste (PDMT)
- Politiets utlendingsenhet (PU)
- Politihøgskolen (PHS)

Særorganene er administrativt og faglig underlagt Politidirektoratet. ØKOKRIM er i tillegg et statsadvokatembete, og er derfor i straffesaksbehandlingen underlagt riksadvokaten.

Politiets sikkerhetstjeneste er direkte underlagt Justis- og politidepartementet, og rapporterer i alle viktige saker til departementet. PST er organisert med en sentral enhet i Oslo, og enheter i samtlige politidistrikter unntatt Oslo. Innenfor tjenestens saksområde har den sentrale enheten i store trekk samme ledelsesfunksjon som Politidirektoratet har overfor politi- og lensmannsetaten. [16]

Politi- og lensmannsetaten i Norge har rundt regnet 11 000 ansatte.[17]

11.4.3 Utvalgets vurderinger og anbefalinger

Utvalget har ingen særskilte vurderinger og anbefalinger knyttet til å sikre den kritiske samfunnsfunksjonen til politiet. Det har sammenheng med at utvalget anser at funksjonsdyktigheten i første rekke kan sikres med god sikkerhet i de kritiske infrastrukturene som politiet benytter seg av. Eksempelvis vil politiets funksjonsdyktighet bli sterkt rammet av svikt i elektronisk kommunikasjonsinfrastruktur og kraftinfrastrukturen.

Utvalget ønsker likevel å peke på to forhold som er av viktighet i denne sammenheng. Dette er forhold som utvalget ikke har hatt anledning til å ta opp til grundig behandling, men som utvalget mener må utredes nærmere i sin bredde. Det første gjelder den sterke veksten i bruk av private sikkerhets- og vekterselskaper hvor selskapene faktisk utøver maktanvendelse, infiltrasjon på arbeids-

[14] St.meld. nr. 42 (2004-2005) *Politiets rolle og oppgaver*, kapittel 6.7.1
[15] St.meld. nr. 42 (2004-2005) *Politiets rolle og oppgaver,* kapittel 4.1.
[16] St.meld. nr. 42 (2004-2005) *Politiets rolle og oppgaver*, kapittel 4.1.
[17] www.politiet.no

plasser og etterforskning av straffbare forhold. En hovedinnvending er at private sikkerhets- og vekterfirmaer ikke er underlagt den samme strenge demokratiske kontrollen som politiet. Dette er i hovedsak oppgaver som er lagt til politiet med hjemmel i politiloven, og som er viktige funksjoner i samfunnet. Likeledes stiller utvalget spørsmål ved om oppgaver som omfatter sivil maktanvendelse, infiltrasjon på arbeidsplasser og etterforskning av straffbare forhold skal overlates til personell uten politifaglig kompetanse. Utvalget vil derfor anbefale at problemstillingen blir tatt opp i hele sin samfunnsmessige bredde med organisatorisk forankring i Justis- og politidepartementet. For det andre viser utvalget til at det planlegges med sikte på å videreføre en fremtidig politireservestyrke og oppjustere antallet til 2 000 personer, og at den fremtidige bruk av politireserven vil bli vurdert av Justis- og politidepartementet.[18] I denne forbindelse mener utvalget at ansvarsdelingen mellom Heimevernet og politireserven bør vurderes. Dette gjelder blant annet oppgaver knyttet til vakthold og sikring av kritisk infrastruktur.

11.5 Nød- og redningstjeneste

I et moderne samfunn er det helt vesentlig å ha et effektivt apparat som kan redde mennesker i nød og begrense konsekvensene ved ulykker og andre uønskede hendelser. I dette kapittelet omtales samfunnsfunksjonen nød- og redningstjeneste, herunder nødetatene, Redningstjenesten og andre redningsaktørers roller. Redningstjenesten er en del av det samlede kriseapparatet som er nærmere beskrevet i kapittel 11.6. Med redningstjeneste forstås den offentlig organiserte virksomhet som utøves i forbindelse med øyeblikkelig innsats for å redde mennesker fra død og skader som følge av akutte ulykkes- eller faresituasjoner, og som ikke blir ivaretatt av særskilt opprettede organer eller ved særlige tiltak.

Norsk redningstjeneste er en nasjonal dugnad hvor alle ressurser i landet som er egnet for akuttinnsats for å redde liv, skal kunne mobiliseres for innsats i Redningstjenesten. Redningstjenesten er basert på et integrert samvirke mellom hovedredningssentralene, nødetatene (politi, brann og helse), Forsvaret og andre offentlige etater, private og frivillige organisasjoner som Røde Kors, Redningsselskapet osv., samt samarbeid og bistand fra andre land i tilfeller der dette er nødvendig. Disse deltar etter anmodning og ledelse fra en av hovedredningssentralene eller en av de lokale redningssentralene, lokalisert ved politidistriktene.

I et moderne samfunn er det avgjørende at befolkningen føler seg trygge på at den livreddende innsats som trer i funksjon når mennesker utsettes for alvorlige hendelser, er så velfungerende som mulig. Dette er av grunnleggende betydning for befolkningens trygghetsfølelse. Det er på det rene at den innsats som gjøres i første fase av en alvorlig hendelse, er avgjørende for hvilket omfang og konsekvenser en alvorlig hendelse kan få, og for hvordan den samlede innsatsen vil bli vurdert i ettertid. Det må forventes at redningstjenesteapparatet organiseres og drives på en tilfredsstillende måte, også ved svikt eller bortfall av kritisk infrastruktur. Dette stiller krav til at redningstjenesten, som kritisk samfunnsfunksjon, kontinuerlig utvikles og innrettes i takt med samfunnsutviklingen, dvs. ut fra forhold som befolkningens ferie- og fritidsvaner (for eksempel ekstremsport), klimaendringer, endringer i trusselbildet mv.

11.5.1 Beskrivelse av samfunnsfunksjonen

Redningstjenesten er et samvirke som hurtig kan mobilisere redningsressurser mellom offentlige etater, frivillige hjelpeorganisasjoner og kommersielle virksomheter som har egnede ressurser for redningsformål. Alle ressurser som er egnet for akuttinnsats organiseres, trenes og brukes ved innsats i den offentlig koordinerte redningstjeneste. Kjernen i redningstjenesten til lands utgjøres av de tre nødetatene politi, brann og helse.[19] Ved redningsaksjoner til sjøs, har Sjøforsvaret, redningshelikoptertjenesten og Redningsselskapet sentrale roller.[20] Økt aktivitet i våre nære farvann, særlig i nord, setter krav til redningstjeneste til sjøs.

Redningstjenesten er regulert i kgl. res. av 4. juli 1980 med senere endringer, samt i bestemmelser, generelle retningslinjer og operative prosedyrer gitt i internasjonale konvensjoner for sjøfart og luftfart. Det er også inngått bilaterale avtaler med naboland.

Den øverste operative samordning og ledelse av redningstjenesten tilligger de to hovedredningssentralene i Stavanger og Bodø. Hovedredningssentralene skal i tillegg vedlikeholde og fornye planverk for egen virksomhet, og føre tilsyn med planverk for de underlagte lokale redningssentralene (LRS). HRS skal også avholde regionale øvel-

[18] St.prp. nr. 1 (2005-2006), side 107.

[19] NOU 2001:31 Når ulykken er ute. *Om organiseringen av operative rednings- og beredskapsressurser.*

[20] Redningshelikoptrene ved 330-skavdronen på fastlandsnorgeog Airlift på Svalbard er de eneste dedikerte redningsressursene for redningstjenesten.

ser for eget ansvarsområde og føre tilsyn med LRS øvelsesvirksomhet. Med lokal redningssentral menes det ledelse- og koordineringsapparat som iverksettes ved politidistriktet under en søk- og redningsaksjon. Politimesteren kan avpasse apparatets størrelse etter situasjonen.

Det totale antallet iverksatte redningsoppdrag var i overkant av 2 500 i 2004. De fleste av disse oppdragene ble koordinert av de lokale redningssentralene. I løpet av de siste 20 årene har det vært en merkbar økning i redningstilfeller, og i takt med utviklingen i samfunnet, forventes denne utviklingen å fortsette.[21]

Kommunikasjon er en forutsetning for en effektiv redningstjeneste. Til sjøs er kystradionettverket viktig og til lands vil det nye nødnettet bli en betydningsfull oppgradering.

Grunnleggende prinsipper for redningstjenesten

Ansvars-, likhets- og nærhetsprinsippet fastholder at ulykker og kriser skal håndteres på lavest mulig nivå og av de etater/myndigheter som ut fra hendelsens art er pålagt ansvaret i det daglige.

Samvirkeprinsippet er en av bærebjelkene i redningstjenesten. Alle offentlige etater med ressurser egnet for søk og redningsformål plikter å delta i redningstjenesten, og ikke bare dekke utgifter som påløper til personell, materiell, planlegging og øvelser. De plikter også å stille ulike rådgivningsfunksjoner og redningsrelevante data mv. kostnadsfritt til disposisjon for hovedredningssentraler og de lokale redningssentraler. Private og frivillige organisasjoner og virksomheter plikter å stille relevante ressurser til rådighet mot dekning av påløpte kostnader.

Samhandling, beredskapsplanlegging og samtrening mellom de forskjellige aktørene i redningstjenesten, gjør redningsinnsatsene mer effektive, oppgaveorienterte og mobile.

Nødetatenes rolle (politi, brann og helse)

Nødetatene utgjør kjernen i redningstjenesten på land. Nedenfor gis det en overordnet beskrivelse av de tre nødetatenes roller.

På kommunalt nivå er det den kommunale legevakten som ivaretar helsevesenets beredskap, mens det på spesialisthelsetjenestenivå er sykehusene som er i kontinuerlig beredskap. For å bidra til at pasienter raskt får et medisinsk tilbud er ambulansetjenesten på samme måte i kontinuerlig beredskap for enten å bringe helsetjeneste til pasienten, eller ved at pasienten bringes til helsetjenesten. Årsaken til behovet for helsetjeneste, vil være bestemmende for de ressursene som skal settes inn for å håndtere hendelsen.

Ambulansetjenesten består av biler, båter, fly og helikopter som raskt kan mobiliseres etter varsling. For å binde sammen de ulike delene av de akuttmedisinske tjenestene er det opprettet lokale legevaktssentraler (LV-sentraler) i kommunene og akuttmedisinske kommunikasjonssentraler (AMK-sentraler) i sykehusene. AMK-sentralene koordinerer den akuttmedisinske innsatsen, men dersom en hendelse gjør det nødvendig vil denne koordineringen bli overtatt av Regional AMK-sentral.

Politiet har en nøkkelposisjon i redningstjenesten, både som skadestedsleder og i egenskap av å ha den lokale redningssentralen, og ved utøvelse av koordinerende ledelse gjennom politidistriktenes operasjonssentraler og politimesterens operative stab. Politiets oppgave innenfor redningstjenesten er å koordinere fellesinnsats for å redde mennesker fra død eller skade som følge av akutte ulykkes- eller faresituasjoner. Tiltakene kan bestå i organisering av skadested og innsats, evakuering, ettersøking, medisinsk førstehjelp, registrering av skadde, vakthold og nødvendige trafikkreguleringer. Politiets ansvar under katastrofer og krisehåndtering gjelder også forhold som går utover selve redningssituasjonen. I naturkatastrofer og lignende situasjoner har politiet en initialplikt i innledningsfasen, inntil annen offentlig myndighet kan overta. Politiets døgnkontinuerlige beredskap, utrustning og kompetanse gir politiet et godt utgangspunkt for å kunne håndtere ulykker, kriser og faresituasjoner. [22]

Brann- og redningsetaten er dimensjonert for å yte innsats etter lokale eller regionale risiko- og sårbarhetsanalyser, og deres utrustning og kompetanse reflekterer dette. Brann- og redningsetaten har lokal tilhørighet, utøver hurtig effektiv teknisk innsats, og er den viktigste tekniske førstelinjeinnsatsen i redningstjenesten. Brann- og redningsetatens innsats ved ulykker redder liv og tilrettelegger for rask og effektiv akuttmedisinsk behandling. Innsats kan eksempelvis være rettet mot brannslokking, redningsdykking, utslipp av kjemikalier, frigjøring av omkomne eller skadde, livreddende førstehjelp, tauredning og sikring av et ulykkessted.

[21] St.meld. nr. 42 (2004-2005) *Politiets rolle og oppgaver,* kapittel 4.2

[22] Det vises til ytterligere omtale i St.meld. nr. 42 (2004-2005) *Politiets rolle og oppgaver*, kapittel 4.2 og kapittel 6.7.

I etterkant av terrorbombene i Madrid, undersøkte DSB nød- og redningsetatenes evne til å håndtere en tilsvarende situasjon i Oslo. I undersøkelsen oppga aktørene at de har god kompetanse og ressurser til å møte store utfordringer. Imidlertid viste det seg at ingen av nødetatene er dimensjonert for å håndtere et skadeomfang av en tilsvarende størrelse som terrorbombene i Madrid.[23]

Frivillige redningsorganisasjoner

De frivillige redningsorganisasjonene utgjør en meget viktig del av redningstjenesten. Deres medvirkning i denne kritiske samfunnsfunksjonen er av avgjørende betydning. Det er politiet som kaller ut og koordinerer innsatsen. Norges Røde Kors Hjelpekorps er med sine vel 13 500 medlemmer fordelt på 320 hjelpekorps, den største frivillige redningsorganisasjonen. De er årlig med på om lag 400 redningsaksjoner. Redningsselskapet har en sentral rolle ved redningsinnsatser til sjøs. Redningsselskapet bemanner sine 28 redningsskøyter 24 timer i døgnet, og berget 108 fartøyer og reddet 40 mennesker i 2004. I tillegg assisterte de over 11 000 mennesker og nesten 5 500 fartøyer i samme år. Også andre bidrar vesentlig, slik som Norsk Folkehjelp, Norske Redningshunder, ulike alpingrupper osv. De frivillige redningsorganisasjonene kan stille spesialtrent personell innen samband, søk/redning i bratt lende og grotter, strandsøk, søk med hund og småfly.

Sivilforsvaret

Det vil ikke være ressursøkonomisk mulig å forvente at alle primæransvarlige myndigheter bygger opp tilstrekkelige ressurser til å håndtere alle ekstraordinære situasjoner. Det er derfor et behov for at staten har forutsigbare ressurser som kan settes inn i slike situasjoner, og derved styrke samfunnets evne til å håndtere store redningsaksjoner og andre hendelser som krever ekstraordinær innsats. Sivilforsvaret er en slik ressurs, og yter forsterkning til alle de tre nødetatene, kommuner og andre myndigheter. Hensikten er å styrke samfunnets evne til å håndtere store redningsaksjoner og andre hendelser som krever ekstraordinær innsats. I fredstid kan Sivilforsvaret sette inn en styrke på om lag 10 000 mannskaper. Kraftsamling av styrken krever imidlertid stor grad av mobilitet som bare til dels finnes i dag.

Et strømlinjeformet og modernisert Sivilforsvar med ressurser av god kvalitet som raskt og effektivt kan komme ulike deler av samfunnet til nytte når det trengs, vil gjøre redningstjenestens krisehåndteringsevne robust og i stand til å yte massiv innsats etter ekstraordinære hendelser med påfølgende brudd i, eller bortfall av for eksempel elektrisitetsforsyning, telekommunikasjon og vannforsyning.

Forsvaret

Forsvaret har faste oppgaver innenfor redningstjenesten knyttet til blant annet Redningshelikoptertjenesten, som i hovedsak utføres av Luftforsvarets 330-skvadron. Andre militære kapasiteter bistår redningstjenesten ved behov. Sjøforsvarets ressurser er av fundamental betydning når det gjelder søk- og redningsaksjoner til sjøs. I Heimevernet ligger det en betydelig kapasitet som kan nyttes til å avverge eller begrense naturkatastrofer eller andre alvorlige ulykker.

NARRE

Direktoratet for samfunnssikkerhet og beredskap (DSB) er gitt i oppdrag å lede utviklingen av et nasjonalt ressursregister for redning og beredskap (NARRE). Arbeidet med å utvikle NARRE skjer i nært samarbeid med Hovedredningssentralene (HRS). NARRE skal dekke behov lokalt, regionalt og nasjonalt, og skal være et verktøy for alle aktuelle beredskapsetater som har behov for å skaffe seg oversikt over ulike rednings- og beredskapsressurser.

11.5.2 Organiseringen av nød- og redningstjenestene

Justisdepartementet har det overordnede administrative samordningsansvaret for land-, sjø- og flyredningstjenesten. Redningstjenesten er operativt organisert med to hovedredningssentraler og 28 lokale redningssentraler (LRS) som tilsvarer antallet politidistrikter, herunder Sysselmannen på Svalbard, samt 16 flyredningssentraler. Den øverst operative samordning og ledelse av redningstjenesten tilligger de to hovedredningssentralene i Stavanger og Bodø som ledes av henholdsvis politimesteren i Rogaland og politimesteren i Salten. Grensen mellom de to sentralene går ved 65 grader nordlig bredde og grensen mellom Nord-Trøndelag og Helgeland politidistrikt.

HRS består av en kollektiv ledelse med representanter for aktuelle offentlige etater, utpekt av de

[23] DSB-rapport 2004. *Erfaringer etter terrorangrepet i Madrid Krisehåndtering og ressurstilgjengelighet i forbindelse med en tenkt tilsvarende hendelse i Oslo.*

respektive departementer. Sjøforsvaret, Luftforsvaret, Politiet, Telenor (kystradio), Helsevesenet og Lufttrafikktjenesten er representert i redningsledelsen. De lokale redningssentraler består av en redningsledelse med politimesteren (eller stedfortreder) som leder. Redningsledelsen består av representanter fra Brannvesenet, Helsevesenet, Havnevesenet, Forsvaret, Telenor, Lufttrafikktjenesten, Den Norske Kirke, Sivilforsvaret og Frivillige organisasjoner.

Organiseringen av helsevesenet og politiet er nærmere redegjort for i henholdsvis kapittel 11.3 og 11.4. Brannvesenet er kommunalt organisert, og underlagt tilsyn av Direktoratet for samfunnssikkerhet og beredskap.

11.5.3 Utvalgets vurderinger og anbefalinger

11.5.3.1 Forslag knyttet til samvirkeprinsippet

Utvalget understreker betydningen av å opprettholde og videreutvikle samvirkeprinsippet i redningstjenesten. Særlig viktig er det å ta hensyn til videreføring av samvirkeprinsippet i forbindelse med omorganisering og privatisering av offentlige virksomheter, se også kapittel 8.5.1.

11.5.3.2 Forslag til styrking av beredskapen ved ekstraordinære hendelser.

DSB utarbeidet i november 2005 et forslag om å styrke samfunnets evne til å håndtere store redningsaksjoner og andre hendelser som krever ekstraordinær innsats. Forslaget bygger på en omfattende kartlegging – basert på samarbeid og bidrag fra andre myndigheter, de tre nødetatene, med flere.

Forslaget fra DSB innebærer en utvikling og modernisering av Sivilforsvarets operative styrker. Ett av de tiltak DSB foreslår er å opprette 20 nye innsatsenheter (Sivilforsvarets innsatsgruppe teknisk) som er spesielt utrustet for innsats ved hendelser som setter samfunnet på prøve.

Innsatsenhetene skal ivareta behovet for teknisk utstyr med stor kapasitet ved ulike typer ekstraordinære hendelser, slik som store redningsaksjoner, strømutfall, store vannlekkasjer og mangelfull skadestedsinfrastruktur. Forslaget går ut på å opprette en slik enhet i hvert av de 20 sivilforsvarsdistriktene. Dette gir mulighet både for rask innsats på ethvert sted i landet og mulighet for kraftsamling av mange enheter over en viss tid ved store hendelser.

Hver innsatsenhet foreslås utrustet med tungt mobilt teknisk utstyr til redningsinnsats, lensing av store mengder vann, strømforsyning osv. Når det for eksempel gjelder tiltak for å styrke beredskapen for å håndtere konsekvensene ved omfattende strømbrudd, foreslår DSB en strømforsyningscontainer med en kapasitet på om lag 100 kVa per innsatsenhet. Dette vil være en viktig strømforsyningskilde ved bortfall av strøm til kritiske samfunnsfunksjoner, strømforsyning på store skadesteder med ødelagt eller manglende infrastruktur, lensing av store mengder vann osv. Tverrfagligheten til innsatsenhetene i DSBs forslag representerer en kosteffektiv ordning sett i forhold til alternativet. Utplasseres tilsvarende materiell fragmentert hos ulike etater vil ikke utstyret kunne nyttes i et tverrsektorielt samvirke. Det kan heller ikke forventes at andre virksomheter vil kunne ha like stor personellreserve i beredskap som det Sivilforsvaret har.

Utvalget anbefaler at DSBs forslag følges opp.

11.6 Kriseledelse

De aller fleste kriser og uønskede hendelser blir håndtert av etater som har dette som daglig oppgave, blant annet av nød- og redningstjeneste og fagmyndigheter. Dette er i tråd med ansvars-, nærhets og likhetsprinsippet. Når hendelser når et visst omfang og/eller berører den nasjonale tryggheтsfølelse, har erfaringer vist at det er nødvendig å forsterke og koordinere på nasjonalt, regionalt og lokalt myndighetsnivå. Hendelsene krever tverretatlig og tverrfaglig innsats, samt store personell- og materiellressurser med stor utholdenhet. Eksempler på hendelser som har utløst, eller vil utløse dette er store naturkatastrofer, pandemier, svikt i kritisk infrastruktur/samfunnsfunksjoner og terrorangrep.

11.6.1 Beskrivelse av samfunnsfunksjonen

Den organisatoriske strukturen i kriseledelsessystemet, uansett myndighetsnivå, baserer seg på følgende organisatoriske prinsipper:

- *Ansvarsprinsippet;* den som har ansvar i en normal situasjon har også ansvar i tilfelle ekstraordinære hendelser.
- *Likhetsprinsippet*; den organisasjon man opererer med til daglig skal være mest mulig lik den organisasjon man har under kriser.
- *Nærhetsprinsippet;* kriser skal håndteres på et lavest mulig nivå.

Disse prinsippene har vært det fundamentale grunnlag for organiseringen av alt offentlig arbeid

med sikkerhet og beredskap i Norge gjennom flere år.

I tråd med ansvarsprinsippet ligger ansvaret for kriseledelse hos den myndighet som har det forvaltningsmessige ansvaret for en sektor. Det konstitusjonelle ansvaret for kriseledelsen ligger hos den enkelte fagstatsråd og hos Regjeringen som kollegium. Den til enhver tid sittende regjering kan imidlertid endre på ansvarsdelingen på departementalt nivå.

Det følger av likhetsprinsippet at det ikke bør etableres organisatoriske enheter løsrevet fra de ordinære ansvarslinjene som trer i funksjon når det oppstår en krisesituasjon. På denne måten ivaretas overføringen av den nødvendige erfaring og fagkompetanse fra en normalsituasjon til en krisesituasjon. Likhetsprinsippet retter seg til den enkelte forvaltningsansvarlige myndighet, og er således ikke til hinder for at det etableres ekstraordinære fora som koordinerer krisehåndtering mellom de ansvarlige myndigheter.

Nærhetsprinsippet innebærer at ansvaret for kriseledelse må ivaretas like godt på lokalt nivå som på sentralt nivå. I henhold til ansvarsprinsippet og den administrative forvaltningspraksis som har utviklet seg som følge av nærhetsprinsippet, forutsettes det at kommunene ivaretar sitt ansvar på lokalt nivå. Organiseringen etter nærhetsprinsippet er begrunnet ut fra behovet for å ivareta kunnskap om lokale forhold, som for eksempel bosetting, næringsvirksomhet, geografi osv.

11.6.2 Nasjonal kriseledelse

11.6.2.1 Behovet for nasjonal kriseledelse

En krise som kan håndteres isolert innenfor et departements myndighetsområde, forutsetter ingen annen organisatorisk struktur enn den departementet selv har etablert. Behovet for en tverrsektoriell nasjonal kriseledelse oppstår i de situasjoner som er så alvorlige eller komplekse at det enkelte departement ikke kan håndtere de alene. I slike situasjoner vil det være behov for informasjonsdeling og koordinering av planer og ressurser for krisehåndtering på tvers av ansvarslinjene.

11.6.2.2 Beskrivelse av ansvarsforhold og organisering

Regjeringen bestemmer selv hvordan den ønsker å organisere seg under kriser.

Nedenfor redegjøres det for sentrale organer som har blitt gitt en rolle i forhold til nasjonal kriseledelse i fredstid. Det er også redegjort for det nasjonale beredskapssystemet, samt ordninger for varsling og informasjon til berørte aktører ved kriser.

Lederdepartement

Det følger av St.meld. nr. 37 (2004-2005) at kriseledelsen på sentralt nivå skal ivaretas av det departement som er mest berørt av en krise. Også andre forhold skal tillegges vekt ved valg av lederdepartement, herunder krisens karakter og hvilket departement som har virkemidler til å håndtere krisen. Det departementet som utpekes til lederdepartement er ansvarlig for koordineringen av krisehåndteringen på sentralt nivå. Lederdepartementets koordineringsansvar overfor øvrige departementer, fratar ikke fagdepartementenes myndighetsansvar.

Regjeringens kriseråd

I komplekse krisesituasjoner som krever koordinering på departementsnivå, skal Regjeringens kriseråd etableres. Rådet skal blant annet vurdere spørsmålet om lederdepartement, koordinere iverksettelsen av tiltak og informasjon til media og publikum.[24] Alle departementsrådene kan ta initiativ til innkalling av Regjeringens kriseråd, og rådet utvides etter behov. Dersom lederdepartement ikke er utpekt, ledes Regjeringens kriseråd av Justis- og politidepartementet. Justis- og politidepartementet er også gitt et særskilt ansvar for å ta initiativ til å innkalle rådet dersom dette ikke gjøres av andre.

De organisatoriske endringene som blir knyttet til sentralt kriseledelse, herunder utpeking av lederdepartement og etablering av Regjeringens kriseråd, medfører ingen endringer i det enkelte fagdepartements myndighetsansvar. Formelle beslutninger må forankres i fagdepartementene på ordinær måte.

Regjeringens krisestøtteenhet

For å kunne ivareta sitt ansvar i en krisesituasjon skal lederdepartementet kunne hente bistand fra Regjeringens krisestøtteenhet. Justis- og politide-

[24] De faste medlemmene i Regjeringens kriseråd er regjeringsråden ved Statsministerens kontor, departementsråden i Justis- og politidepartementet, departementsråden i Forsvarsdepartementet, departementsråden i Helse- og omsorgsdepartementet og utenriksråden i Utenriksdepartementet. I tillegg skal rådet i lys av den aktuelle krisen utvides med den eller de departementsrådene som er berørt av den aktuelle krisen.

partementet har det administrative ansvaret for krisestøtteenheten. Enheten skal bistå lederdepartement og regjeringens kriseråd og øke de ressursene departementene kan trekke på i krisesituasjoner. Enheten skal kunne utvides ved behov. Etableringen av krisestøtteenheten er en oppfølging av sårbarhetsutvalgets forslag om etablering av en nasjonal krisehåndteringsenhet, Reinåsutvalgets anbefalinger og St.meld. nr. 37 (2004-2005). [25]

Regjeringens krisestøtteenhet er under oppbygging, og en endelig konkretisering av oppgavene ventes i løpet av våren 2006.

11.6.2.3 Beredskapsutvalget

Koordineringen på norsk side i forhold til internasjonale tiltak som fulgte etter terrorangrepene i USA 11. september 2001 ble ivaretatt av Utenriksdepartementet i nær kontakt med berørte departementer og Statsministerens kontor. Utenriksdepartementets organ ble videreført og har gått under navnet «Beredskapsutvalget». Dette er ikke et organ med besluttende myndighet, men en møteplass mellom embetsmenn på høyt nivå for å diskutere den sikkerhetspolitiske, utenrikspolitiske og trusselmessige situasjon.[26] Organet sammenkalles etter ønske og behov.

11.6.2.4 Kontaktgruppen

Koordineringen av beredskapen innenlands etter 11. september 2001 ble ivaretatt av Justis- og politidepartementet. Departemenet ledet en kontaktgruppe som bestod av representanter fra de beredskapsansvarlige departementer og det tidligere Direktoratet for sivilt beredskap. Den såkalte «Kontaktgruppen» sørget for at departementene fikk oppdatert og lik informasjon om situasjonsbildet og var et forum for utveksling av informasjon om nasjonale beredskapstiltak.[27] Kontaktgruppen er opprettholdt og er senere blitt brukt i krisesituasjoner.

11.6.2.5 Kriseledelse ved terror- og sabotasjesituasjoner

«Den rådgivende stab» har hatt til oppgave å gi råd til justisministeren og den berørte politimesteren ved terror- og sabotasjesituasjoner. Denne staben er til vurdering i lys av omorganiseringen av Regjeringens kriseledelsesapparat, jf. St.meld. nr. 37 (2004-2005).

Det følger av dette at i situasjoner hvor det er utøvd terror eller sabotasje vil normalt Regjeringens kriseråd bli sammenkalt for å gi råd til Regjeringen og strategisk ledelse i lederdepartementet, samt eventuelt sørge for nødvendige fullmakter. Politidirektoratet etablerer iht. eget planverk krisestab for å støtte berørte politimestere med nødvendige ressurser og samordning. Organisasjonen er fleksibel både med hensyn til bemanning og hvem som er representert, slik at den kan tilpasses situasjonen.

Terror- og sabotasje er en form for alvorlig kriminalitet, og den operative håndteringen av terror- og sabotasjesituasjoner er politiets ansvar. Politiet skal lokalisere og pågripe gjerningsperson(er) som har iverksatt eller truer med å iverksette slike handlinger i fred, krise eller krig, såfremt det åpenbart ikke er stridshandlinger utført av militære stridskrefter tilhørende en fremmed makt. Forsvarets bistand til Politiet er regulert i kgl. res. av 28. februar 2003. Det er en forutsetning at bistand fra Forsvaret ytes i de tilfeller der politiets ressurser ikke strekker til.

Forsvarets spesialkommando (FSK) er opprettet for å yte bistand til politiet i forbindelse med terror- og sabotasjehandlinger offshore. Når det gjelder bistand til politiet i forbindelse med å bekjempe terroranslag, kan HV i gitte situasjoner være en viktig ressurs. I lys av et uforutsigbart trusselbilde hvor det ikke kan ses bort fra at politiets samlede ressurser ikke strekker til, er det viktig at HV ved behov kan stille fleksible og kompetente bistandsressurser til disposisjon for politiet. Slik bistand antas primært å kunne være aktuell i forbindelse med situasjoner der det iverksettes omfattende objektsikring, eller hvor beskyttelsesbehovet vil kunne strekke seg over en lengre tidsperiode.

Nasjonalt beredskapssystem[28]

Et endret trusselbilde, ikke minst med bakgrunn i hendelsene 11. september 2001, synliggjorde behovet for et krisehåndteringsverktøy også for den lavere del av krisespekteret. NATO har derfor utviklet og godkjent et nytt beredskapssystem, det såkalte *NATO Crisis Response System (NCRS)*. En viktig hensikt med NCRS er å oppnå en tettere militær/sivil integrasjon og en lavere terskel for bruk av systemet.

[25] NOU 2000:24 *Et sårbart samfunn*. Rapport fra evalueringsutvalget for flodbølgekatastrofen i Sør-Asia 2005. 26/12; St.meld. nr. 37 (2004-2005) *Flodbølgekatastrofen i Sør-Asia og sentral krisehåndtering*.

[26] St.meld. nr. 17 (2001-2002) *Samfunnssikkerhet*. Kapittel 3.4

[27] St.meld. nr. 17 (2001-2002) *Samfunnssikkerhet*. Kapittel 3.4.

[28] Omtalen av det nasjonale beredskapssystem er basert på et ugradert innspill fra DSB.

Nasjonene i NATO, inklusive Norge, har revidert og utviklet nasjonale systemer parallelt med at NATO utviklet sitt. Nytt nasjonalt beredskapssystem ble fastsatt gjennom kgl. res. av 29. april 2005, og erstatter det gamle systemet som dermed settes ut av kraft.

Beredskapssystemet for Forsvaret (BFF) og Sivilt Beredskapssystem (SBS) utgjør det Nasjonale beredskapssystem (NBS) som igjen er harmonisert med NCRS.

Det nasjonale beredskapssystemet er et krisehåndteringsverktøy for Regjeringen og skal tilrettelegge for, gjennom forhåndsplanlagte tiltak/handlemåter, å forebygge eller redusere skadeomfanget ved kriser, som for eksempel naturkatastrofer og terroranslag eller ved krig. Bruk av systemet er særlig aktuelt når det er et koordineringsbehov på tvers av normale ansvarslinjer, eller når det er behov for særlig hjemmelsgrunnlag for å iverksette tiltak.

BFF og SBS er prinsipielt forskjellig idet BFF gjelder for ett departement (FD) med ansvarsfordeling også på lavere nivå, mens SBS gjelder for alle de øvrige departementer med ansvarsfordeling på departementsnivå. Systemet er planleggingsgrunnlag for relevante beredskapsplaner hos underliggende etater/virksomheter, slik at tiltak som blir iverksatt i det nasjonale beredskapssystemet kan gjennomføres. Den enkelte tiltakseier er ansvarlig for at dette blir fulgt opp.

Beredskapssystemet inneholder konkrete beredskapstiltak som kan iverksettes, enten ved kgl.res. eller av ansvarlig statsråd. Systemet er tilrettelagt for rask iverksetting av de enkelte tiltak.

Dersom et tiltak blir iverksatt av NATO, velger nasjonene selv om de vil iverksette dette nasjonalt. Når NATO iverksetter tiltak, antas det å være et press på nasjonene til også å gjøre det samme, men enkeltnasjoner kan også hindre NATO i å erklære tiltak på grunn av krav til konsensus (konsensusprinsippet sikrer stor nasjonal kontroll).

Systemet kan iverksettes nasjonalt uavhengig av NATO. Det kan være særlig hensiktsmessig å iverksette forberedende tiltak også ved lavt krisenivå.

FD har ansvar for forvaltning av BFF. DSB forvalter SBS på vegne av JD, og utfører alle oppgaver knyttet til systemet for dem.

Bruk av systemet vil bli øvet gjennom den årlige NATO-øvelsen CMX (Crisis Management Exercise).

NorCERT/VDI

NSM har det operative ansvaret for forebyggende IKT-sikkerhet i nasjonal kritisk infrastruktur og for håndtering av sikkerhetstruende hendelser. VDI (Varslingssystem for Digital Infrastruktur) og NorCERT (*Norwegian Computer Emergency Response Team - CERT*) er nasjonalt senter for varsling og håndtering av alvorlige angrep mot eller fra norske datamaskiner og nettverk. Senterets målgruppe er virksomheter med kritisk infrastruktur og kritiske samfunnsfunksjoner i offentlig og privat sektor.

VDI er et varslingssystem som identifiserer, sammenstiller og varsler om trusler og angrep mot datanettverk i Norge. NorCERT ivaretar forebyggende tiltak for effektiv hendelseshåndtering, varsling, rådgivning, assistanse ved og håndtering av sikkerhetshendelser og analyse og trusselvurdering for kritisk infrastruktur. VDI og NorCERT er basert på et nært samarbeid mellom myndighetene, private bedrifter og offentlige etater og er det nasjonale kontaktpunkt for tilsvarende nasjonale koordineringsenheter for varsling og rådgivning i utlandet.

NorCERT vil ha en sentral rolle i en beredskapssituasjon. NorCERT bistår relevante sektormyndigheter i forbindelse med iverksettelse av nasjonale beredskapstiltak på informasjonssikkerhetsområdet. Det forutsettes at det er en direkte linje mellom NorCERT og den eller de sektormyndigheter som har ansvar for de aktuelle tiltak i det sivile beredskapssystemet.

Varsling av befolkningen

En viktig del av myndighetenes beredskap er umiddelbar varsling av befolkningen ved akutt fare. Det primære verktøyet er bruk av Sivilforsvarets tyfonanlegg sammen med beredskapskanalen NRK P1 over FM-nettet.

Behovet for varsling over tyfonanlegg og radio oppstod i en annen sikkerhetspolitisk virkelighet enn dagens. Nye risikoområder knyttet til et sårbart samfunn og fremveksten av terrorisme rettet mot vestlige interesser gjør likevel at behovet er like stort i dag. Behov for varsling av befolkningen kan oppstå ved spredning av giftig gass, forurenset drikkevann, dambrudd, eksplosjonsfare, terroraksjoner, flom og lignende hvor hurtig og korrekt informasjon til et stort antall mennesker er avgjørende. Signalet VIKTIG MELDING – LYTT PÅ RADIO er blitt benyttet i nyere tid. Blant annet under gassulykken på Lillestrøm 5. april 2000 da signalet ble sendt lokalt og politimesteren gikk ut med evakueringsordre på radio. Ordningen prøves fire ganger per år ved at NRK sender informasjon når tyfonanleggene prøves.

Bruken av NRK til å varsle befolkningen/sende melding fra Statsmyndighet er hjemlet i *Lov om kringkasting (lov 1992-12-04 nr 127) § 2-4.* NRKs

beredskapsansvar er dels regulert av *Forskrift om virksomheten i Norsk rikskringkasting under beredskap og krig*, fastsatt ved kgl.res. av 6. oktober 1989. NRK er også pålagt ansvar knyttet til Regjeringens presse- og informasjonstjeneste (RPI) hos Statsministerens kontor (SMK) gjennom forskrift og avtaler mellom NRK og SMK.

Det er videre inngått avtale mellom Justis- og politidepartementet, NRK, Telenor, Norkring og Norsk Lokalradioforbund: *Samarbeid om lokalradiostasjoners virksomhet under kriser og katastrofer* av 31.12.01 (Lokalradioavtalen). Avtalen sikrer at utpekte lokalradiostasjoner ved behov videreformidler NRK P1 under kriser og katastrofer. Det er fylkesmann eller politimester som definerer når en slik situasjon foreligger og som varsler avtalepartene om dette.

NRK er organisert som et aksjeselskap med statsråden i Kultur- og kirkedepartementet (KKD) som generalforsamling. KKD forvalter eierinteresser i NRK. KKD fordeler beredskapsmidler til allmennkringkastere. Midlene er de siste årene delt mellom NRK og TV2.

Det er fremmet forslag fra enkelte kringkastere om å avvikle dagens FM-nett i 2014 og erstatte det med et nytt digitalt bakkenett for radio – DAB (*Digital Audio Broadcasting*).[29] I løpet av 2006 skal det nye bakkenettet dekke 80 % av landet. Politiske myndigheter har ikke tatt endelig beslutning om slukking av FM-nettet.

Varsling over fast- og mobiltelefon

Direktoratet for samfunnssikkerhet og beredskap (DSB) har utført en test av befolkningsvarsling ved hjelp av talemelding på fasttelefon. Resultatet av testen var vellykket, men systemet har sine begrensninger ved at det ikke når alle. Direktoratet ser i tillegg på mulighetene med bruk av *cell broadcasting*, et system som varsler alle mobiltelefoner som oppholder seg innenfor et gitt geografisk område. Teknologien som dette bygger på er lite utsatt for kapasitetsbegrensninger i mobilnettet.

Internett som informasjonskanal til befolkningen

Internett er en viktig informasjonskanal ved større hendelser som berører mange. Eksempelvis øker nettavisenes besøkstall dramatisk ved større hendelser. Erfaringer har ført til at de store nettavisene har god kapasitet.

Ulike myndigheter har egne nettsteder til informasjonsspredning, men mange mangler planer for bruk ved kriser. Erfaringsmessig slutter også mange nettsteder å fungere ved stor oppmerksomhet hvis dette ikke er forberedt på forhånd. Norske myndigheter mangler per i dag et eget dedikert nettsted med samordnet informasjon som er i stand til å håndtere mye trafikk på en sikker måte. Gjennom St.meld. nr. 39 (2002-2003) *Samfunnssikkerhet og sivilt-militært samarbeid*, åpnet Regjeringen Bondevik II opp for å etablere en internettside som en kanal for offentlig informasjon om pågående kriser og generell beredskapsinformasjon. DSB er gjennom Justisdepartementets tildelingsbrev for 2006, utpekt til å etablere denne nettportalen som skal fungere som et samordnet nettsted på tvers av alle virksomheter med beredskapsansvar for å supplere og understøtte deres informasjonsformidling knyttet til beredskapsspørsmål og som informasjonskanal under kriser.

11.6.3 Regional kriseledelse og regionalt sikkerhetsarbeid

Fylkesmannen har et tverrsektorielt og geografisk områdeansvar for samfunnssikkerheten i sitt fylke. Fylkesmannsembetene ivaretar en rekke sikkerhets- og beredskapsoppgaver på vegne av departementene og DSB. Fylkesmennene samordner og fører tilsyn med beredskapsplanleggingen i fylket, inkludert i kommunene, og støtter opp under kommunenes beredskapsarbeid. Dette gjelder blant annet utarbeidelse av kommunale risiko- og sårbarhetsanalyser, beredskapsplaner, øvelser og ivaretakelse av sikkerhetshensyn i den ordinære samfunnsplanleggingen. Mange fylkesmenn har også gjennomført en risiko- og sårbarhetsanalyse på fylkesnivå. Fylkesmennene er også ansvarlig for det sivil-militære samarbeidet i fylket. Ved omfattende krisesituasjoner er Fylkesmannen gitt en samlende og koordinerende rolle i forhold til den statlige oppfølgingen av krisehåndteringen på regionalt nivå, jf. kgl. res. av 12. desember 1997. Fylkesmannen har også et særskilt ansvar for planmessig koordinering i tilfelle atomulykke, jf. kgl. res. av 26. juni 1998. Fylkesmannen disponerer et fylkesberedskapsråd og en stab til støtte for planlegging av beredskapstiltak og utøvelse av krisehåndtering. Relevante myndigheter og virksomheter som representerer en rekke samfunnssektorer er representert i dette rådet.

Ansvarsdelingen mellom politiet og Fylkesmannen følger normalt ansvarsprinsippet. I hen-

[29] Innstilling fra arbeidsgruppe oppnevnt av Kultur- og kirkedepartementet (via Medietilsynet) for vurdering av videre utbygging, rammevilkår og modeller for digital radio (DAB) 2005. *Digitalradio i Norge.*

hold til politilovens § 27 tredje ledd, kan politiet iverksette nødvendige koordinerte tiltak for å sikre liv og helse inntil vedkommende myndighet (kommune, statsetat osv.) har kontroll igjen over eget ansvarsområde. Andre sivile myndigheter har imidlertid ansvar for beredskap og krisehåndtering innen eget område i situasjoner hvor liv og helse ikke er truet og eventuelt i krisefaser etter at redningsinnsats er avsluttet.

11.6.4 Lokal kriseledelse og lokalt sikkerhetsarbeid

Kommunene representerer et sentralt offentlig element som sammen med andre lokale offentlige aktører, private bedrifter, lag og foreninger bidrar til å gjøre samfunnet robust. I tillegg har kommunen ressurser for å følge opp de som på en eller annen måte blir rammet av en krise.

Kommunenes mest sentrale roller kan beskrives som myndighet, som tjenesteyter og som samfunnsaktør. Alt dette gjør kommunen til en svært viktig del av samfunnet.

11.6.4.1 Kommunen som myndighet

Kommunen er planmyndighet innenfor hele kommunens territorium og er selv arealforvalter for deler av det. Kommunens bidrag til å forebygge mot skader gjennom god planlegging mot forhold som fjell-, leire-, snø- og jordskred og skadeflom er derfor viktig. Kommunene har etter bestemmelsene i plan- og bygningsloven ansvar for å sikre en forsvarlig bruk og vern av arealer og bygninger innenfor kommunens grenser. Kommunene har videre en selvstendig undersøkelsesplikt med hensyn til farer både ved utarbeidelse av arealplaner og ved vurdering av dele- og byggetillatelser. Risikoområder eller potensielle fareområder må undergis en spesiell vurdering i arealplanleggingen. Hvis det er grunn til å tro at et område kan være utsatt for en naturbetinget fare, må kommunen påse at det er innhentet tilstrekkelig fagkyndige uttalelser om faren før plan vedtas. Eventuelt må det foretas ekspertundersøkelse av faren.

Risiko- og sårbarhetsanalyser på generell basis er et viktig verktøy for kommunene, men det er per i dag ikke noen lovfestet plikt for kommunen til å lage slike. De aller fleste kommuner har likevel gjort slike analyser, men med varierende kvalitet. Slike analyser vil bidra til at kommunene kan forebygge og håndtere kriser og større ulykker, og til at det ikke blir bygd inn ny eller økt sårbarhet i samfunnet.

11.6.4.2 Kommunen som tjenesteyter

Kommunen har stor mulighet til å påvirke lokalsamfunnets robusthet gjennom sitt eget apparat for tjenesteproduksjon (eventuelt gjennom krav til andre som yter tjenesten ved privatisering/konkurranseutsetting), til sine institusjoner og anlegg. Ikke minst gjelder dette dersom kommunen utnytter mulighetene for samordning tjenestene imellom. Kommunenes tjenester er pålagt i henhold til lover og forskrifter eller de er selvvalgt. Helsetjenester, undervisning, brannvern, pleie- og omsorgstjenester er i stor grad lovpålagte. Særlover gir innbyggere rettigheter til slike tjenester, som dessuten søkes standardisert eller kvalitetssikret gjennom minstestandarder. Tjenestene innenfor kultur og næringsutvikling er derimot stort sett selvpålagte og lite regulert. For tekniske tjenester som vann, avløp, brann- og redningsinnsats og renovasjon gjelder forskrifter som skal sikre kvalitet og hindre uønskede effekter for omgivelsene.

Kommunene leverer drikkevann til innbyggerne, enten direkte selv eller gjennom kommunalt eller interkommunalt eide selskaper. Kommunen er distributør av kraft gjennom lokale nettselskaper, kraft som i visse tilfeller også er lokalt produsert. Kommunene er ansvarlige for primærhelsetjenesten, barnehager og grunnskole og har et omfattende pleie- og omsorgsapparat. Etter bestemmelsene i brann- og eksplosjonsvernloven har kommunene plikt til å etablere og drifte et brannvesen. Kommunen skal gjennomføre en risiko- og sårbarhetsanalyse som skal sørge for at brannvesenet blir best mulig tilpasset de oppgaver det kan bli stilt overfor. Loven legger i tillegg føringer for kommunene når det gjelder lokalt og regionalt samarbeide slik at de samlede forebyggende beredskapsmessige ressurser utnyttes best mulig. Helseberedskapsloven pålegger kommunene å ha en kriseplan for sosial- og helsemessig beredskap. Kravet til beredskapsplan gjelder kommunene, fylkeskommunene og staten ved de regionale helseforetakene for de helse- og sosialtjenestene de skal sørge for et tilbud av, eller er ansvarlig for. Beredskapsplanen skal også omfatte tjenester som etter lov eller avtale tilbys av private virksomheter som en del av de respektive tjenestene.

11.6.4.3 Kommunen som samfunnsaktør

Kommunen er et viktig element i det demokratiske Norge. Som politisk organ kan kommunen ta opp nær sagt hvilket som helst aspekt kommunen måtte ønske. De folkevalgte er et talerør for befolkningen og vil kunne ha påvirkningskraft helt opp i de nasjonale besluttende organer. Kommunene

forvalter lover og forskrifter, har hovedansvar for utviklingen av samfunnet innenfor kommunens areal, er ofte den største arbeidsplassen innenfor kommunen og besitter unik lokalkunnskap.

Kommunen kan utnytte sin posisjon til å påvirke private aktører til å innarbeide tilsvarende hensyn i deres planlegging og virksomhet. At kommunen har en sentral rolle fratar ikke andre aktører for deres medansvar. Ved å samarbeide med offentlige organer på andre nivåer kan kommunen dessuten bidra til er mer effektiv samlet offentlig innsats på dette feltet.

Kommunens politiske og administrative ledelse kan fungere som pådriver overfor aktører de i utgangspunktet ikke har mulighet for å styre eller gi rammer overfor. Eksempler på slike aktører er næringslivet, frivillige- og interesseorganisasjoner, fylkeskommunale organer eller statlige institusjoner. Juridisk sett har kommunen da samme posisjon og status som enhver annen organisasjon eller bedrift som ønsker å påvirke andre organisasjoner eller bedrifter. Det må skje gjennom frivillig samarbeid, gjensidige avtaler, forhandlinger o.l. Kommunen som grunneier eller skogeier innehar ikke andre rettigheter enn enhver annen grunneier eller skogeier. Samtidig vil kommunen ut fra sin spesielle karakter kunne oppfattes som en spesielt viktig og betydningsfull aktør, fordi den i mange sammenhenger også innehar myndighetsroller.

11.6.4.4 Kommunens rolle ved kriser

En del av kommunens rolle som samfunnsaktør er å være kriseleder. Denne rollen er annerledes fra det å være rednings- eller skadestedsleder, noe som er et HRS/politiansvar. Kommunen vil alltid ha en lokal (kriseleder)rolle enten krisen berører innbyggerne direkte eller indirekte.

I utgangspunktet vil det være kommunens ordinære ledelse som også fungerer som kriseledelse. Ordføreren og rådmannen avklarer seg i mellom hvem av dem som skal ha kriseledelsen og hvem som skal være talsperson i forhold til mediene. Publikum og media forventer at øverste leder står frem og gir krisen et ansikt. I en kommune er det naturlig at ordføreren tar denne rollen. Viktigheten av lederrollen som ordføreren i en kommune har, skal ikke undervurderes i en krise. Under Tsunamikatastrofen var alle landets ordførere varslet og forberedte på å ta imot og ta hånd om både skadde, døde og pårørende da de kom hjem.

Kommunens rolle ved krise, for eksempel et langvarig strømutfall i en kuldeperiode, vil også kunne være å håndtere utfordringer innenfor egen tjenesteyting, slik som for eksempel sterkt pleietrengende eldre eller andre sterkt pleietrengende brukere representerer når deler av kritisk infrastruktur faller ut.

Kommunens ressurser vil kunne brukes aktivt, for eksempel med bruk av bygninger, pleiepersonell, lærerer osv. for å bidra i håndteringen av en krise og i gjenopprettingen etter selve krisen. Hvis krisen ikke skjer i eller i nærheten av kommunens territorium, kan skolene eller andre institusjoner brukes som del av pårørendehåndtering, sorgarbeid osv.

11.6.4.5 Kriseforebyggende arbeid og beredskap i kommunene

Det følger av nærhetsprinsippet og administrativ forvaltningspraksis at kommunene har et ansvar for sikkerhet og beredskap på det lokale nivå. Det fremgår imidlertid av St.meld. nr. 25 (1997-98) at det kommunale beredskap skal styrkes ved at Justis- og politidepartementet skal utrede grunnlaget for en sektorovergripende kommunal beredskapsplikt. En slik generell beredskapsplikt er senere anbefalt av sårbarhetsutvalget. Forslaget er vurdert og behandlet i St.meld. nr. 17 (2001-2002) Samfunnssikkerhet og Regjeringens (Bondevik II). Konklusjon er at en slik plikt skal innføres. Det fremgår av St.prp. nr. 1 (2004-2005) at innføringen av en slik plikt blir sett i sammenheng med ny lov om Sivilforsvaret.[30]

Risiko og sårbarhetsanalyser i kommunene danner grunnlaget for kriseplaner. ROS-analysene danner også grunnlaget for kommunenes innsatsapparat gjennom brann- og redningsetaten. Systematisk samfunnssikkerhets- og beredskapsarbeid handler om tiltak for å forebygge og effektivt kunne håndtere hendelser og situasjoner som truer liv, helse, miljø og viktige samfunnsverdier og krever ekstraordinær innsats. Kommunene takler til daglig uønskede hendelser.

Kommunen må være forberedt på blant annet disse oppgavene ved en krisesituasjon:

- ta hånd om skadde personer
- yte bistand ved evakuering
- innkvartering og forpleining
- forpleining til uføre som ikke har anledning til å forlate hjemmet
- forsyningsstøtte til redningsmannskaper
- informasjon til pårørende, befolkningen og media
- sikre helsemessig trygge næringsmidler inklusiv drikkevann
- sikre nødstrøm ved strømstans

[30] St.prp. nr. 1 (2004-2005) for Justis- og politidepartementet, side 135.

– gjennomføre regulerings- og rasjoneringstiltak
– rette opp skader på kommunikasjoner og andre anlegg
– rydde et skadested og yte en innsats for å beskytte miljøet
– verne kulturelle verdier

Innenfor den enkelte fagsektor eller virksomhet kan det være behov for egne kriseplaner eller nødprosedyrer. Dette gjelder blant annet for evakuering, helseberedskap, brann og redning, sikker vannforsyning, akutt forurensning, smittevern, nødstrøm, nødkommunikasjon, vern om kulturelle verdier og for å reparere skadet infrastruktur.

Kommunen har selv eller i samarbeid med nabokommunene en egen brann- og redningsetat som er bemannet, trent og utrustet til å takle et bredt spekter av små og store hendelser.

Mange kommuner har tekniske ressurser som er av viktighet for krisehåndtering. Teknisk etat har mange steder en omfattende maskinpark som kan brukes i en del krisesituasjoner innen eller i umiddelbar nærhet av kommunens territorium. Kommunens egne bygningsmasse som rådhus, skoler, helseinstitusjoner, pleie- og omsorgssentra, bygninger for tekniske installasjoner og lagre kan brukes til mange formål under og etter en krise, og må således ses på som viktige lokale ressurser. En del av dem har også tilfluktsrom.

Gjennom ansvaret for barnehager og grunnskolen, primærhelsetjenesten, pleie- og omsorgstjenesten for pleietrengende eldre og andre brukere samt barnevernet, har kommunene et omfattende apparat som også kan brukes under kriser. Den omfattende vektleggingen av omsorg i den kommunale oppgaveportefølje bør gjøre den godt trent til også å yte viktige og nødvendige bidrag i forbindelse med en krise.

Kommunen er i posisjon til å trekke på og koordinere lokale frivillige ressurser. Gjennom den daglige kontakt kommunen har med disse grupper og gjennom det aktive arbeid som drives for å få offentlige og private ressurser til å virke sammen under diverse arrangementer, gjør at det under kriser vil være legitimt og lett å få frivillige ressurser til å virke sammen med kommunens.

Kommunen er en viktig informasjonsformidler om situasjon og behov som skal formidles oppover i det offentlige hierarkiet. Først og fremst er kontakten mot Fylkesmannen og dermed samordningskanalen til DSB svært viktig. Fagkanalene for helse og for skole er svært viktige i forhold til informasjonsformidling begge veier.

11.6.5 Utvalgets vurderinger og anbefalinger

Erfaringer fra alvorlige krisesituasjoner i den senere tid, blant annet tsunamien i Sør-Asia, terrorangrepene i Madrid og London og orkanen Katrina, synliggjør viktigheten av at kriseledelsessystemet er organisert og innrettet på en slik måte at krisesituasjoner kan håndteres effektivt. Foruten samfunnets robusthet, er et effektivt kriseledelsessystem den viktigste forutsetningen for at normalsituasjonen blir gjenopprettet raskt etter en krise. Det er en klar forventning i samfunnet til at myndighetene ivaretar dette på en så god måte som mulig.

Det er ikke mulig å forutse og forhindre alle typer trusler som materialiserer seg. Uansett hvor godt sikkerhet og robusthet er ivaretatt, må det påregnes at det kan oppstå situasjoner med svikt eller ødeleggelse i kritisk infrastruktur og kritiske samfunnsfunksjoner.

Det følger av dette at det til enhver tid er behov for en effektiv beredskap og et effektivt apparat for å lede krisehåndteringen. Ettersom større kriser inntreffer relativt sjelden og ofte uten forvarsel, er det en utfordring å sikre at de ansvarlige aktørene til enhver tid ivaretar sine oppgaver og ressurser på en tilfredsstillende måte. Det er derfor viktig at kriseledelsesapparatet er tilstrekkelig utstyrt, øvet og opplært til å håndtere de situasjoner som måtte oppstå. Dette gjelder kriseledelsesapparatet på alle nivåer, fra strategisk til operativt nivå.

På sentralt nivå er det etablert en rekke organer med roller og ansvar i krisesituasjoner knyttet til forskjellige scenarier. Det synes å være en tendens til at kriseledelsessystemet omorganiseres i etterkant av nasjonale krisesituasjoner. Det ble gjort etter storflommen på Østlandet i 1995, terrorangrepene i USA i 2001 og tsunamien i Sør-Asia i 2004. Dette kan skyldes at de rådgivende og operative organene som inngår i ledelsesapparatet mister fokus og blir innaktive etter en tid. En annen forklaring kan være at organenes mandat er avgrenset til spesifikke scenarioer og således ikke er fleksible nok til å omfatte alle typer krisesituasjoner. Det synes uansett å være en utfordring å ivareta de strukturer som er etablert samtidig som behovet for fleksibilitet ivaretas.

11.6.5.1 Forslag knyttet til kriseledelsesapparatet

Utvalget anbefaler:

1. Innrettingen og prioriteringen av kriseledelsesapparatet må ikke nedprioriteres som følge av at det går lang tid mellom det inntreffer kriser av nasjonal størrelse. Prioriteringen og innret-

tingen av det nasjonale kriseledelsesapparatet bør derfor opprettholdes til enhver tid.
2. Kriseledelsesapparatet må være tilstrekkelig fleksibelt organisert til å kunne håndtere alle typer scenarioer som kan oppstå. Det bør ikke være slik at det sentrale kriseledelsesapparatet organiseres ulikt avhengig av situasjonen (unntatt i tilfelle krig). Dette tilsier at forholdet mellom Regjeringens kriseråd og andre organer som eventuelt skal tre i funksjon under kriser avklares.
3. Krisestøtteenheten bør gis meningsfylte oppgaver i det daglige som ivaretar og styrker kompetansen knyttet til nasjonal kriseledelse. Dette kan være oppgaver knyttet til nasjonale og internasjonale nettverk for kriseledelse. Oppgaver som i dag ligger hos myndigheter og som knytter seg til nasjonal kriseledelse bør vurderes i sammenheng med konkretiseringen av oppgaveporteføljen til Regjeringens krisestøtteenhet. Utvalget ser at dette kan gjøres ved hospiteringsordninger.
4. Det må være gode og etablerte rutiner for overføring av lederansvaret mellom fagdepartementene og Justis- og politidepartementet i tilfelle kompliserte kriser. I størst mulig grad bør det på grunnlag av aktuelle krisescenarier defineres hvem som peker seg ut som lederdepartement. Dette bør kunne avklares gjennom en kombinasjon av analyser, tilsyn og øvelser og forankres i en oppdatert nasjonal beredskapsplan for ekstraordinære påkjenninger mot samfunnet.
5. Ved større kriser er det behov for en samordnet håndtering på tvers av ansvarslinjene. Dette forutsetter at også planverket er koordinert. Utvalget vil peke på at det er behov for å uniformere departementenes planverk bedre enn i dag.
6. Fylkesmannsembetenes vaktberedskap og ansvar innenfor krisehåndtering bør tydeliggjøres, blant annet når det gjelder rekvirering av ressurser og i forhold til å komme frem til gode prioriteringer mellom ulike brukere ved avbrudd i kritisk infrastruktur.
7. Prioriterte deler av forvaltningen må gis tidsmessige og funksjonelle graderte samband i sine krisehåndteringslokaler som tillater sikker kommunikasjon på nivå til og med HEMMELIG. Det må forutsettes at sambandssystemene baseres på en teknologisk plattform som tillater at de kan kommunisere med hverandre sømløst.
8. Det må gjennomføres regelmessige øvelser for å teste og videreutvikle den nasjonale kriseberedskapen i forhold til mulige infrastrukturkriser. Øvelsene må følges opp med gode evalueringer og kontinuerlige tilpasninger og forbedringer i planverk og andre tiltak. Det bør i den sammenheng tilstrebes å benytte SBS/BFF-planverket som en del av øvelsene der det er relevant.
9. Kommunene må få en generell beredskapsplikt.

11.6.5.2 Forslag knyttet til trossamfunnenes rolle i forebygging og håndtering av kriser

De ulike trossamfunnene i Norge utgjør en plattform for å bygge bro og skape forståelse mellom ulike kulturer og trosretninger. Usikkerhet om det som oppleves som fremmed, kan avklares med kunnskap og samarbeid. Trossamfunnene utgjør derfor en plattform hvor mistenksomhet og uro kan reduseres og forebygges.

Menneskers religiøse tilknytning spiller en rolle i forhold til dagens trusselbilde ved at enkelte grupper legitimerer og utfører terrorhandlinger ut fra sin religion. Det understreker viktigheten av at også trossamfunn er med på å diskutere relevante løsninger på slike utfordringer.

Mange mennesker søker til sitt trossamfunn ved kriser, og trossamfunnene utgjør derfor en ressurs for disse personene når kriser skal håndteres. Dialog mellom myndigheter og ulike trossamfunn er på denne måten et relevant verktøy for å håndtere kriser.

Utvalget mener med dette som bakgrunn at det bør opprettes et permanent rådgivende utvalg med bånd til Justis- og politidepartementet. Det vil bidra til å dra nytte av de ressursene som finnes i de ulike trossamfunnene, og det vil virke inkluderende. Et slikt rådgivende utvalg bør ha det følgende som oppgaver:

- gi myndighetene råd om hvordan usikkerhet og mistenksomhet mot eller mellom ulike trossamfunn kan håndteres, i forbindelse med kriser der norske interesser er involvert
- gi myndighetene råd om hvordan religiøs ekstremisme kan forebygges og håndteres
- gi myndighetene råd om hvordan de ulike trossamfunnene kan bidra i det psykososiale arbeidet etter en krise

Utvalget understreker betydningen av at et permanent rådgivende utvalg får tid til å utvikle en felles plattform som grunnlag for samarbeidet. Utvalget ønsker også å understreke betydningen av at et permanent rådgivende utvalg blir representativt sammensatt av ulike trosretninger i Norge. Som et

første skritt foreslås etablert en arbeidsgruppe bestående av representanter for noen sentrale trossamfunn. Det foreslås at arbeidsgruppens oppgave skal være å utarbeide retningslinjene og grunnlaget for utvalget.

11.6.5.3 Forslag knyttet til varsling av befolkningen

NRK har en beredskapsmessig viktig funksjon som formidler av myndighetenes informasjon ved nasjonale kriser og katastrofer. NRK P1 er utpekt som beredskapskanal. P1 dekker hele landet, og er sammen med Sivilforsvarets tyfonanlegg den beste plattformen for å nå ut hurtig både lokalt, regionalt og nasjonalt. Utvalget merker seg at avtaler mellom ulike myndigheter og NRK ble gjort innenfor rammen av den kalde krigen. Utvalget anbefaler følgende:

1. At avtaler og innretting tilpasses dagens sikkerhets- og beredskapsmessige utfordringer. Utvalget anbefaler i den sammenheng at rollene til SMK, KKD, JD og andre myndigheter ses i sammenheng og revideres.
2. Utvalget anbefaler at KKDs midler avsatt til informasjonsberedskap til mediabedrifter gjennomgås for på mest mulig effektiv måte å styrke beredskapsinnsatsen hos mediene.
3. Utvalget anbefaler at FM-sendenettet kun kan slukkes når et nytt digitalt bakkenett for radio har en like god dekning som dagens sendenett. Det må være klart at varslingsfunksjonen som er tilagt NRK P1 videreføres i DAB-nettet.

Kapittel 12
Beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner i andre land

Den internasjonale betegnelsen på arbeidet med beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner er *Critical Infrastructure Protection (CIP)*. Det skilles således ikke mellom begrepene kritisk infrastruktur og kritiske samfunnsfunksjoner. I dette kapittelet brukes derfor begrepet kritisk infrastruktur som en samlebetegnelse. Utvalget har besøkt relevante myndigheter i Canada, USA, Storbritannia, Tyskland, Nederland, Sverige, Sveits og Singapore. Besøkene har gitt verdifulle innspill til utvalgets arbeid. I dette kapittelet redegjøres det for arbeidet som pågår i de nevnte landene.[1]

Samtlige land baserer arbeidet med sikring av kritisk infrastruktur på ansvarsprinsippet og nærhetsprinsippet. Det er imidlertid variasjoner mellom landene i forhold til hvilken organisasjon som har et overordnet koordinerende ansvar for beskyttelse av kritisk infrastruktur. Det finnes således eksempler på at det koordinerende ansvaret ligger til Forsvarsdepartementet, Sikkerhetsdepartementet, Innenriksdepartementet osv. Et annet generelt trekk er at landene tilnærmer seg beskyttelse av kritisk infrastruktur i forhold til både villede og ikke-villede uønskede hendelser, også omtalt som en *all-hazards approach,* selv om landene naturlig nok prioriterer forskjellige sider av trusselbildet med bakgrunn i konkrete sikkerhetshendelser eller trusler om slike hendelser.

De fleste land er enige om at definisjonen av kritisk infrastruktur skal benyttes for å angi retningen for arbeidet med beskyttelse av kritisk infrastruktur, og at det ikke er avgjørende å ha en perfekt definisjon av begrepet kritisk infrastruktur. Selv om det er variasjoner i landenes definisjoner av kritisk infrastruktur, er målsetningen med arbeidet felles for alle land; beskyttelse av kritisk infrastruktur skal ivareta samfunnets funksjonsdyktighet. På ulike måter definerer derfor landene begrepet kritisk infrastruktur som de objekter, systemer, tjenester og ressurser som samfunnet ikke klarer seg uten. Samtidig erkjennes det at definisjonen av dette begrepet må være dynamisk slik at den kan endres dersom det anses hensiktsmessig.

Det er små forskjeller i hvilke sektorer med kritisk infrastruktur de ulike landene identifiserer. Forskjellene kan skyldes særegenheter ved sårbarhetsbildet i disse landene, for eksempel sårbarheter knyttet til geografiske forhold, eller et ønske om å peke på at en sektor har betydning for rikets sikkerhet. Bruk av ulike metoder for kartlegging av kritisk infrastruktur, kan også være en årsak til forskjellene. Følgende sektorer er identifisert i alle landene utvalget har sett på: Energisektoren, elektronisk kommunikasjonsektoren, transportsektoren, finanssektoren, helsesektoren, og vannsektoren.

12.1 USA

I USA er ansvaret for å ivareta den overordnede nasjonale innsats for å samordne planleggingen og ansvarsforholdene knyttet til sikring av kritisk infrastruktur på føderalt, statlig og lokalt nivå samt innenfor privat sektor, lagt til *Department of Homeland Security.*

Homeland Security Presidential Directive, det såkalte HSPD-7, ble gitt 17. desember 2003. Direktivet etablerte en policy for føderale myndigheter knyttet til identifiseringen og prioriteringen av USAs kritiske infrastruktur og kritiske ressurser og beskyttelsen av disse mot terrorangrep. Direktivet pålegger de sektoransvarlige myndigheter å utarbeide planer for sikring av kritisk infrastruktur. DHS koordinerer dette arbeidet innenfor sine egne og 7 andre departementers områder.

DHS benytter følgende definisjon på kritisk infrastruktur, jf. *USA Patriot Act of 2001, section 1016(e)*:

> *Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national*

[1] Redegjørelsene i dette kapittelet er klarert med myndighetskontaktene i de landene som er besøkt.

economic security, national public health or safety, or any combination of those matters.

I tillegg brukes begrepet kritiske ressurser om:

Publicly or privately controlled resources essential to the minimal operations of the economy and government.

Eksempler på «kritiske ressurser» kan være dammer, kjernekraftverk, næringslivssentra, m.m.

I USA har man identifisert følgende kritisk infrastruktur sektorer[2]:

- Mat og landbruk
- Bank og finans
- Kjemisk og farlig materiale *(Chemical and hazardous materials*)
- Forsvarsindustri *(Defense industrial base)*
- Nød- og redningstjenester *(Emergency services)*
- Energi
- Monumenter og ikoner (bygninger av symbolverdi)
- Informasjonsteknologi og telekommunikasjon
- Post og shipping *(Postal and shipping)*
- Helsetjenester
- Transport
- Vann og avløp

I tillegg har man i USA identifisert følgende kritiske ressurser:

- Demninger
- Kjernekraftverk
- Offentlige bygninger *(Government facilities)*
- Næringsbygg *(Commercial Facilities)*

For å ivareta sitt koordineringsansvar har DHS laget en nasjonal plan for sikring av kritisk infrastruktur og kritiske ressurser i USA. Planen inkluderer mål, rammeverk og tiltak for sikring av kritisk infrastruktur, basert på presidentens nasjonale strategier [3] laget i 2003 og *Homeland Security Act of 2002*. Planen beskriver et rammeverk for å vurdere, og håndtere nasjonal risiko knyttet til kritiske infrastrukturer og kritiske ressurser som følger av terrorisme og andre katastrofescenarier. Det er lagt vekt på å beskrive nøkkelaktørers roller og ansvar for implementeringen av planen og systemet for koordinering og utveksling av informasjon. Denne nasjonale planen er dessuten samordnet med andre nasjonale planer, som for eksempel *National Response Plan*.[4]

I tiden etter etableringen av DHS (som var en følge av 11. september 2001), har det vært rettet spesielt fokus på å bygge opp DHS sine evner til å beskytte samfunnet mot terrorisme. For at arbeidet med å beskytte samfunnet skal kunne ivaretas på en helhetlig måte, har det vært viktig å integrere de nye aktivitetene knyttet til å beskytte samfunnet mot terrorisme med aktiviteter som beskytter samfunnet mot andre typer katastrofer, som for eksempel orkaner, jordskjelv osv. Flere av de tiltakene som kan tenkes iverksatt for å håndtere slike uønskede hendelser er like, uavhengig av katastrofens art, herunder de konsekvensreduserende tiltak.

Mange eiere og operatører innenfor de forskjellige samfunnssektorene har valgt å organisere seg i representative råd (*Sector Coordinating Councils*) hvor saker knyttet til sikkerhet tas opp på en samordnet måte. Som følge av dette har sektormyndighetene (*Sector-specific agencies*) som er utpekt gjennom *Homeland Security Presidential Directive 7 (HSPD-7)*, etablert tverretatlige koordinerende råd (*Government Coordinating Councils*) som kontaktpunkter til hver sektors SCC. Innenfor mange samfunnssektorer har det tidligere også blitt etablert private samarbeidsordninger for informasjonsdeling og analyse (*Information Sharing and Analysis Mechanisms*). I tillegg arbeides det for å etablere ordninger for informasjonsdeling mellom SCC og det såkalte *Homeland Security Information Network (HSIN)*, som er et informasjonsnettverk knyttet til DHS.

Utdannings- og forskningsinstitusjoner bidrar i vesentlig grad til arbeidet med det offentlige og private arbeidet knyttet til sikring av kritisk infrastruktur i USA. For eksempel har *George Mason University* ansvaret for det såkalte *Critical Infrastructure Protection Program*, som inkluderer omlag 40 universiteter, og som initierer både offentlige og private forsknings- og utviklingsaktiviteter knyttet til sikring av kritisk infrastruktur. Programmet er føderalt finansiert. *National Defense University*, er et militært universitet som utdanner statlig og lokalt ledelsespersonell innen «*homeland defense*». I det siste har DHS gitt flere universiteter tittelen *centers of excellence* knyttet til *food and bio-defense*. I USA finnes det for øvrig en rekke kompetansemiljøer som er uavhengige av det offentlige og som publiserer studier og anbefalinger knyttet til nasjonal sikkerhet, for eksempel *Heritage Foundation*.

[2] Opplyst til utvalget på møte med DHS i USA 2005.

[3] White House 2003. *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. February 2003; White House 2003. *The National Strategy to Secure Cyberspace*. February 2003.

[4] Department of Homeland Security 2004. *National Response Plan*. December 2004.

Nasjonal kriseledelse i USA[5]

I medhold av *Homeland Security Act of 2002* har *Secretary of Homeland Security* (sikkerhetsministeren), ansvaret for å koordinere føderal kriseledelse i USA uansett krisens art. Loven pålegger alle føderale myndigheter å bidra innenfor sitt ansvarsområde med alle tilgjengelige ressurser og støtte til krisehåndteringen under ledelse av den koordineringsansvarlige ministeren. *Departement of State* (Utenriksdepartementet) ivaretar koordineringen mot utlandet.

Som følge av dette har DHS bygget opp beredskapen mot terrorisme og andre katastrofer. DHS har ansvaret for å koordinere nasjonal kriseledelse i USA, og koordinerer den føderale innsatsen i tett kontakt med andre føderale myndigheter, statlige myndigheter, lokale myndigheter, ikke-statlige organisasjoner og private aktører. Det legges til grunn at alle krisesituasjoner har en lokalt forankring og alle innsatser som iverksettes som svar på slike hendelser må starte på lokalt nivå. Som det ble bekreftet under orkanen Katrina, må alle lokale myndigheter være forberedt til å kunne respondere på en hendelse de først 48-72 timene. Dersom en krise eskalerer og ikke kan håndteres av de ressurser og kapabiliteter som befinner seg innenfor en stat, kan den aktuelle guvernøren anmode om føderal støtte til kriseledelse. Flere stater i USA har etablert kriseplaner som er øvet, og hvor roller, ansvar og koordineringsrutiner er tydelige. De fleste av disse planene inkluderer planlegging og koordinering mot de som har ansvar for lokal infrastruktur.

Homeland Secruity Operations Center (HSOC) er det nasjonale operative senter for krisehåndtering på føderalt nivå, og frembringer informasjon og situasjonsoversikter av hendelser. HSOC er operativt 24 timer i døgnet, 7 dager i uken, og er bemannet med den nødvendige ekspertise fra ulike føderale, statlige og lokale offentlige organer. *National Response Coordination Center (NRCC)* inngår i HSOC og er det tverrsektorielle senter som står for den operative koordineringen av føderale innsatser. *Federal Emergency Management Agency (FEMA)* har ansvaret for NRCC. FEMA er en del av DHS.

På strategisk nivå ivaretas koordineringen gjennom *Interagency Incident Management Group (IIMG)* som er en bredt sammensatt gruppe bestående av berørte myndigheter. IIMG fungerer som rådgivende enhet for *Secretary of Homeland Security* under en nasjonal krise. Medlemmene av IIMG overvåker håndteringen av krisen og myndighetenes implementering av tiltak.

På regionalt nivå ivaretar et *Regional Response Coordination Center (RRCC)* krisehåndteringen.

12.2 Canada

I Canada er ansvaret for sikring av kritisk infrastruktur fordelt i henhold til ansvarsprinsippet. Samtidig ivaretar Canadas sikkerhetsdepartement, *Public Safety and Emergency Preparedness Canada (PSEPC)*, en koordinerende rolle. Fagdepartementene har egne strategier for sikring av kritisk infrastruktur som gjelder for den enkelte sektoren. Disse sektorstrategiene er basert på Canadas nasjonale sikkerhetspolicy (*Securing an Open Society*).

PSEPC har under utarbeidelse en nasjonal strategi for sikring av kritisk infrastruktur. I dette arbeidet konsulteres provinsene/territoriene, privat sektor og internasjonale partnere. Strategien vil også være kompatibel med den nasjonale informasjonssikkerhetsstrategien (*National Cyber Security Strategy*). Hovedmålet i strategien vil være at kritisk infrastruktur er tilstrekkelig robust, og dermed i stand til å sikre leveransen av kritiske varer og tjenester til befolkningen.

Canada benytter nå følgende definisjon av kritisk infrastruktur[6]:

> *National Critical Infrastructure refers to those physical and information technology facilities, networks, services and assets, that if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada.*

Det er identifisert 10 kritiske infrastruktursektorer i Canada[7]:

- Energi *(Energy and Utilities)*
- Informasjons- og kommunikasjonsteknologi
- Finans
- Helse
- Mat
- Vann
- Transport
- Offentlig sikkerhet *(Safety)*
- Sentraladministrasjonen *(Government)*
- Industri og produksjon *(Manufacturing)*

[5] Department of Homeland Security 2004. *National Response Plan.* December 2004; Utvalgets møte med DHS i USA 2005.

[6] Opplyst under utvalgets møte med PSEPC i Canada 2005.

[7] Opplyst under utvalgets møte med PSEPC i Canada 2005.

PSEPC har ansvaret for *National Critical Infrastructure Assurance Program (NCIAP)*, som er et offentlig/privat samarbeidsprogram med det formål å bidra til informasjonsdeling og til koordinering av tiltak for sikring av kritisk infrastruktur. Videre skal det bidra til å definere roller og ansvar mellom private virksomheter, myndighetene og andre aktører.

Arbeidet med sikring av kritisk infrastruktur tar utgangspunkt i et helhetlig perspektiv på sikkerhet og beredskap. I Canada kalles dette «*integrated risk management*», og består av både forebyggende og konsekvensreduserende tiltak. Det vektlegges at arbeidet med sikring av kritisk infrastruktur skal ivaretas både av den enkelte virksomhet, næringslivets bransjeorganisasjoner, provinsene/territoriene samt sentraladministrasjonen.

Nasjonal kriseledelse i Canada[8]

I hver canadisk provins og territorium er det etablert en *Emergency Management Organization (EMO)*. Dersom en krise eskalerer, og ikke kan håndteres på lokalt nivå, er det den regionale EMO som står for kriseledelsen.

I tråd med ansvarsprinsippet har det enkelte departement med underliggende virksomheter ansvar for å bistå EMOene ved behov, samt ivareta sitt myndighetsansvar ved nasjonale kriser.

Dersom en krise eskalerer, og ikke kan håndteres av EMO, rettes det en forespørsel fra den aktuelle EMO til PSEPC. Ved nasjonale kriser ivaretar PSEPC kontakten med de regionale og lokale krisestyringsapparater. PSEPC har dessuten oversikt over tilgjengelige rednings- og beredskapsressurser, herunder fagekspertise som kan kalles på ved ulike scenarioer.

PSEPC ivaretar sitt ansvar for nasjonal kriseledelse gjennom det nasjonale krisehåndteringssenteret *Government Operations Centre (GOC)*, som er lokalisert i Ottawa. Senteret er operativt 24 timer i døgnet, 7 dager i uken. GOC understøttes av beredskapspersonell fra relevante fagmyndigheter ved behov.

12.3 Sverige

I Sverige er arbeidet med sikring av kritisk infrastruktur (*samhällsviktiga infrastrukturen*) fordelt blant myndighetene i henhold til ansvarsprinsippet. Også kommunene har viktige oppgaver i dette arbeidet. Størstedelen av den kritiske infrastrukturen eies og drives av private virksomheter. *Krisberedskapsmyndigheten (KBM)* ivaretar en koordinerende rolle og et tverrsektorielt perspektiv på arbeidet. KBM er underlagt Forsvarsdepartementet.

KBM koordinerer til sammen 31 myndighetsorganer i Sverige som har et spesielt ansvar for å minske samfunnets sårbarhet og for å ivareta krisehåndteringsevnen. Myndighetsorganene er delt inn i 6 grupper, såkalte samarbeidsområder: *Teknisk infrastruktur, Transporter, Spridning av farliga ämnnen, Ekonomisk säkerhet, Områdesvis samordning, samverkan och information* og *Skydd, undsättning och vård*. KBM koordinerer også arbeidet opp mot kommuner, *länsstyrelser*, landsting og næringslivet.

KBM disponerer årlig om lag 1,8 mrd. SEK for arbeidet med å styrke kriseberedskapen i Sverige. En del av disse midlene brukes for å redusere sårbarheten i kritisk infrastruktur. Midlene fordeles på bakgrunn av risiko- og sårbarhetsanalyser og dialog mellom KBM og de aktuelle virksomheter. Kritisk infrastruktur i Sverige omfatter blant annet strømforsyning, telekommunikasjon, enkelte IT-systemer, kringkasting og forsyningssystemer som vann- og avløpssystem og fjernvarme. Også transport og viktige myndighetstjenester anses også som kritisk infrastruktur i Sverige. [9]

På oppdrag fra den svenske regjeringen, har KBM i 2005 påbegynt et arbeid med å definere nærmere hva som anses å være *samhällsviktig verksamhet* ut i fra et kriseberedskapsperspektiv. I utredningen foreslår KBM at dersom det oppstår en krise på grunn av at en virksomhet slutter å fungere og/eller om håndteringen av en pågående krise krever at en virksomhet fungerer, så bør den betraktes som *samhällsviktig*. For at en virksomhet skal fungere er den avhengig av ulike infrastrukturer som for eksempel veg-, el- og telenett. Utredningen er knyttet opp til den internasjonale diskusjonen om CIP (*critical infrastructure protection*) og kan bidra til å knytte sammen en rekke prosesser som relaterer seg til dette området. Den svenske tilnærmingen vil omfatte både villede og ikke villede hendelser.

I lys av energiforsyningens betydning for samfunnssikkerheten, fikk den svenske Energimyndigheten i 2001 i oppdrag å utvikle et helhetlig konsept for sikkerhet i den svenske energiforsyningen. Formålet med det såkalte HEL-prosjektet har vært å bidra til offentlig og privat samarbeid

[8] www.ocipep.gc.ca; Utvalgets møte med PSEPC i Canada 2005 og påfølgende dialog.

[9] Planeringsprocessen 2003:7. *Samhällets krisberedskap 2005. Planeringsinriktning.* Kriseberedskapsmyndigheten.

for å finansiere de tiltak som er nødvendig for å få tilfredsstillende sikkerhet på plass. Ved KBM gjennomføres nå et større prosjekt for å kartlegge og analysere viktige avhengighetsforhold mellom de kritiske infrastrukturene.

Regjeringen arbeider nå med en proposisjon till riksdagen om samfunnets sikkerhet og beredskap. Den skal etter planen være ferdig i mars 2006.

Nasjonal kriseledelse i Sverige[10]

Myndighetene som har det daglige ansvaret innenfor sine forvaltningsområder har også ansvar for å håndtere kriser som oppstår innenfor sitt fagområde, og beslutter selv organiseringen ved håndtering av krisesituasjoner. Samtidig er det forutsatt at berørte virksomheter skal samarbeide i tilfelle kriser. Kommunene, *Länsstyrelsene* og Regjeringen har i tillegg et ansvar for samordningen mellom de berørte aktører på henholdsvis lokalt, regionalt og sentralt nivå.

Ved tverrsektorielle kriser skal *Krisberedskapsmyndigheten (KBM)* avgi helhetlige situasjonsrapporter til Regjeringen og myndigheter som har ansvar for å håndtere krisen. Innhenting av informasjon for å utarbeide situasjonsrapportene skjer gjennom et nettverk bestående av *Länsstyrelser*, sentrale myndigheter og andre aktuelle aktører.

KBM har en egen »Situasjonssentral» som bemannes ved kriser. KBM kan også bistå kommuner, landsting og myndigheter i krisehåndtering, blant annet gjennom å gi råd og eksperthjelp i spørsmål knyttet til informasjonshåndtering, ledelsesmetodikk og teknisk støtte.

12.4 Tyskland

Det tyske *Bundesamt für Bevölkerungschutz und Katastrophenhilfe (BBK)*, er et nyopprettet direktorat underlagt det tyske føderale innenriksministeriet (BMI). BBK er det nasjonale kontaktpunkt for samfunnssikkerhet, med kapabiliteter innen beredskapsplanlegging, utdanning og rådgivning. BBK vurderer både villede og ikke-villede hendelser ved innrettingen av sikkerhets- og beredskapsarbeidet. Arbeidet er basert på en ny strategi for beskyttelse av sivilbefolkningen.

En av oppgavene som er tillagt BBK, er beskyttelse av kritisk infrastruktur i Tyskland. Dette ansvaret omfatter imidlertid ikke arbeidet for å sikre kritisk elektronisk kommunikasjon-infrastruktur, som koordineres av *Bundesamt für Sicherheit in der Informationatechnik (BSI)*.

Den tyske definisjonen av kritisk infrastruktur er:

> *Critical infrastructures (CI) include organizations and systems with tremendous importance for the society that, if disrupted, would have sustained influence on supply chains and public safety and could lead to further dramatic consequences.*[11]

Følgende sektorer er identifisert som kritiske infrastruktursektorer i Tyskland[12]:

- Energi
- Forsyning (vann, mat, helse og redningstjenester)
- Informasjonsteknologi og kommunikasjon (i samarbeid med BSI)
- Transport
- Farlig materiale *(Haz-mat)*
- Bank og finans
- Offentlige tjenester *(Government Services)*
- Andre kritiske infrastrukturer (media, forskningsinstitusjoner, nasjonale symboler)

BBK har prioritert arbeidet med å skaffe seg en oversikt over hva som finnes av viktig infrastruktur og kartlegge trusler, risikoer og sårbarheter. Blant BBKs oppgaver er også å gi råd til offentlige og private aktører om forebyggende og krisehåndterende tiltak for beskyttelse av kritiske infrastrukturer.

I Tyskland har det vært viktig å bygge opp et samarbeid om sikkerhet mellom staten og private markedsaktører. BMI og BBK har jevnlige koordineringsmøter med ulike sektormyndigheter og viktige private aktører. Formålet med møtene er å forsøke å utarbeide noen standarder og anbefalinger i forhold til beskyttelse av infrastruktur. Dette er mye basert på frivillighet fra partenes side. Det er et mål at basisbeskyttelsetiltak skal kunne benyttes av alle infrastruktursektorer, og kunne benyttes av både private og offentlige aktører. Det er utarbeidet sjekklister og gjøremålslister for egenbeskyttelse.

[10] www.krisberedskapsmyndigheten.se; Opplyst under utvalgets møte med KBM og påfølgende dialog 2005.

[11] Opplyst under utvalgets møte med BBK/BSI i Tyskland 2005, og påfølgende dialog.

[12] Opplyst under utvalgets møte med BBK/BSI i Tyskland 2005, og påfølgende dialog.

Nasjonal kriseledelse i Tyskland[13]

BBK er ansvarlig for å koordinere krisehåndteringen på sentralt nivå i Tyskland. Innenfor BBK er det etablert et felles føderalt og statlig informasjons- og situasjonssenter *Gemeinsames Melde- und Lagezentrum von Bund und Ländern (GMLZ)*. GMLZ er ansvarlig for samordning av informasjonshåndteringen og ressursallokering i tilfelle alvorlige og omfattende krisesituasjoner i Tyskland. Senteret arbeider også på oppdrag av BMI og ivaretar Tysklands ansvar innenfor internasjonale krisehåndteringsmekanismer.

GMLZ skal bidra til effektivt samarbeid knyttet til sikkerhet og beredskap på lokalt, regionalt, nasjonalt og internasjonalt nivå. Ut over dette skal senteret jevnlig levere situasjonsoversikter til forskjellige steder. Ved siden av jevnlig situasjonsovervåking, skal GMLZ motta og bearbeide og formidle informasjon og prognoser over scenarioutvikling under en krise. Senteret gjennomfører også ekspert- og ressursutredninger og formidler resultatene til relevante aktører. For dette formål benytter situasjonssenteret seg av det tyske nødinformasjonssystemet deNIS, så vel som et stadig voksende nettverk av egne og eksterne eksperter fra forskjellige tjenestesteder og myndigheter innen området befolkningsbeskyttelse.

Andre sentrale aktiviteter i Tyskland på dette området, knytter seg til legemiddelberedskapen, forskning innen ARBC-midler og utdanning i samfunnssikkerhet.

12.5 Nederland

Nederlandske myndigheter har gjennomført et eget prosjekt for å kartlegge kritisk infrastruktur. Målet med prosjektet har vært å få etablert et sett med tiltak for å beskytte den infrastrukturen som regjeringen og næringslivet er avhengig av. Prosjektet var forankret i Innenriksministeriet.

I Nederland benyttes følgende definisjon av begrepet kritisk infrastruktur:[14]

> *Infrastructures are deemed critical if they constitute an essential, indispensable facility for society, and if their disruption would rapidly bring about a state of emergency or could have adverse societal effects in the longer term.*

Nederland har identifisert 12 kritisk infrastruktursektorer. Det er påvist sterk gjensidig avhengighet mellom sektorene og de kritiske infrastrukturene. I tillegg er Nederland avhengig av internasjonal og utenlandsk kontrollert infrastruktur.

Det er identifisert følgende kritiske infrastruktursektorer i Nederland[15]:

- Energi
- Telekommunikasjon
- Drikkevann
- Mat
- Helse
- Finans
- Vanndemninger og kontroll med vann
- Offentlig sikkerhet *(Public order and safety)*
- Rettssystemet *(Legal order)*
- Sentraladministrasjonen *(Civil administration)*
- Transport
- Kjemisk og nukleær industri *(Chemical and nuclear industry)*

Innenriksministeriet har en koordinerende rolle i forhold til sektormyndighetene. Det koordinerende ansvaret endrer ikke ansvaret til andre departementer eller sektormyndigheter. Det er åtte andre departementer som har ansvar for kritisk infrastruktur. I Nederland blir krav til sikkerhet mot uønskede tilsiktede hendelser gradvis innarbeidet i sektorlovene. Det har dessuten vært en revisjon av beredskapslovene og krisehåndteringssystemet i Nederland etter at trusselen fra den kalde krigen opphørte.

Det arbeides kontinuerlig med å identifisere nøkkelpunkter og kritiske noder i infrastrukturen, og det gjennomføres ROS-analyser knyttet til disse. Basert på analysene har det blitt gjennomført et samlet sett med tiltak for å redusere sårbarhetene.

I tillegg til Innenriksministeriets koordinerende rolle overfor andre sektorer på infrastrukturbeskyttelse, har Nederland en egen anti-terrorkoordinator som er ansvarlig for å gjennomføre tiltak for å beskytte personer og spesielle objekter.

Den sivile sikkerhetstjenesten i Nederland jobber med å fremme tiltak for å beskytte kritisk infrastruktur både i offentlige og private virksomheter. Deler av sikkerhetstjenestens oppgaver består blant annet i å innhente og videreformidle trusselinformasjon og gi råd om beskyttelsestiltak. Det

[13] Opplyst under utvalgets møte med BBK/BSI i Tyskland 2005 og påfølgende dialog.

[14] International CIIP Handbook 2004. *An Inventory and Analysis of Protecion Policies in Fourteen Countries.* Eidgenössische Technische Hochschule Zürich (ETH).

[15] Opplyst under utvalgets møte med Innenriksministeriet i Nederland 2005 og påfølgende dialog. Dette fremgår også i International CIIP Handbook 2004. *An Inventory and Analysis of Protecion Policies in Fourteen Countries.* Eidgenössische Technische Hochschule Zürich (ETH). .

gis sektorspesifikke vurderinger knyttet til de ulike sektorene.

Blant annet på bakgrunn av drapene på filmskaperen Theo Van Gogh i 2004 og politikeren Pim Fortuyn i 2002, drap som begge var delvis politisk motivert, er det etablert et eget prosjekt som skal undersøke forhold som kan true tryggheтsfølelsen i Nederland og skaper sosial og politisk ustabilitet.

Nasjonal kriseledelse i Nederland[16]

I tråd med ansvarsprinsippet er hvert departement ansvarlig for krisehåndteringen innenfor sin sektor i Nederland. Koordineringen av krisehåndteringen på nasjonalt nivå ligger til Innenriksministeriet. Departementet utarbeider dessuten sektorovergripende strategisk policy på området, med hovedfokus på ivaretakelse av effektiv samordning mellom de ulike nødetatene.

Innenfor hvert departement er det et *Departemental Coordination Center (DCC)* som står for departementets håndtering av kriser. Ved tverrsektorielle kriser, etableres en strategisk gruppe på embetsnivå, som har ansvar for å koordinere den nasjonale krisehåndteringen. I tillegg kan det opprettes en politisk gruppe bestående av de berørte ministere. Denne gruppen ledes av innenriksministeren.

I forbindelse med tverrsektorielle kriser vil det såkalte *National Coordination Centre (NCC)* fungere som en interdepartemental støtte-, koordinerings- og informasjonskanal. Ved internasjonale kriser (eller nasjonale kriser som fordrer internasjonal hjelp) fungerer NCC også som nasjonalt kontaktpunkt. NCC ligger som et stabselement i linjen rett under innenriksministeren.

12.6 Storbritannia

Den britiske sikkerhetstjenesten MI5 har gjennom det såkalte *National Security Advice Centre (NSAC)* ansvaret for rådgivning knyttet til fysisk sikring og personellsikkerhet i kritisk infrastruktur.

NSAC samarbeider tett med *National Infrastructure Security Coordination Centre (NISCC)*, som har ansvar for å redusere risikoen for elektroniske angrep mot kritisk infrastruktur i Storbritannia. NISCC ble etablert i 1999 og er et tverretatlig samarbeidsorgan som trekker ressurser fra andre deler av sentraladministrasjonen, herunder bidrar det britiske forsvaret, etterretningstjenestene, politiet, m.fl. med ressurser og kompetanse. NISCC har ansvaret for *Uniras*[17] som er en statlig CERT. *Communications-Electronics Secruity Group (CESG)* har myndighetsansvaret for elektronisk kommunikasjonsssikkerhet *(«technical authority for Information Assurance»)*, og er en sentral bidragsyter til NISCC. *Cabinet Office* bidrar med overordnede policy og koordinering av arbeidet med sikring av kritisk infrastruktur i Storbritannia.

I Storbritannia defineres kritisk infrastruktur som:

> *Those assets, services and systems that support the economic, political and social life of the UK whose importance is such that any entire or partial loss or compromise could:*
> – *cause large scale loss of life*
> – *have a serious impact on the national economy*
> – *have other grave social consequences for the community*
> – *be of immediate concern to the national government.*[18]

Det er definert følgende kritiske infrastruktursektorer i Storbritannia:[19]

- Kommunikasjon
- Nød- og redningstjenester *(Emergency Services)*
- Energi
- Finans
- Mat
- Myndigheter og offentlige tjenester *(Government & Public Service)*
- Helse
- Offentlig sikkerhet *(Public Safety)*
- Transport
- Vann

Arbeidet med sikring av kritisk infrastruktur i Storbritannia tar utgangspunkt i målsetninger om, å beskytte sivilbefolkningen og opprettholde et velfungerende samfunn, å sikre at de personer og virksomheter som trenger det evner å sikre seg mot og håndtere alvorlige situasjoner, å legge til rette for at virksomheter også utenfor kritisk infrastruktur er i stand til å fungere så normalt som mulig under en krisesituasjon.

[16] Opplyst under utvalgets møte med Innenriksministeriet i Nederland 2005 og påfølgende dialog.

[17] Tidligere ble UNIRAS benyttet som forkortelse for *Unified Incident Reporting and Alert Scheme*. I Storbritannia har man nå gått over til å bruke dette som egennavn.

[18] www.niscc.gov.uk, samt utvalgets møte med NISCC og påfølgende dialog 2005.

[19] www.niscc.gov.uk, samt utvalgets møte med NISCC og påfølgende dialog 2005.

Arbeider utføres gjennom aktiviteter innenfor følgende hovedområder:
- trusselvurderinger
- rådgivning og informasjonsdeling *(Outreach)*
- varslingstjenester
- forskning og utvikling

Når det gjelder aktiviteter rettet mot privat sektor har NISCC etablert fora hvor en rekke virksomheter med ansvar for kritisk infrastruktur kommer sammen og utveksler nyttig informasjon som kan bidra til å styrke sikkerhetsarbeidet hos alle deltakerne. Disse såkalte *Information Exchanges* finnes blant annet innenfor telesektoren, finanssektoren og blant virksomheter med SCADA[20] systemer. NISCC har også planer om å etablere flere WARPs[21] som er lokale web-basert forum som drives av grupper av (frivillige) deltakere som er enige om å utveksle informasjon og erfaring innen IT-sikkerhetsarbeidet. Dessuten gir NISCC informasjon gjennom en webside (*ITsafe*), som tilbyr rådgivning og veiledning for private nettbrukere og mindre bedrifter.

NSAC har utarbeidet 10 råd/hovedpunkter for ivaretakelse av god sikkerhet. Disse omfatter råd knyttet til gjennomføring av risikoanalyse, planlegging av sikkerhetstiltak, bevisstgjøringsarbeid, sikkerhetsrutiner, personkontroll, opprettholdelse av drift under ulike former for påkjenninger mv.

Nasjonal kriseledelse i Storbritannia[22]

I Storbritannia reguleres beredskapsansvar og ansvar for kriseledelse i *The Civil Contingency Act 2004*. Loven erstattet *The Civil Defence Act 1948* og *The Emergency Powers Act 1920*. De lokale myndigheters roller og ansvar for kriseledelse er sterkt fremhevet, og loven regulerer dessuten myndighetenes fullmakter i tilfelle kriser.

Innenfor de rammene som er satt, ivaretas kriseledelsen i Storbritannia på tre funksjonelle nivåer; det operative, taktiske og strategiske nivå. Disse nivåene betegnes henholdsvis *bronze*, *silver* og *gold*. Det enkelte myndighetsorgan yter innsats i tråd med sitt ansvar og tilgjengelige ressurser.

Når en situasjon er spesielt krevende, både hva gjelder omfang og kompleksitet, kan det være aktuelt å etablere en tverrsektoriell kriseledelse på det strategiske nivå *gold*. Den strategiske kriseledelsen betegnes *Strategic Co-ordinating Group (SCG)*, eller bare *gold* og består av personell på strategisk nivå fra berørte myndighetsorganer.

Normalt er det politiet som ivaretar lederansvaret for den strategiske kriseledelse, men dersom det anses hensiktsmessig ut fra krisens art kan ansvaret bli tillagt en annen myndighet (for eksempel helsemyndighetene).

På departementalt nivå, er ansvaret for kriseledelse og beredskap forankret i *The Cabinet Office* og *Home Office*. For å understøtte ansvaret til *The Cabinet Office* ble det i 2001 etablert et sekretariat *Civil Continencies Secretariat (CCS)*.

12.7 Sveits

Arbeidet med sikring av kritisk infrastruktur i Sveits er basert på målsetninger og tiltak i *Security Policy Report 2000* og *Strategy for the Information Society Switzerland* som er utarbeidet av *Federal Council (Bundeskanzlei, BK)*. Arbeider med sikring av kritisk infrastruktur i Sveits er fordelt på flere departementer.

I Sveits er begrepet kritisk infrastruktur definert på følgende måte:

> *Organisations or institutions which are of essential importance to society, the failure or disruption of which will cause long-term bottlenecks in the supply chain or have other dramatic consequences for large sections of the population.*[23]

Det er ikke utarbeidet en offisiell liste over de kritiske infrastruktursektorene i Sveits. Arbeidet med sikring av kritisk infrastruktur konsentrerer seg om følgende sektorer[24]:
- Sentraladministrasjonen *(Public administration)*
- Rednings- og beredskapstjenester *(Civil Defense and Emergency Services)*
- Telekommunikasjon
- Energi
- Finans
- Industri og produksjon (*Industry/manufacturing)*
- Media
- Helse
- Transport og logistikk
- Vann

Fedearl Strategy Unit for Information Technology (Informatikstrategiorgan Bund, ISB), har et sen-

[20] SCADA = *Supervisory Control and Data Acquisition*
[21] WARP = *Warning, Advice, and Reporting Point*
[22] Kilde: www.cabinetoffice.gov.uk og www.ukresilience.info/ccact, samt utvalgets møte med britiske myndigheter og påfølgende dialog.
[23] Centre for International Security Policy, Critical Infrastructure Protection report [udatert].
[24] International CIIP Handbook 2004. *An Inventory and Analysis of Protecion Policies in Fourteen Countries*. Eidgenössische Technische Hochschule Zürich (ETH).

tralt ansvar for sikring av kritisk infrastruktur i Sveits. ISB er underlagt *Federal Department of Finance (EFD*) og har ansvaret for varslings- og analysesenteret *MELANI* (*Melde- und Analysestelle Informationssicherung*) og SONIA (*Sonderstab Information Assurance*). MELANI er et samarbeid mellom ISB, *Federal Office of Police (Bundesamt für Polizei, fedpol)*, og *Swiss Education and Research Network (SWITCH)*. MELANI baserer seg på frivillig rapportering om IKT-relaterte sikkerhetshendelser i privat og offentlig sektor. SONIA er en »*task force*» som blir sammenkalt ved hendelser som kan føre til alvorlige skader på kritisk infrastruktur. Gruppen er bredt sammensatt med representanter fra alle de viktige samfunnssektorene så vel beslutningstakere som spesialister. En viktig oppgave er å gi forslag og beslutningsunderlag for myndighetene, og å sikre koordinering av tiltak mellom de ulike delene av infrastrukturene.

I internasjonal sammenheng har sveitsiske myndigheter og forsknings- og utdanningsinstitusjoner utmerket seg som betydelige initiativtakere til internasjonalt samarbeid innen sikring av kritisk infrastruktur, og kanskje særlig kritisk elektronisk kommunikasjonsinfrastruktur. Et sentralt initiativ er «*Comprehensive Risk Analysis and Management Network (CRN)*» ved *Swiss Federal Institute of Technology (Eidgenössische Technische Hochschule, ETH)*, som besitter en betydelig kompetanse innen ulike tilnærmingsmåter for sikring av kritisk infrastruktur. Hvert annet år utgir ETH den såkalte *CIIP Handbook* som er et anerkjent oppslagsverk på området.

Nasjonal kriseledelse i Sveits[25]

I Sveits ble en ny lov om samfunnssikkerhet vedtatt 1. januar 2004, *Federal Law on Civil Protection and Protection and Support* (BZG). Loven regulerer forebyggende og konsekvensreduserende tiltak.

Federal Office for Civil Protection (FOCP) ble etablert i 2003 og understøtter kantonene, kommunene og øvrige ansvarlige myndigheter i deres arbeid knyttet til sikkerhet og beredskap. Ansvar og aktiviteter som tidligere lå i *Federal Department of Defence, Civil Protection and Sport (DDPS)*, ble samlet ved etableringen av FOCP, for å tydeliggjøre viktigheten av samfunnssikkerhetsarbeidet.

I likhet med de aller fleste land, organiserer Sveits sitt kriseledelsesapparat i tråd med ansvarsprinsippet. Ved store og komplekse hendelser kan det være behov for strategisk støtte. I slike situasjoner etableres det en sentral stab med adhoc spesialister fra berørte myndigheter som ivaretar den sentrale kriseledelsen. Staben rapporterer direkte til nærmeste ansvarlige myndighet.

12.8 Singapore

Det har ikke vært noe sentralt organ som har hatt totalansvaret for Singapores nasjonale sikkerhet. Ansvaret for sikkerhet har vært fordelt på de forskjellige fagmyndighetene. Hovedskillet har gått mellom Forsvaret og Forsvarsdepartementet (*Singapore Armed Forces/Ministry of Defence*) som har hatt ansvaret for forsvaret av landet mot ytre trusler, og politiet, Innenriksdepartementet (*Ministry of Home Affairs*) og ulike sektormyndigheter som har hatt ansvaret for innenlands sikkerhet.

Etter 11. september 2001 ble det imidlertid ansett som nødvendig å utarbeide en ny nasjonal sikkerhetsdoktrine i Singapore.

I 2003 ble visestatsministeren gitt koordineringsansvaret for forsvars- og sikkerhetspolitikken. Endringen gikk ut på å koordinere forsvars- og sikkerhetsarbeidet slik at ressurser kunne flyttes raskt i takt med endringene i trusselbildet. Den nye tittelen for denne funksjonen i regjeringen er *Coordinating Minister for National Security (CMNS)*.

I 2004 ble det etablert et nytt organ; *National Security Coordination Secretariat (NSCS)*, som er underlagt statsministeren. Organet erstattet det tidligere *National Security Secretariat*, og ledes av den såkalte *Permanent Secretary for National Security and Intelligence Coordination* som rapporterer til den koordineringsansvarlige ministeren (CMNS).

Den koordineringsansvarlige ministeren leder også den såkalte *Security Policy Review Committee (SPRC)*, hvor også forsvarsministeren, innenriksministeren og utenriksministeren deltar.

Innenfor statsministerens kontor er det såkalte *National Security Coordination Secretariat (NSCS)*, gitt i oppgave å drive planlegging, utvikling og koordinering på området nasjonal sikkerhet. Dette sekretariatet blir understøttet av to helt sentrale organer; *National Security Centre (NSCC)* og *Joint Counter Terrorism Centre (JCTC)*.

Omorganiseringen som er gjennomført i Singapore har vært ansett som helt nødvendig i lys av det som tidligere ble oppfattet som en altfor sterk oppdeling av ansvar for sikkerhet mellom ulike organer og komiteer. Den nye organiseringsmo-

[25] Opplyst under utvalgets møte med sveitsiske myndigheter og påfølgende dialog i 2005, samt www.bevoelkerungsschutz.ch.

dellen er likevel ikke så sentralisert som den amerikanske modellen, men samsvarer på den måten at en sentral myndighet er gitt ansvaret for bekjempelse av terrorisme. Modellen er lik den Australske organisasjonsmodellen, i den forstand at koordineringen av politikkutformingen skjer på øverste nivå i regjeringen.

Det ble startet et nasjonalt program for sikring av kritisk infrastruktur i 2002, det såkalte *National Critical Infrastructure Assurance (NCIA) Programme*. Formålet med dette programmet er sikre at kritisk infrastruktur i Singapore er tilstrekkelig beskyttet og robust til å tåle et terrorangrep og på denne måten forhindre at dette får alvorlige samfunnsmessige konsekvenser.

I første fase av NCIA ble følgende kritisk infrastruktursektorer identifisert:
- Vann
- Energi
- Helse
- Kommunikasjon *(info-communication)*
- Transport
- Finans

I neste fase av programmet er det identifisert tre nye sektorer; matforsyning (*Food Supply Sector System and Local Distribution Infrastructure*), næringslivet (*Economic sector/Industries*) og miljø (*Environmental Services*). Fase II i NCIA ble startet i januar 2006.

Nasjonal kriseledelse i Singapore

Siden 1978 har regjeringen i Singapore opprettholdt en kriseledelsesstruktur som heter *Executive Group (EG)*. EG består av flere myndigheter, og har vært tatt i bruk ved flere krisesituasjoner, blant annet ødeleggelsene av *Hotell New World* i 1986 og flykapringen av Singapore Airlines i 1991. I 2003 ble EG aktivert for å koordinere Singapores respons mot SARS.

For å oppnå bedre operativ koordinering har innenriksdepartementet videreutviklet det nasjonale kriseledelsessystem; *Homefront Crisis Management System (HCMS)*. Dette består av den såkalte *Homefront Crisis Ministerial Committee (HCMC)* og *Homefront Crisis Executive Group (HCEG)*.

HCMC ledes av innenriksministeren og består av et utvalg av medlemmer fra regjeringen. HCMC gir strategisk og politisk støtte til krisehåndtering med det for øye å opprette normalsituasjonen så raskt som mulig. HCEG ledes av den såkalte *Permanent Secretary of the Ministry of Home Affairs*. HCEGs oppgave består primært i å gi strategisk støtte ved kriseledelse. HCEG gir støtte til HCMC og koordinerer tverrdepartementale saker, samt sikrer gjennomføringen av de strategiske beslutninger som tas. HCEG er igjen støttet av tverretatlige og tverrfaglige krisestyringsorganer som sikrer rask koordinering mellom ulike myndigheter.

Singapore anser seg selv som relativt skjermet for naturkatastrofer, og det anses å være liten sannsynlighet for at landet skal bli rammet av tsunamier, jordskjelv, sykloner mv. Det har gjort at kriseledelsessystemet i liten grad fokuserer på dette. Tidligere forårsaket sykloner under monsuntiden, flommer, men byggingen av et avansert avløpssystem har redusert sårbarheten som følge av dette. Likevel vil det være slik at dersom en naturkatastrofe mot formodning skulle ramme Singapore, vil det nasjonale kriseledelsessystemet, HCMS, bli tatt i bruk. Dette vil for øvrig også være tilfelle ved for eksempel utbrudd av fugleinfluensa.

Singapores perspektiv på internasjonal terrorisme

Singapore anser seg selv som et mål for internasjonal terrorvirksomhet, ettersom landet er del av det såkalte *Daulah Islamiyah Nusantara* – ideen om et islamsk storrike bestående av mesteparten av Sør-Øst Asia. Singapore oppfattes som en sekulær, moderne stat, som står i kontrast til det ekstreme terrorgrupper står for.

Forhold som gjør dette samfunnet sårbart er blant annet at mange utenlandske selskaper er lokalisert der, at millioner av turister besøker landet hvert år, at økonomien er sterkt avhengig av internasjonal handel mv.

Selv om internasjonal terrorisme ikke truer Singapores eksistens, kan det få alvorlige konsekvenser for samfunnet både i form av menneskelig og materielle skader. Terrorisme kan også sette grupperinger i samfunnet mot hverandre, og på den måten svekke det multikulturelle og multireligiøse samfunnet som Singapore anser som så viktig for sin videre fremgang.

Muslimene i Singapore har tatt sterk avstand fra Al-Qaida og tilsvarende terrorgrupper rundt om i verden, herunder Jemaah Islamiyah (JI), og fordømt terrorhandlinger. I Singapore er man bevisst at også andre trosretninger spiller en viktig rolle, ved at disse må være forsiktige med å koble handlingene som begås av terrorister til de lokale muslimske miljøene, for på denne måten å skape splittelse fremfor samarbeid.

12.9 EU – European Programme for Critical Infrastructure Protection - EPCIP

I 2004 påbegynte EU-kommisjonen et arbeid med å utarbeide et program for å sikre kritisk infrastruktur innenfor rammen av EU-samarbeidet. Programmet går under navnet *European Programme for Critical Infrastructure Protection* – EPCIP. Den overordnede målsettingen med programmet er å sikre et adekvat og likt nivå på forebyggende sikkerhet for kritisk infrastruktur. Omfanget ble i første omgang avgrenset til å beskytte grenseoverskridende kritisk infrastruktur mot terrorhendelser. Kommisjonen foreslo samtidig å opprette et system for varsling av uønskede hendelser til og mellom aktører med kritisk infrastruktur. Det påtenkte systemet går under navnet *Critical Infrastructure Warning Information Network* – CIWIN. Hensikten er å få på plass et system som legger til rette for koordinert og effektiv respons i tilfelle krisesituasjoner.

Tanken om et europeisk program for sikring av kritisk infrastruktur oppstod i Rådet. Med det som bakgrunn utarbeidet Kommisjonen[26] en kommunikasjon med særskilt fokus på beskyttelse av grenseoverskridende infrastruktur mot terrorhendelser.[27] For å sikre innspill til dokumentet inviterte Kommisjonen medlemslandene til å delta på to seminarer. Norge og enkelte andre ikke-medlemsland ble også invitert. Tilbakemeldinger fra seminarene dannet grunnlaget for utarbeidelsen av en Grønnbok i november 2005.[28] Grønnboken er nå utgangspunktet for videre tilbakemeldinger fra medlemslandene samt enkelte andre land som Norge. Omfang, innretning og videre prosess ble ikke avklart under utvalgets arbeid.

[26] Arbeidet med EPCIP er ledet av *Directorate-General for Justice, Freedom and Security (Direction générale Justice, Liberté et Sécurité* – DG JLS).

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

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

12.10 NATO

I forbindelse med trusselen fra terrorisme og bruk av masseødeleggelsesmidler har NATOs sivile side de senere årene vært opptatt av infrastrukturer og sårbarhet. Til grunn for alliansens arbeid er det utarbeidet et styringsdokument (*EAPC(SCEPC)D (2003)15 - Critical infrastructure Protection – Concept Paper*) som åtte sivile plankomiteer forholder seg til. Dokumentet peker på sårbarhet og nødvendighet av samarbeid mellom operatører og beredskapsmyndigheter for å redusere sårbarhet. Vedlagt dokumentet følger en *road map* som trekker opp linjene for det videre arbeidet i NATO. Tiltakene er i all vesentlig grad av informasjonsmessig karakter. Således har det vært avholdt så vel interne som eksterne seminarer og konferanser om emnet. I henhold til *the road map* er det også utarbeidet en presentasjon om *CIP and CEP in NATO Context* med kommentarer til bruk i landene knyttet til NATO. Presentasjonen omtaler NATOs interesse for kritisk infrastruktur og peker på viktigheten av gode relasjoner mellom operatører av kritisk infrastruktur og beredskapsmyndigheter. Målgruppen for denne presentasjonen er universell.

Høsten 2005 holdt NATOs *Civil Protection Committee* et større seminar som i sin helhet var viet kritisk infrastruktur.[29] Som følge av seminaret vil NATO i fortsettelsen blant annet arbeide med:

- Bedre retningslinjer for videre arbeid basert på praktiske erfaringer.
- Etablering av et kontaktnett mellom landene for utveksling av informasjon.
- Etablering av en gruppe som kan evaluere uønskede hendelser som måtte ha inntruffet og trekke ut nødvendig lærdom av slike
- Utvikling av et nærmere samarbeid med andre internasjonale organisasjoner for informasjonsutveksling, samt det å hindre duplisering i arbeidet.
- Utvikling av opplæringsprogram med tanke på å redusere sårbarhet, basert på Internett.
- Utarbeidelse av et nytt spørreskjema for å kartlegge status i landene
- Revisjon av the *road map*.

[29] Utvalgets leder var *key note speaker* på dette seminaret som ble holdt i Moldova.

Kapittel 13
Forsknings- og utredningsaktiviteter

I dette kapittelet behandles et utvalg av sentrale utredningsaktiviteter som knytter seg til beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner. Dette er ikke ment å være en uttømmende redegjørelse. På ulike måter behandler disse utredningene trusler, risikoer og sårbarheter i samfunnet. Arbeidene er av betydning for innretting og prioritering av sikkerhets- og beredskapsarbeidet både innenfor den enkelte samfunnssektor og i samfunnet generelt.

13.1 Sårbarhetsutvalgets utredning

I september 1999 ble sårbarhetsutvalget nedsatt for å utrede samfunnets sårbarhet med sikte på å styrke samfunnets sikkerhet og beredskap. Rapporten ble ferdig juli 2000. Sårbarhetsutvalget konkluderte blant annet med at samfunnet er langt mer sårbart enn tidligere, og at svikt i noen få grunnpilarer og funksjoner i samfunnet kan resultere i kritiske problemer for samfunnet som helhet. Sårbarhetsutvalget påpekte at tap av telekommunikasjon og energiforsyning vil få særlig alvorlige konsekvenser. Sårbarhetsutvalget viste videre til at andre aspekter som bidrar til økt sårbarhet, herunder teknologiske endringer, økende kompleksitet i samfunnet, økende krav til effektivitet og kostnadsreduserende tiltak, redusert antall personell i viktige samfunnssektorer og økende privatisering av offentlige tjenester. Utvalget tok også for seg utfordringer knyttet til terrorisme. Sårbarhetsutvalgets arbeid er et sentralt grunnlag for forståelse av sårbarheter i kritisk infrastruktur, og dette utvalgets arbeid bygger videre på sårbarhetsutvalgets vurderinger og anbefalinger.

Sårbarhetsutvalgets vurderinger og anbefalinger var det sentrale grunnlaget for Regjeringens politikk knyttet til samfunnssikkerhet og beredskap slik det fremgår av St.meld. nr. 17 (2001-2002) Samfunnssikkerhet og St.meld. nr. 39 (2003-2004) Samfunnssikkerhet og sivilt-militært samarbeid.

13.2 Pågående og avsluttede aktiviteter

Beskyttelse av samfunnet (BAS) - prosjektene

Det mest omfattende og helhetlige arbeidet som er gjort i Norge om sårbarhet i kritisk infrastruktur og kritiske samfunnsfunksjoner er i de såkalte BAS-forskningsprosjektene ved Forsvarets forskningsinstitutt (FFI). Forskningen har på flere områder vært en premissgivende for myndighetenes arbeid.

Prosjektseriens langsiktige mål er å bidra til et gjennomarbeidet konsept for beskyttelse av samfunnet, samt støtte opp under en løpende prioritering av sårbarhetsreduserende tiltak. I BAS-studiene har det inngått sårbarhetsanalyser av ulike sektorer, studier av tilsiktede og utilsiktede trusler mot samfunnet og kosteffektivitetsanalyser av sårbarhetsregulerende og skadebøtende tiltak. BAS har så langt omfattet følgende prosjekter:

- 1994-1997 Samfunnets sårbarhet og organiseringen av beredskap (BAS1)
- 1997-1999 Sårbarhet i offentlig telekommunikasjon (BAS2)
- 1999-2001 Sårbarhet i kraftforsyningen (BAS3)
- 2001-2003 Sårbarhet i transportsektoren (BAS4)
- 2003 Sårbarhet i vannforsyningen (SIV)
- 2004-2006 Sårbarhet i samfunnskritiske IKT-systemer (BAS5)

TERRA - Forskning på terrorisme og asymmetrisk krigføring

TERRA-prosjektet tar sikte på å legge et bredere grunnlag for forståelsen av transnasjonale radikale islamistbevegelser som er en av de viktigste drivkreftene bak dagens internasjonale terrorisme. Prosjektet er et aktørfokusert prosjekt og sikter mot å frambringe ny kunnskap om ideologi, motivasjoner, handlingsmønstre, aksjonsformer og støttenettverkene til transnasjonale radikale islamistorganisasjoner.

Prosjektet inneholder flere hovedaktiviteter. En av disse er dybdestudier av et utvalg radikale islamistorganisasjoner tilknyttet al-Qaida nettverket. Samspillet mellom ideologi, aksjonsformer og støttenettverk står sentralt. Casestudiene inkluderer en

større studie om radikal islamisme i Europa, islamistgrupper i Midtøsten, Nord-Afrika og Asia, samt noe aktivitet på situasjonen i Irak. En annen hovedaktivitet er mer teoretisk rettede studier om transnasjonalisme, globalisering og islamistbevegelser. En tredje del fokuserer mer spesifikt på ideologene bak al-Qaida. Oppgradering og vedlikehold av kildesamlinger og kunnskapsbaser om radikal islamisme er en fjerde delaktivitet. En siste mer praktisk og kundeorientert del inkluderer studier av terrorgruppers bruk av våpen/virkemidler, målutvelgelse, eventuelt andre korte oppdragsorienterte studier.

Konsortium for forskning på terrorisme og internasjonal kriminalitet

Iverksetting av tiltak rettet mot terrorisme og internasjonal kriminalitet krever innsikt og kunnskap. Forvaltningen innehar kompetanse gjennom ulike sikkerhets- og beredskaps- og politimyndigheter. Ut over dette bidrar forskningsmiljøer med bredde og ny forståelse, og er en viktig ressurs som bidragsyter til myndighetenes håndtering av tiltak. Forskningsmiljøenes mer generelle rolle som aktør i den offentlige debatt, bidrar også til å løfte problemstillinger og fakta ut i det offentlige rom.

Forsvarets forskningsinstitutt (FFI) og Norsk utenrikspolitisk institutt (NUPI) inngikk i 2002 et forskningssamarbeid i form av et konsortium for forskning på terrorisme og internasjonal kriminalitet. Fra 2004 gikk Politihøgskolen (PHS) inn i samarbeidet. Hensikten var å samle ressurspersonene ved ulike institutter til ett sterkt faglig miljø for å kunne komplementere hverandres ferdigheter gjennom spesialisering, i stedet for å drive dobbeltarbeid om de samme temaene. Tilsammen fremstår konsortiet nå som et slagkraftig miljø, og er et av de største og tyngste i Europa. På den bakgrunn er det nylig etablert et skandinavisk nettverk for terrorismeforskning.

Riksrevisjonens forvaltningsrevisjon av IT-sikkerhetsarbeidet

Riksrevisjonen har vurdert hvorvidt myndighetenes arbeid med IT-sikkerheten i samfunnet er i samsvar med Stortingets forutsetninger. I denne forbindelse har Riksrevisjonen undersøkt blant annet organiseringen av myndighetenes arbeid med IT-sikkerhet, plan- og gjennomføringsprosesser knyttet til IT-sikkerhet, myndighetenes arbeid for å beskytte samfunnskritisk IT-infrastruktur, arbeidet med utviklingen av en sikkerhetskultur på IT-området, samt myndighetenes planlagte og iverksatte tiltak innenfor telesikkerhet og – beredskap spesielt. I dokument nr. 3:4 (2005–2006) *Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur,* som ble overlevert Stortinget 22. november 2005, konkluderes det med at IT-sikkerhetsarbeidet er preget av mange aktører og uklare ansvarsforhold, herunder mangelfull avklaring av ansvarsforhold på departementsnivå. Riksrevisjonen har gjennomgått Nasjonal strategi for informasjonssikkerhet fra 2003, og det konkluderes med at få planlagte tiltak i strategien er gjennomført. Riksrevisjonen mener IT-sikkerhetsarbeidet må gis høyeste prioritet og at styringen av dette arbeidet må koordineres bedre enn det som er tilfelle i dag.

Østfoldundersøkelsen

I forbindelse med den anstrengte kraftsituasjonen våren 2003 ble landets energiverk pålagt å revidere sine planer for kraftrasjonering ved utkobling. Østfold Energi reviderte og utarbeidet rasjoneringsplanene våren 2003 for et område som dekker 2/3 av Østfold. Det ble gjennomført en detaljert undersøkelse av virkningen på samfunnet og laget planer for rasjonering med roterende sonevise strømutkoblinger basert på dette.

Undersøkelsen viser at strømnettet ikke er konstruert med tanke på rasjonering ved utkobling. Undersøkelsen gir dessuten en god illustrasjon på hvor avhengig samfunnets sikkerhet er av en stabil strømforsyning, og på at reelle prioriteringer forutsetter detaljerte analyser.

OECDs studie av IKT-sikkerhetsarbeidet i Norge

Organisasjonen for økonomisk samarbeid og utvikling (OECD) sin rapport *Emerging Systemic Risks in the 21st Century - An agenda for Action* (OECD, 2003) blir fulgt opp gjennom et nytt prosjekt: Risk *Management Policies in Selected OECD Countries*. Norge deltar i dette prosjektet med et *Case Study* som omhandler nasjonal organisering av tiltak med hensyn til IKT-sikkerhet. Målet med dette er dels å gi bidrag til generelle retningslinjer fra OECD med hensyn til risikostyring, dels å bidra til norsk policy på området IKT-sikkerhet.

Andre forsknings- og utredningsaktiviteter

Ved NTNU og SINTEF foregår det forskning som direkte omhandler eller grenser opp mot sårbarheter i kritisk infrastruktur. Det gjelder innenfor områder som transport, kraftforsyning, vannforsyning og IKT. Eksempler på forskningsaktiviteter er problemstillinger knyttet til deregulering i trans-

portsektoren, sårbarhet i den nordiske kraftsektoren, sårbarhet i det norske distribusjonsnettet for kraftforsyning, rehabiliteringsplanlegging av vannforsyningsnett og hendelsesrapportering og oppfølging av IKT-sikkerhetsbrudd via videreutvikling av sikkerhetskultur i olje og gass-sektoren.

Forskningen ved sikkerhetsmiljøet ved Universitetet i Stavanger (UiS) og ved Senter for Risikostyring og Samfunnssikkerhet (SEROS) har som formål å bidra til å bygge et sikrere og mer robust samfunn. Mye av den forskningsaktiviteten som foregår har direkte eller indirekte relevans for kritisk infrastruktur, enten ved forskning på sårbarhet i systemer eller i forskning innen trusler mot systemene. Eksempler på sektorer og temaer med relevant forskning er transportsektoren, helsesektoren, informasjonssikkerhet og sårbarhet i samfunnskritisk IKT.[1]

Flere forskningsprogrammer under Norges forskningsråd er relevante for beskyttelsen av kritisk infrastruktur og kritiske samfunnsfunksjoner. Dette gjelder blant annet Energiprogrammet, NORKLIMA og IKTSOS.

13.3 Utvalgets vurderinger og anbefalinger

Utviklingen i trussel-, risiko- og sårbarhetsbildet tilsier styrket oppmerksomhet på å bedre samfunnets evne til forebygge kriser og ulykker, og unngå alvorlig svikt i kritiske samfunnsfunksjoner, installasjoner, systemer og tjenester. Dette forutsetter en kontinuerlig satsning på forsknings- og utviklingsaktiviteter.

Det er samtidig viktig å følge det internasjonale forsknings- og utviklingsarbeidet på området, herunder å samarbeide med internasjonale organisasjoner og myndigheter om felles forsknings- og utviklingsprosjekter dersom dette anses viktig for innhenting og formidling av læringspunkter.

13.3.1 Forslag knyttet til utvidelse av Forsvarets forskningsinstitutts mandat

Forsvarets forskningsinstitutt (FFI) har siden 1994 vært en premissleverandør for forskning på samfunnets sårbarhet i sivil sektor til norske myndigheter. FFIs forskning har bidratt til myndighetenes prioriteringer slik de er nedfelt i stortingsmeldinger, stortingsproposisjoner og andre styrende dokumenter. En styrke er at arbeidet skjer i et integrert miljø hvor sivile og militære utfordringer blir sett under ett. Forskningen har blitt til i tett samarbeid med miljøer som arbeider med sikkerhetspolitikk og terrorforskning ved FFI.

Forskning om samfunnets sårbarhet har ikke vært en del av FFIs ordinære virksomhet, men har vært organisert som brukerfinansierte to- og treårige ad-hoc-prosjekter. I tillegg har FFI hatt flere korte oppdrag om samfunnets sårbarhet ved siden av. Oppdragsgivere har variert med tema. Justis- og politidepartementet og Direktoratet for samfunnssikkerhet og beredskap har stått som hovedoppdragsgivere i hele perioden. I det siste prosjektet så langt, om sårbarhet i samfunnskritiske IKT-systemer, arbeider FFI tett med flere akademiske institusjoner og private og offentlige virksomheter.

Prosjektene har blitt finansiert som spleiselag mellom ulike myndighetsorganer. I det siste prosjektet har Norges forskningsråd stått for om lag halvparten av finansieringen gjennom forskningsprogrammet IKT Sikkerhet og sårbarhet (IKTSOS).

Det fremstår som en utfordring at FFIs forskning på samfunnets sårbarhet i sivil sektor finansieres ad-hoc fra prosjekt til prosjekt og at kompetansen står i fare for å forvitre mellom hvert prosjekt. Utvalget ser det som uheldig med manglende kontinuitet i et forskningsmiljø som har vært ledende og premissgivende på temaet samfunnssikkerhet og sårbarhet i kritisk infrastruktur. Utvalget vil derfor anbefale at FFIs mandat utvides til også å omhandle samfunnets sårbarhet i sivil sektor. Det vil etter utvalgets mening bidra til å se moderne sikkerhetspolitiske utfordringer i et større perspektiv, og hente ut synergieffekter mellom militær og sivil sektor på forskningen.

Utvalget vil også på generelt grunnlag påpeke viktigheten av å bygge videre på samfunnssikkerhetskompetansen i FFI. Økt sivilt-militært forskningssamarbeid antas å bidra til at det gis koordinerte råd til den sivile og militære ledelse om den vitenskapelige og tekniske utviklingens konsekvenser for vårt lands sikkerhets- og beredskapspolitikk. I denne sammenheng viser utvalget til viktigheten av sivilt-militært forskningssamarbeid blant annet forskning innen terrorisme, personellutrustning, beskyttelse mot masseødeleggelsesmidler, beskyttelse av kjøretøyer mv.

13.3.2 Forslag knyttet til forskningsprogrammet SAMRISK

I april 2005 anbefalte en utredningsgruppe opprettelsen av et eget program i Norges forskningsråd på

[1] For flere detaljer, se Sørli, Kjetil 2005. *Sårbarhet i kritisk infrastruktur – utfordringer. Innledende utredning om kritisk infrastruktur til Utvalg for sikring av landets kritiske infrastruktur.* Direktoratet for samfunnssikkerhet og beredskap – i del 2, vedlegg 3.

samfunnssikkerhet og risikoforskning (SAMRISK).[2] Gruppen skrev at: «Programmet skal gi økt kunnskap om trusler og farer, sårbarhet og risikohåndtering og dermed bidra til å ivareta sikkerhet og beredskap på tvers av sektorer og aktivitetsområder.»

Viktige mål for forskningen i SAMRISK var etter utredningsgruppens syn:

- Å bygge ny kunnskap som fremmer samfunnssikkerheten i et bredt perspektiv (både innen *safety* og *security* og på tvers av arenaer og sektorer). Dette innebærer forskning for å skape grunnlag for politikkutforming og realiserbare løsninger, samt et bidrag til å skape offentlig debatt.
- Å bygge nettverk mellom departementer, etater, virksomheter (både private og offentlige) og forskningsmiljøer, dvs. å motvirke fragmenterte og suboptimale løsninger i sikkerhetsarbeidet og sikre praktisk anvendelse av ny kunnskap.
- Å kvalifisere norske forskningsinstitusjoner for internasjonalt forskningssamarbeid (for eksempel *security*-forskningen i det 7. rammeprogram). Den norske samfunnssikkerhet må ses i et internasjonalt perspektiv, og globaliseringens betydning for sikkerheten i vårt samfunn må belyses.

Utvalget ser forskning som et viktig virkemiddel for å redusere samfunnets sårbarhet og for å sikre kritisk infrastruktur. En øremerking av forskningsmidler vil stimulere til økt forskningsaktivitet på området. Det vil gi myndigheter og beslutningstakere større muligheter til å være i forkant med å avdekke nye sårbarheter, og bidra til en mer proaktiv håndtering.

Flere forskningsmiljøer eksisterer i dag. De arbeider delvis uten kontakt med hverandre, og de har til dels forskjellig fokus og agenda. Å tilrettelegge for et eget forskningsprogram vil etter utvalgets mening bidra til å styrke og samordne komplekse og tverrsektorielle utfordringer. Det vil videre bidra til koordinert innsats mellom de ulike forskningsmiljøene. Utvalget mener at SAMRISK-modellen er et godt utgangspunkt for både å styrke og samordne forskningen.

13.3.3 Forslag om å gi prioritet til sikkerhet og beredskap i forskningsprogrammer ved Norges forskningsråd

Utvalget vil understreke verdien av at forskningsprogrammer ved Norges forskningsråd som er relevante for beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner, innarbeider og gir prioritet til sikkerhets- og beredskapsmessige utfordringer. Dette kan for eksempel gjelde prosjekter innenfor Energiprogrammet og NORKLIMA.

13.3.4 Forslag knyttet til Konsortium for forskning på terrorisme og internasjonal kriminalitet

Konsortium for forskning på terrorisme og internasjonal kriminalitet har som modell vist styrke ved at det har lyktes med å koble forsknings- og brukermiljøer. I tillegg til at grunnforskningen har økt og er blitt formidlet, har brukermiljøene bestilt skreddersydde forskningsoppdrag tilpasset deres egne kunnskapsbehov i møte med et bredt forskningsmiljø, og ikke bare enkeltinstitusjoner.

Frem til nå har brukergruppene tilbudt mindre økonomiske bidrag for å finansiere grunnforskningen på området. I tillegg har de støttet med enkeltbidrag ved bestilling av egne oppdrag. Konsortiet har lyktes med å bygge opp et sterkt forskningsmiljø på feltet, men står overfor utfordringer med å vedlikeholde og videreutvikle miljøet på lengre sikt. Manglende forutsigbarhet knyttet til finansieringen av konsortiet kan bidra til tap av viktig kompetanse innenfor et område hvor samfunnet møter stadig nye utfordringer. Utvalget vil derfor understreke viktigheten av å opprettholde og videreutvikle denne kompetansen. Utvalget vil videre se det som relevant at Justis- og politidepartementet blir en del av brukermiljøet.

13.3.5 Forslag knyttet til forskning på gjensidige avhengigheter i kritisk infrastruktur

Det foreligger en del forsknings- og utredningsmateriale på gjensidige avhengigheter mellom kritiske samfunnsfunksjoner og kritiske infrastrukturer, men nøyaktig hvordan de gjensidige avhengighetene påvirker utfallet av større sammenbrudd er vanskelig å forutsi.[3] Høy grad av kompleksitet tilsier at nytteeffekten av slike analyser er størst når de utføres på mindre og avgrensede objekter og systemer. For eksempel vil analyser av punkter i

[2] Innstilling fra en utredningsgruppe nedsatt av Norges forskningsråd 2005. *Samfunnssikkerhet og risikoforskning (SAMRISK)*.

[3] For FFIs tilnærming, se Hæsken, Ole Morten. Olsen, Thor Gunnar. Fridheim, Håvard. *Beskyttelse av samfunnet (BAS) – Sluttrapport.* Forsvarets forskningsinstitutt. FFI/Rapport-97/01459.; For en illustrasjon på den nederlandske fremgangsmåten, se Ministry of the Interior and Kingdom Relations 2003. *Critical Infrastructure Protection in The Netherlands.* The Netherlands. April 2003, side 15-17. http://www.ministerremkes.nl/contents/pages/5018/DGOOV-NCC-QuickScan.pdf

elektroniske overføringsnett og punkter i strømnettet kunne avdekke behov for tiltak som reduserer sårbarhet som følge av gjensidige avhengigheter dem i mellom. Utvalget anbefaler med dette som bakgrunn at det blir startet et forskningsprosjekt rettet mot mulighetene for å redusere gjensidige avhengigheter i kritisk infrastruktur. Utvalget anbefaler at forskningsprosjektet blir initiert og koordinert av Justis- og politidepartementet. Utvalget forutsetter at prosjektet vil kunne bli delvis finansiert av relevante virksomheter med ansvar for kritisk infrastruktur, og delvis av en nyopprettet tilskuddsordning, jf. utvalgets anbefaling i kapittel 6.7.3. Utvalget ser det som naturlig at en eventuell oppfølging av forslagene kan delfinansieres av en nyopprettet tilskuddsordning.

Kapittel 14
Økonomiske og administrative konsekvenser

Utvalget har som en del av sitt mandat å vurdere de administrative og økonomiske konsekvensene av sine forslag og anbefalinger.

De forslag og anbefalinger som utvalget fremmer faller innenfor flere kategorier av virkemidler:

- Rettslige og regulatoriske (påbud, standarder, normer osv.)
- Økonomiske (tilskuddsordninger)
- Organisatoriske (endring av oppgaver i statlige organer)
- Pedagogiske (informasjons- og holdningskampanjer)

14.1 Generelt

For en del av forslagene vil en konkret tallfesting av økonomiske konsekvenser være problematisk. Ikke minst vil det være vanskelig å balansere utgiftsmessige forhold mot den gevinst som må tas med i betraktningen i form av en forbedret sikkerhetstilstand. Dette er et dilemma som gjelder alle sikkerhetsrelaterte tiltak: Så vel administrative som økonomiske investeringer har som formål å unngå en uønsket utvikling eller uønskede hendelser og konsekvenser, men den konkrete gevinsten lar seg vanskelig dokumentere på en inntektsside. En alternativ tilnærmingsmåte ville være å vurdere kostnader ved scenarieteknikk som tok utgangspunkt i en rekke uønskede hendelser man søker å unngå ved tiltakene. Dette vil heller ikke være en fullgod metode, da utfallsrommet for mulige konsekvenser av disse hendelsene er meget stort.

Et fruktbart utgangspunkt bør være å ta utgangspunkt i en samfunnsmessig verdivurdering av de kritiske infrastrukturer som det tas sikte på å beskytte. I denne sammenheng vises det til kapitlene foran hvor det begrunnes hvorfor noen infrastrukturer må betraktes som kritiske.

14.1.1 Balansering av kostnader

Når virkningene av tiltak som retter seg mot bedre sikkerhet er så vanskelig å dokumentere, er det også et problem å vurdere, enn si måle, hva som er et riktig kostnadsnivå. Selv om det er store verdier som står på spill, er det i det minste en teoretisk grense for når innsatsmidlene har nådd et punkt hvor det ikke er mulig å oppnå særlig bedre gevinst i forhold til reduserte konsekvenser.

Minimalisering av alle tenkelige risikoer kan umulig være noen fornuftig målsetting. Det vil for det første være et spørsmål hvor store ressurser samfunnet bør ofre totalt sett på å gjøre samfunnet mindre risikoutsatt i forhold til andre samfunnsoppgaver. For det andre vil det være et spørsmål om fordelingen av ressursene rettet mot samfunnssikring på de ulike områdene, slik som sikring mot terror, trafikksikring, katastrofer knyttet til olje- og gassutvinning, forebygging av smittsomme sykdommer osv.

Det er også av interesse å vurdere prioritering av innsatsmidler brukt på forebyggende sikkerhetsarbeid kontra beredskap.

Uavhengig av det forebyggende arbeidet er samfunnet helt avhengig av til en hver tid å ha en beredskap knyttet til kritisk infrastruktur. En kan likevel spørre seg om det brukes for lite ressurser på forebygging ved å iverksette tiltak på forhånd (pro-aktivt) i forhold til å bøte på en oppstått skade (re-aktivt). Årsaken til at det er slik er nok sammensatt, men kan blant annet ha å gjøre med at det er vanskeligere å få aksept for å bruke ressurser på forhold som ikke har inntruffet, og som kanskje ikke engang kommer til å inntre i overskuelig fremtid. Da er det nok lettere å fokusere på hendelser som man har erfaring med.

For å få til en best mulig balanse mellom skadebøtende og hendelsesbaserte tiltak på den ene siden og skadeforebyggende og risikobaserte tiltak på den annen, er det nødvendig med virkemidler av både politisk, kunnskapsmessig, økonomisk og normativ art. Det er også avgjørende hvilken risiko som aksepteres, og hvilke sikkerhetstiltak som er praktisk anvendelige.

Utvalgets ulike forslag ligger innenfor alle de kategoriene som her er nevnt. Mange av forslagene må sies å være slike som tar sikte på å styrke det forebyggende arbeidet med et bredt spekter av virkemidler, selv om beredskapsarbeidet også har fått en helt sentral plass.

14.2 Forslag som gjelder regulatoriske virkemidler

Det er særlig tre forslag fra utvalget av regulatorisk karakter hvor det er viktig å gjøre en konsekvensvurdering.

14.2.1 Forslag om å utarbeide en generell, sektorovergripende lov om beredskap

Forslaget om en ny generell lov om beredskap vil få konsekvenser av administrativ og økonomisk art, i de tilfeller hvor virksomheter som faller inn under loven blir pålagt beredskapstiltak, som de ikke er pålagt med hjemmel i annen lovgivning eller som de ikke har iverksatt på selvstendig grunnlag. Det må derfor forutsettes at de økonomiske og administrative konsekvensene vil variere i ikke ubetydelig grad, og at en realistisk vurdering av disse konsekvensene ikke kan gjøres på generelt grunnlag.

Utvalget har ikke laget en endelig liste over hvilke virksomheter som den foreslåtte lovens virkeområde omfatter. Lovens virkeområde vil måtte bli nærmere definert som resultat av den prosessen utvalget har lagt opp til for utpeking av virksomheter med ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner.

Det følger av utvalgets forslag at loven skal regulere hvem som skal være tilsynsmyndighet. Utvalget har ikke konkludert på dette punkt, men viser til at det kan tenkes løsninger hvor tilsynet i medhold av loven deles mellom sektortilsynene. Dette vil gi en mulighet til å se sektorlovgivningen og den sektorovergripende lovens bestemmelser i sammenheng. Det vil uansett måtte utpekes et sentralt tilsynsorgan som ivaretar en koordinerende rolle. I denne sammenheng peker utvalget på at ansvarslinjene mellom sektortilsynene, Nasjonal sikkerhetsmyndighet og Direktoratet for samfunnssikkerhet og beredskap bør vurderes. Utvalget mener at Justis- og politidepartementet må ha det overordnede ansvaret for loven.

14.2.2 Forslag knyttet til sikkerhetsloven

Forslagene knyttet til sikkerhetsloven dreier seg i stor grad om en oppfordring til å videreføre et arbeid som har vært i gang i lang tid. To utvalg, nedsatt av Forsvarsdepartementet, har utarbeidet forslag til nødvendig lovendring og forskrifter om objektsikkerhet. Ett konkret forslag er av organisatorisk art, idet utvalget foreslår at fullmakten til å fatte enkeltvedtak om lovens virkeområde overfor private rettssubjekter flyttes fra Forsvarsdepartementet til Justisdepartementet.

Når det gjelder utredning av administrative og økonomiske konsekvenser ved en gjennomføring av forslagene knyttet til sikkerhetsloven, vil utvalget vise til den rapport som ble utarbeidet av det første utvalget som Forsvarsdepartementet nedsatte. Den endelige vurderingen av disse konsekvensene må skje i forbindelse med fremlegging av et endelig forslag om lovendring og forskrift.

Utvalget har merket seg at arbeidsgruppen under Forsvarsdepartementet som la frem forslag til forskrift om objektsikkerhet også hadde vurdert mulige økonomiske konsekvenser. Selv om det i den foreslåtte forskriften slås fast at den enkelte virksomhet skulle dekke egne omkostninger som følge av pålegg, ble det også åpnet for mulighet til å søke om dispensasjon fra sikkerhetskravene eller om å få offentlig tilskudd for å dekke omkostninger ved objektsikkerhet som virker urimelig tyngende. Utvalget forutsetter at slike tiltak vurderes igjen i forbindelse med utredning om økonomiske konsekvenser for objekteiere.

14.2.3 Forslaget om lovbestemt offentlig eierskap i vann- og avløpssektoren

Vannforsyning og avløpshåndtering er i dag i all hovedsak et kommunalt ansvar. Blant de 90 % av befolkningen som er tilknyttet et vannverk, får hele 95 % av disse sitt drikkevann fra vannverk som er offentlig eid. Et lignende forhold gjør seg gjeldende for avløpsanleggene.

En lovfesting av offentlig eierskap til VA-infrastrukturen vil derfor ha meget små konsekvenser. Det viktigste motivet i forbindelse med dette forslaget er nettopp å bevare en situasjon med offentlig eierskap i fremtiden. Som det er pekt på i kapittel 10.4.3 kan konsekvensene av ikke å ta i bruk dette virkemiddelet bli alvorlige dersom eierskapet går fra det offentlig til private investorer med vesentlig kortere tidshorisont på inntjeningskravet for sine investeringer enn det en offentlig eier kan ha. Unntaket fra et lovpålagt eierskap vil som beskrevet i kapittel 10.4.3.1 være VA-virksomheter som ikke er offentlig eid i dag, dvs. som er organisert som private andelslag eid av abonnentene.

Utvalget tror bestemmelsen om eierskap kan finne sin plass innenfor rammene av en eventuell ny sektorlov for vann og avløp. En videre konsekvensutredning av en slik lov ligger utenfor utvalgets oppgave og mandat, da det kun er eierskapsforholdet som er vurdert.

14.3 Forslag angående krav til teleoperatører

Utvalget antar at de avtaler om tiltak som Post- og teletilsynet må gjøre overfor teleoperatørene dersom kravet om full autonomi skal utgå, vil ha en kostnadsside for staten. Dette skyldes at de nødvendige beredskapstiltakene vil være slike som operatørene ikke ville ha implementert under andre omstendigheter. Utvalget ser for seg at størrelsen på de midler staten i dag bruker på særskilte beredskapstiltak i telesektoren vil måtte økes betraktelig.

Utvalget har ikke den nødvendige kompetanse til å vurdere hvilke tiltak som vil være nødvendig for å sikre drift av telesystemene i tilfredsstillende grad i en situasjon med isolasjon/brudd med internasjonale nett. Post- og teletilsynet arbeider med avtaler med teleoperatørene som alternativ til full autonomi.

14.4 Forslag som gjelder organisatoriske virkemidler

Utvalget fremmer en del forslag og anbefalinger som i første rekke har karakter av organisatoriske endringer og tilpasninger innen forvaltningen. Et eksempel på dette er forslaget om å tydeliggjøre Justisdepartementets koordinerende rolle og ansvar ved ivaretakelse av rikets sikkerhet og vitale nasjonale interesser.

En oppfølging av de koordineringsoppgavene utvalget peker på i denne sammenheng vil måtte få noen konsekvenser både administrativt og økonomisk. Det vil være vanskelig å ivareta dette ansvaret fullt ut uten at departementet får tilført flere ressurser.

Når det gjelder forslag som gjelder styrking av samarbeid mellom ulike etater (eksempelvis forslag knyttet til forholdet mellom NSM, PST og DSB og forslag om opprettelse av en samordningsgruppe for vannsektoren) legger utvalget til grunn at oppfølging av slike forslag ikke vil få nevneverdige administrative eller økonomiske konsekvenser, utover det som kan dekkes innenfor de ordinære budsjettene for de enkelte etatene.

14.5 Forslag som gjelder økonomiske virkemidler

14.5.1 Forslag om en økonomisk tilskuddsordning

Det vises til omtale av forslaget i kapittel 6.6.3. Dersom dette forslaget skal tas til følge, vil det innebære at det må budsjetteres med friske midler. Utvalget har ikke tatt stilling til hvor stort beløp som det bør bidras med til en slik ordning, men peker på at en tilsvarende ordning i Sverige har en årlig ramme på om lag 2 milliarder svenske kroner.

I forslaget er det lagt inn en forutsetning for tilskudd til private virksomheter at tiltakene finansieres gjennom en kostnadsdeling. Tildeling av midler vil altså frembringe ytterligere friske midler i tillegg til det som tas fra selve tilskuddsordningen.

En tilskuddsordning slik det er foreslått vil også ha noen administrative konsekvenser for de offentlige organer som skal forvalte denne. I forslaget er det pekt på JD. Når det gjelder nødvendig faglig kompetanse for å kunne initiere og vurdere konkrete tilskudd forutsettes det at direktoratene allerede innehar denne. Det må videre påregnes noe ekstra arbeid med selve koordineringen og administreringen av ordningen.

14.5.2 Forslag knyttet til forskning og utredning

SAMRISK

I april 2005 anbefalte en utredningsgruppe nedsatt av Norges forskningsråd opprettelsen av et forskningsprogram på samfunnssikkerhet og risikoforskning (SAMRISK). Infrastrukturutvalget har ikke foretatt en egen vurdering av kostnadene knyttet til opprettelsen av SAMRISK-programmet, men viser til utredningsgruppen innstilling hvor det står: «En økonomisk ramme på 12-14 mill. kroner per år vil representere en god start.» [1]

Utvidelse av mandatet til Forsvarets forskningsinstitutt

Forslaget om utvidelse av mandatet til Forsvarets forskningsinstitutt vil innebære at sivile myndigheter må bidra med finansiell støtte til FFI på fast basis.

[1] Innstilling fra en utredningsgruppe nedsatt av Norges forskningsråd 2005. *Samfunnssikkerhet og risikoforskning (SAMRISK)*.

Litteraturliste

Arnesen, Signe Astrup. Bjørgo, Tore. Mærli, Morten Bremer 2004 *Hva gjør Norge utsatt for terrorisme? Trusselscenarier og norsk sårbarhetsforvaltning*. Underlag til Nasjonal sårbarhets- og beredskapsrapport, Direktoratet for samfunnssikkerhet og beredskap (DSB). NUPI.

Aven, Terje og Wiencke, Herman Steen 2005. *Rammeverk for gjennomføring av risiko og sårbarhetsanalyser av samfunnskritisk infrastruktur*. SEROS Senter for risikostyring og samfunnssikkerhet – i NOU 2006:6 *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastruktur og kritiske samfunnsfunksjoner*. Del 2, vedlegg 9.

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

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

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

Davidsen, Bjørnar og Nilsen, Bjørn 2005. *Risikobildet. Notat til infrastrukturutvalget.* Nasjonal sikkerhetsmyndighet – i NOU 2006:6 *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastruktur og kritiske samfunnsfunksjoner.* Del 2, vedlegg 6.

Department of Homeland Security 2004. *National Response Plan*. December 2004.

Dokument nr. 3:4 (2005-2006). *Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur.*

DSB-rapport 2004. *Erfaringer etter terrorangrepet i Madrid Krisehåndtering og ressurstilgjengelighet i forbindelse med en tenkt tilsvarende hendelse i Oslo.*

DSB-rapport 2005. *Nasjonal sårbarhets- og beredskapsrapport 2004. NSBR-04*. Direktoratet for samfunnssikkerhet og beredskap (DSB). (Unntatt offentlighet)

DSB-rapport 2006. *Nasjonal sårbarhets- og beredskapsrapport 2005. NSBR-05. Håndtering av store hendelser og potensiell aldring i kritiske infrastrukturer*. Direktoratet for samfunnssikkerhet og beredskap (DSB). Internettutgaven.

ECON-notat nr. 2005-05. *Kritisk infrastruktur og offentlig eierskap* - i NOU 2006:6 *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastruktur og kritiske samfunnsfunksjoner*. Del 2, vedlegg 12.

ECON-rapport 2004:005. *Konsekvenser av ny regulering i VA-sektoren i kommunene.*

ECON-rapport 21/01. *Robust forsyningsevne i krig og fred.*

Fakta Olje- og energidepartementet og Oljedirektoratet 2005. *Norsk petroleumsverksemd.*

Fridheim, Håvard et.al. 2005. *Nasjonal autonomi for elektroniske kommunikasjonsnett og -tjenester*. Forsvarets forskningsinstitutt. FFI/Rapport-2005/00175 (BEGRENSET).

Hagen, Janne Merete. Nystuen, Kjell Olav. Fridheim, Håvard og Rutledal, Frode 2000. *Norsk kraftforsyning – Dagens system og fremtidig utvikling.* Forsvarets forskningsinstitutt. FFI-rapport 2000/04450.

Hagen, Janne og Fridheim, Håvard 2005. *Hva er kritisk infrastruktur?* Forsvarets forskningssinstitutt. Notat 2005/00363 – i NOU 2006:6 *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastruktur og kritiske samfunnsfunksjoner.* Del 2, vedlegg 1.

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

Høringsutkast Moderniseringsdepartementet 2005. *En veileder ved utskilling av virksomhet fra staten*. Høringsutkast april 2005.

Innst. S. nr. 9 (2002–2003). *Innstilling fra forsvarskomiteen og justiskomiteen om samfunnssikkerhet - Veien til et mindre sårbart samfunn.*

Innstilling fra arbeidsgruppe oppnevnt av Kultur- og kirkedepartementet (via Medietilsynet) for vurdering av videre utbygging, rammevilkår og modeller for digital radio (DAB) 2005. *Digitalradio i Norge.*

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

International CIIP Handbook 2004. *An Inventory and Analysis of Protecion Policies in Fourteen Countries.* Eidgenössische Technische Hochschule Zürich (ETH).

Lavik, Randi 2001. *Dagligvaretilgang i ulike regioner – utvikling 1980-2000*. Statens institutt for forbruksforskning. Rapport 5-2001.

Lia, Brynjar 2004. *Nye aksjonsformar i internasjonal terrorisme: Konsekvensar for norsk samfunnstryggleik*. Innspel til Nasjonal sårbarhets- og beredskapsrapport, Direktoratet for samfunnssikkerhet og beredskap (DSB) 2004. Forsvarets forskningssinstitutt.

Lia, Brynjar og Nesser, Petter 2005. *Terror mot jarnvegar: Eit oversyn over typiske terroraksjonar mot togpassasjertransport.* Forsvarets forskningssinstitutt. FFI Rapport-2005/01451.

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

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

Norges Bank 2004. *Årsrapport om betalingsformidling 2004.*

NORVAR-rapport 130/2003. *Gjenanskaffelseskostnader for norske vann- og avløpsanlegg.*

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

NOU 2001:31 Når ulykken er ute. *Om organiseringen av operative rednings- og beredskapsressurser.*

NOU 2003:14 *Bedre kommunal og regional planlegging etter plan- og bygningsloven II.*

NOU 2004:7 *Statens forretningsmessige eierskap. Organisering og forvaltning av eierskapet.*

NOU 2004:26 *Hjemfall.*

Nærings- og handelsdepartementet og Landbruksdepartementet 2002. *Risiko- og sårbarhetsanalyse av dagligvareforsyningen til Nord-Norge.*

Ot.prp. nr. 49 (1996-97) *Om lov om forebyggende sikkerhetstjeneste (sikkerhetsloven).*

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

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

Politiets sikkerhetstjeneste (PST) 2005. *Politiets sikkerhetstjenestes ugraderte trusselvurdering 2005.*

Prosjektrapport Energimyndigheten 2004. *Ökad samverkan för den svenska elforsörjingens säkerhet och beredskap.* HEL-projektet.

Rapport fra en tverretatlig arbeidsgruppe 2002. *NTP 2006-2015. Strategiske analyser. Virkninger av klimaendringer for transportsektoren - forstudie.* Jernbaneverket, Kystverket, Luftfartsverket, Statens vegvesen

Rapport fra evalueringsutvalget for flodbølgekatastrofen i Sør-Asia 2005. *26/12.*

Scandpower Risk Management, Forsvarets forskningsinstitutt, Aquateam, Hjellnes-COWI 2003. *Sårbarhet i vannforsyningen.*

SINTEF-rapport 2005. *Brytningstider for vann- og avløpssektoren? Om konsekvenser for kommunene av en eventuell liberalisering.*

SL RAP 35/2005. *Flysikkerhet i norsk luftfart under omstillingsprosesser.* Havarikommisjonen for sivil luftfart og jernbane.

St. meld. nr. 24 (2003-2004) *Nasjonal transportplan 2006-2015.*

St.meld. nr. 17 (2001-2002) *Samfunnssikkerhet. Veien til et mindre sårbar samfunn.*

St.meld. nr. 19 (2002-2003) *En verden av muligheter - globaliseringens tidsalder og dens utfordringer.*

St.meld. 22 (2001-2002) *Et mindre og bedre statlig eierskap.*

St.meld. nr. 37 (2004-2005) *Flodbølgekatastrofen i Sør-Asia og sentral krisehåndtering.*

St.meld. 38 (2003-2004). *Om petroleumsvirksomheten.*

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

St.meld. nr. 42 (2004-2005) *Politiets rolle og oppgaver.*

St.prp. nr. 1 (2004-2005) for Justis- og politidepartementet.

St.prp. nr. 1. Tillegg nr. 3 (2004-2005).

St.prp. nr. 42 (2003-2004) *Den videre moderniseringen av Forsvaret i perioden 2005-2008. Strategisk konsept for Forsvaret 2005-2008. Styrke og relevans.*

Statistisk sentralbyrå 2005. *Naturressurser og miljø 2005.*

Statistisk sentralbyrå 2005. *KOSTRA: Kommunal avløpsstatistikk 2004.*

Statistisk sentralbyrå 2005. *KOSTRA: Kommunal vannforsyning 2004.*

Statskonsult 2005. *Ivaretagelse av sikkerhet og beredskap i fristillingsprosesser* – i NOU 2006:6 *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastruktur og kritiske samfunnsfunksjoner.* Del 2, vedlegg 10.

Statskonsult 2005. *Statlige styringsmidler – Sikkerhet og beredskap – i NOU 2006:6 Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastruktur og kritiske samfunnsfunksjoner.* Del 2, vedlegg 8.

Synstnes, Hans M. 2005. *Navigasjonssystemer og samfunnssikkerheten. Arbeidsnotat til Infra-*

strukturutvalget. Nasjonal sikkerhetsmyndighet – i NOU 2006:6 *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastruktur og kritiske samfunnsfunksjoner.* Del 2, vedlegg 11.

Sørli, Kjetil 2005. Notat – *Et blikk på begrepet samfunnssikkerhet for å operasjonalisere »nasjonal trygghetsfølelse»*. Direktoratet for samfunnssikkerhet og beredskap – i NOU 2006:6 *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastruktur og kritiske samfunnsfunksjoner*. Del 2, vedlegg 4.

Sørli, Kjetil 2005. *Notat – om definisjonen av kritisk infrastruktur*. Direktoratet for samfunnssikkerhet og beredskap – i NOU 2006:6 *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastruktur og kritiske samfunnsfunksjoner.* Del 2, vedlegg 2.

Sørli, Kjetil 2005. *Oppfølging av sårbarhetsutvalgets rapport. Delrapport til Utvalg for sikring av landets kritiske infrastruktur*. Direktoratet for samfunnssikkerhet og beredskap – i NOU 2006:6 Når sikkerheten er viktigst. *Beskyttelse av landets kritiske infrastruktur og kritiske samfunnsfunksjoner*. Del 2, vedlegg 7.

Sørli, Kjetil 2005. *Sårbarhet i kritisk infrastruktur – utfordringer. Innledende utredning om kritisk infrastruktur til Utvalg for sikring av landets kritiske infrastruktur*. Direktoratet for samfunnssikkerhet og beredskap – i NOU 2006:6 *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastruktur og kritiske samfunnsfunksjoner.* Del 2, vedlegg 3.

Vinje, Finn-Erik 2005. *Sikkerhet – Safety/Security. En begrepsutredning* – i NOU 2006:6 *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastruktur og kritiske samfunnsfunksjoner*. Del 2, vedlegg 5.

White House 2003. *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* February 2003

White House 2003. *The National Strategy to Secure Cyberspace*. February 2003

Møteliste

Nedenfor følger en liste over de virksomheter, organisasjoner og enkeltpersoner som utvalget med sin tids- og ressursramme har hatt mulighet til å møte. Det gjøres oppmerksom på at det har vært avholdt flere møter med enkelte av disse. I tillegg kommer møter hvor utvalget har orientert om sitt arbeid.

- Andøya Rakettskytefelt
- Apenes, Georg (Datatilsynet)
- Arbeids- og sosialdepartementet
- Avinor
- BaneTele
- Beredskapsforum for statlig varekrigsforsikring
- Beredskapsutvalget for finansiell infrastruktur (Norges Bank, Kredittilsynet og Bankenes Betalingssentral)
- Bjørgo, Tore
- Bundesamt für Bevölkerungsschutz und Katastrofenhilfe, Tyskland
- Bundesamt für Sicherheit in der Informationtechnik, Tyskland
- Bygg- og anleggforum
- Department of Homeland Security, USA
- Det norske Veritas
- Direktoratet for samfunnssikkerhet og beredskap
- Dørum, Odd Einar (Justisminister)
- Electronic Security Products
- Energibedriftenes landsforening
- Energimyndigheten, Sverige
- Energiveteranene (v/Hans O. Bjøntegård og Erling Diesen)
- Ericsson, Norge
- Etterretningstjenesten
- EU-delegasjonen i Brussel v/justisråden, energiråden og transportråden
- Federal Bureau of Investigation, USA
- Federal Office for National Economic Supply, Sveits
- Federal Office of Communication, Sveits
- Fiskeri- og kystdepartementet
- Forsikringsforum
- Forsvarets forskningsinstitutt (TERRA og BAS)
- Forsvarsdepartementet
- Fylkesmannen i Nordland
- Fylkesmannen i Rogaland
- Gassco
- Geodata
- George Mason University, USA
- Heritage Foundation, USA
- Home Office, Storbritannia
- Hovden, Jan (Norges teknisk-naturvitenskapelige universitet)
- Hovedredningssentralen i Nord-Norge
- Hovedredningssentralen i Sør-Norge
- Hydro
- Industry Canada, Canada
- Islamsk råd Norge
- Justis- og politidepartementet
- Kommunenes Sentralforbund
- Kongsberg D&A
- Kongsberg Satellite Services
- Koordineringsutvalget for informasjonssikkerhet (KIS)
- Krisberedskapsmyndigheten, Sverige
- Kultur- og kirkedepartementet
- Kvarme, Ole Christian Mælen (Biskop i Oslo)
- Kystdirektoratet/Kystverket
- Landsorganisasjonen
- Longyearbyen Lokalstyre
- Luftfartstilsynet
- Lyse
- Melde- und Analysestelle Informationssicherung, Sveits
- Microsoft, Norge
- Ministry of Home Affairs, Singapore
- Ministry of the Interior and Kingdom Relations, Nederland
- Moderniseringsdepartementet/Fornyings- og administrasjonsdepartementet
- Nasjonal sikkerhetsmyndighet
- National Defence University, USA
- National Infrastructure Security Coordination Centre, Storbritannia
- National Security Advice Centre, Storbritannia
- NATO (Civil Protection Committee)
- NorCERT/Varslingssystem for digital infrastruktur
- Nordområdeutvalget
- Norges rederiforbund
- Norges vassdrags- og energidirektorat
- Norsk polarinstitutt

- Norsk rikskringkasting
- Norsk Romsenter
- NORUT IT, Tromsø
- Nærings- og handelsdepartementet
- Næringslivets hovedorganisasjon
- Næringslivets sikkerhetsorganisasjon
- Næringslivets sikkerhetsråd
- Nødnettprosjektet
- Olje- og energidepartementet
- Oljedirektoratet
- Oljeindustriens landsforening
- Oseberg C-plattformen – Hydro
- Oslo Kommune – beredskapsetaten
- Oslo Kommune – vann- og avløpsetaten
- Petroleumstilsynet
- Politidirektoratet
- Politiets sikkerhetstjeneste
- Politimesteren i Rogaland
- Post- og teletilsynet
- Prosjektgruppen for Sivilforsvarsloven
- Public Safety and Emergency Preparedness Canada, Canada
- Reiten, Eivind
- Riksantikvaren
- Rikstrygdeverket
- Rogalandsforskning
- Ryssdal, Kristine
- Røde Kors
- Samferdselsdepartementet
- Sjøfartsdirektoratet
- Smith, Eivind
- Sosial- og helsedirektoratet
- Standard Norge
- Statens havarikommisjon for transport
- Statens helsetilsyn
- Statens jernbanetilsyn
- Statkraft
- Statnett
- Statoil
- Statsministerens kontor
- Storberget, Knut (Justisminister)
- SvalSat, Longyearbyen
- Sysselmannen på Svalbard
- Telenor ASA
- Telenor Svalbard
- Thales
- Totalforsvarsforum Østlandet
- Universitetet i Stavanger
- Universitetet i Tromsø
- VA-nett
- Vegdirektoratet/Statens vegvesen
- Veolia Water
- Verdipapirsentralen
- Vinje, Finn-Erik
- Vogt, Kari
- Willoch, Kåre
- Yara

Forkortelser[1]

AMK-sentraler: Akuttmedisinske kommunikasjonssentraler
ARBC: Kjernefysiske, Radiologiske, Biologiske, Kjemiske
BAS: Beskyttelse av samfunnet
BBS: Bankenes Betalingssentral
BFF: Beredskapssystemet for Forsvaret
BFI: Beredskapsutvalget for finansiell infrastruktur
CEP: Civil Emergency Planning
CERT: Computer Emergency Response Team
CIIP: Critical Information Infrastructure Protection
CIP: Critical Infrastructure Protection
CIWIN: Critical Infrastructure Warning Information Network
COSPAS/SARSAT: Cosmicheskaya Sistyema Poiska Avariynich Sudov (Space System for the Search of Vessels in Distress)/Search and Rescue Satellite-Aided Tracking
CRN: Comprehensive Risk Analysis and Management Network
DAB: Digital Audio Broadcasting
DHS: Department of Homeland Security (USA)
DSB: Direktoratet for samfunnssikkerhet og beredskap
EOS-tjenestene: Etterretnings-, overvåknings- og sikkerhetstjenestene, dvs. Etterretningstjenesten, Politiets sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet.
EPCIP: European Programme for Critical Infrastructure Protection
ESA: European Space Agency
ETH: Eidgenössische Technische Hochschule (Sveits)
EU: Den europeiske union
EUMETSAT: European Organisation for the Exploitation of Meteorological Satellites
FD: Forsvarsdepartementet
FFI: Forsvarets forskningsinstitutt
FKD: Fiskeri- og kystdepartementet
FSK: Forsvarets spesialkommando
GPS: Global Positioning System
HMS: Helse, miljø og sikkerhet
HRS: Hovedredningssentral
IKT: Informasjons- og kommunikasjonsteknologi
IMO: International Maritime Organisation
ISP: Internet Service Provider
ISPS-koden: International Ship and Port Facility Code
JD: Justis- og politidepartementet
KBM: Krisberedskapsmyndigheten (Sverige)
KBO: Kraftforsyningens beredskapsorganisasjon
KILE: Kvalitetsjusterte inntektsrammer ved ikke levert energi
KKD: Kultur- og kirkedepartementet
KRIPOS: Den nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet
KRU: Koordinerings- og rådgivningsutvalget for etterretnings- og sikkerhetstjenestene
LMD: Landbruks- og matdepartementet
LRS: Lokal redningssentral
LV-sentraler: Lokale legevaktssentraler
MSIS: Meldingssystem for smittsomme sykdommer
NARRE: Nasjonalt ressursregister for redning og beredskap
NATO: North Atlantic Treaty Organisation
NAV: Ny arbeids- og velferdsforvaltning
NBS: Nasjonalt Beredskapssystem
NCRS: NATO Crisis Response System
NHD: Nærings- og handelsdepartementet
NICS: Norwegian Interbank Clearing System
NISCC: National Infrastructure Security Coordination Centre (Storbritannia)
NorCERT: Norwegian Computer Emergency Response Team

[1] Forkortelser fra kapittel 12 - Beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner i andre land er bare i liten grad tatt med i listen over forkortelser. Forkortelsene i kapittel 12 er forklart i løpende tekst.

NOAA: National Oceanic and Atmospheric Administration (USA)
NOS: Norsk Oppgjørssentral
NSM: Nasjonal sikkerhetsmyndighet
NUPI: Norsk utenrikspolitisk institutt
NVE: Norges vassdrags- og energidirektorat
OECD: Organisasjonen for økonomisk samarbeid og utvikling
PDMT: Politiets data- og materielltjeneste
PHS: Politihøgskolen
PRS: Public Regulated Service
PSEPC: Public Safety and Emergency Preparedness Canada (Canada)
PST: Politiets sikkerhetstjeneste
PT: Post- og teletilsynet
PU: Politiets utlendingsenhet
ROS-analyser: Risiko- og sårbarhetsanalyser
SAMRISK: Forskningsprogrammet samfunnssikkerhet og risikoforskning
SBS: Sivilt Beredskapssystem
SCADA: Supervisory Control and Data Acquisition
SDØE: Statens direkte økonomiske engasjement
SIS: Senter for informasjonssikring
SMK: Statsministerens kontor
SWIFT: Society for Worldwide Interbank Financial Telecommunication
TSU: Tekniske sikkerhetsunderskelser
UP: Utrykningspolitiet
VA: Vann- og avløp
VDI: Varslingssystem for Digital Infrastruktur
VPS: Verdipapirsentralen
WHO: Verdens helseorganisasjon
ØKOKRIM: Den sentrale enhet for etterforsking og påtale av økonomisk kriminalitet og miljøkriminalitet

Del II
Vedlegg

Vedlegg 1

Hva er kritisk infrastruktur?

Hagen Janne, Fridheim Håvard, Forsvarets forskningsinstitutt
FFI/NOTAT-2005/00363

1 Innledning

Hensikten med dette notatet er å drøfte begrepet kritisk infrastruktur nærmere. Drøftingen gjøres med utgangspunkt i forskningen som er gjort i prosjektserien «Beskyttelse av samfunnet» (BAS), som Forsvarets forskningsinstitutt (FFI) har arbeidet med siden 1994.

BAS ga ut rapporten «Viktige samfunnsfunksjoner» i 1997 (1). Rapporten beskrev hvilke funksjoner i samfunnet som ville være viktige for nasjonal krisehåndtering og ga en rangering av de mest kritiske funksjonene. Dette arbeidet har blitt brukt flittig som innspill til offentlige utredninger og grunnlagsdokumenter innen sivilt beredskap i de seneste årene

Imidlertid har verden gått videre etter at denne rapporten ble skrevet, og en del sentrale rammebetingelser for beredskapsarbeidet i Norge er vesentlig endret siden midten av 90-tallet. I tillegg har internasjonal forskning innen samfunnssikkerhet arbeidet mye med å identifisere det som kan kalles «kritiske infrastrukturer», et begrep som det første BAS-prosjektet ikke benyttet. Problemstillingen med å identifisere kritiske funksjoner i samfunnet er med andre ord minst like aktuell i dag som den var for 10 år siden. Det er derfor hensiktsmessig ta et kritisk blikk på FFIs tidligere arbeider innen dette feltet i lys av utviklingen som har skjedd.

BAS5-prosjektet «Critical Information Infrastructure Protection», som skal pågå frem til slutten av 2006, vil også sette søkelyset på kritiske samfunnsfunksjoner og infrastruktur. FFI vil her arbeide sammen med Direktoratet for samfunnssikkerhet og beredskap (DSB) for å identifisere og rangere samfunnskritiske funksjoner og kritisk infrastruktur. Imidlertid er det ønske om noen foreløpige resultater allerede nå, i forbindelse med oppstarten av Infrastrukturutvalget. Dette notatet er derfor utviklet i løpet av kort tid (en drøy uke) for å oppsummere de arbeidene FFI har gjort tidligere, og for å gjøre en første vurdering hva som er de kritiske infrastrukturene i dagens samfunn.

2 Formålet med og avgrensninger for notatet

Begrepsbruken knyttet til infrastruktur er ikke konsistent. Ulike begreper benyttes for samme forhold, uten at det finnes klare definisjoner. Knyttet til infrastruktur kommer en bl.a. fort borti uttrykk som samfunnsfunksjoner, samfunnssektorer, tjenester osv. Ting blir ikke bedre av at begrepsbruken varierer internasjonalt. Norge har et rikt ordforråd for forhold knyttet til begrepet «samfunn» og kan lett bruke avledninger av dette. Den direkte engelske oversettelsen «society» har ikke den samme omfattende og mangfoldige betydningen, og et begrep som «societal function» (råoversettelse av samfunnsfunksjon) gir ingen mening. På engelsk vil man derfor se ordet «infrastructure» brukt i stedet.

Videre er det en utfordring at begrepene ofte suppleres med forsterkende ord som «viktig», «kritisk» osv., uten at det finnes klare kriterier for hvorfor disse er brukt. Er det noen forskjell mellom kritiske infrastrukturer og viktige samfunnsfunksjoner, eller uttrykker dette samme sak?

Et annet spørsmål er om infrastruktur kun betegner fysiske nettverk som man kan «ta og føle på», eller om mer abstrakte og sosiale forhold også må inkluderes i begrepet. De fleste vil vel være enige i at det norske strømnettet er en infrastruktur[1], men hva med forhold som sosiale nettverk, organiseringen av sivilt beredskap og prosesser for saksbehandling og beslutninger i departementene? Utgjør dette også infrastrukturer?

Dette er forhold som BAS5-prosjektet vil se nærmere på i sitt arbeid de nærmeste månedene. Dette notatet vil derfor ikke gi alle svar, men i alle fall reise problemstillingene overfor Infrastrukturutvalget. Det gjøres imidlertid et forsøk på å skille begrepene «kritisk infrastruktur» og «samfunnsfunksjon». Notatet presenterer et forslag til definisjon av disse begrepene, basert på en «bottom up-

[1] Sågar en kritisk en

tilnærming» av hva samfunnets leverer til sine beboere. Det gjøres også et forsøk på å spesifisere hva som er de kritiske infrastrukturene. Det må imidlertid understrekes at dette er foreløpige arbeider, og at FFI forbeholder seg retten til å gå rett inn i svingdøren og endre tilnærming på et senere stadium i prosjektarbeidet.

Innledningsvis gir notatet en beskrivelse av de resultatene som BAS har levert tidligere innen denne problemstillingen (kapittel 3). Deretter presenteres en gjennomgang av sentrale rammebetingelser for samfunnssikkerhet og sivilmilitært samarbeid i Norge: totalforsvarstenkningen, beredskapsprinsipper, trusselbildet og generell samfunnsutvikling (kapittel 4). Det pekes på hva som har vært de største endringene innen disse feltene fra midten av 90-tallet og til i dag.

Den viktigste delen av notatet er diskusjonen rundt hva som er de kritiske infrastrukturer i dagens samfunn og hvilke avgrensninger som kan gjøres for dette begrepet (kapittel 5). Store deler av terminologidiskusjonen er plassert der. Notatet oppsummeres til slutt i kapittel 6.

3 BAS-prosjektene og «Viktige samfunnsfunksjoner»

I Norge var FFI tidlig ute med å ta tak i problemstillingen med å identifisere viktige samfunnsfunksjoner. Det første BAS-prosjektet gjennomførte en analyse av samfunnsviktige funksjoner i 1997 og kategoriserte disse etter viktighet (1). Som tidligere nevnt benyttet ikke BAS begrepet «kritisk infrastruktur» i sin 1997-rapport, men de funksjonene som ble pekt på som mest kritiske var alle basert på grunnleggende teknologiske infrastrukturer i samfunnet: *kraftforsyning, telekommunikasjon, transport, ledelse/informasjon og olje-/drivstofforsyning.*

Analysen så på samfunnet som et produksjonsapparat som skulle understøtte sivilbefolkningens ve og vel og Forsvarets behov i en krise eller under militært angrep på landet. Arbeidet ble gjort med utgangspunkt i et bredt trusselbilde. Selv om trusselbildet på midten av 90-tallet fremdeles fokuserte på faren for en militær invasjon, ble BAS-prosjektets analyse gjennomført med bakgrunn i et bredere scenariogrunnlag:

- Kortvarige militære angrepsscenarier (for eksempel begrensede angrep mot Finnmark)
- Terror- og sabotasjeangrep
- Ulike fredstidsscenarier, som naturkatastrofer, kriminalitet, ulykker osv.

Tidligere beskrev det sivile beredskap flere beredskapsprogrammer som kan knyttes til samfunnsfunksjoner (se f.eks. St.meld. nr. 48 (1993-94)) (2). Beredskapsprogrammene hadde som formål å sørge for at Forsvaret fikk nødvendig støtte i en krise eller krig, at samfunnet fungerte så godt som mulig i alle situasjoner og at sivilbefolkningen fikk best mulig beskyttelse. Her var det tenkt helhetlig i forhold til å opprettholde samfunnets funksjoner i kriser og i krig. Gjennom å bearbeide listene over beredskapsprogrammer definerte det første BAS-prosjektet følgende samfunnsfunksjoner:

1. Ledelse/informasjon
2. Kraftforsyning
3. Telekommunikasjon
4. Olje- og drivstofforsyning
5. Transport
6. Arbeidskraft
7. Vannforsyning
8. Bank- og pengevesen
9. Bygg og anlegg
10. Industri og varehandel
11. Helse
12. Ernæring
13. Brann og redning
14. Politi og orden

Disse 14 samfunnsfunksjonene må ses på som en svært grov inndeling av samfunnet, som var basert på tidligere tenkning på hvordan samfunnet og offentlig sektor var bygd opp og planlagt å fungere i krisesituasjoner. Funksjonenes innbyrdes betydning for samfunnet ble analysert, og konklusjonen var at sterke gjensidige avhengigheter ville gi dominoeffekter for resten av samfunnet dersom svikt oppstod i en av funksjonene. Dette kunne potensielt gi alvorlige begrensninger i evnen til å håndtere kriser. En viktig konklusjon var også at gjensidige avhengigheter mellom ulike samfunnsfunksjoner ikke gjorde det mulig å utelukke noen i beredskapssammenheng. Alle er mer eller mindre viktige, men noen er mer kritiske enn andre og har rollen som bærebjelker for all øvrig samfunnsvirksomhet.

I ettertid kan det hevdes at dette ikke er noen uttømmende og fullstendig liste, og at den er sterkt preget av en tradisjonell teknologisk/mekanisk forståelse av hvordan samfunnet fungerer. Rapporten understreket da også at resultatene var usikre, og at de måtte ses på som en pekepinn på hvordan identifikasjon av viktige samfunnsfunksjoner kunne gjøres. Til tross for dette fikk rapporten en relativt stor gjennomslagskraft som underlagsdokument innen sivilt beredskap. Dette gjelder blant annet en matrisepresentasjon av gjensidige avhen-

gigheter mellom de ulike samfunnsfunksjonene, som ofte benyttes i offentlige utredninger og stortingsmeldinger.

4 Forutsetninger og rammebetingelser for samfunnssikkerhet

BAS-arbeidene om samfunnsviktige funksjoner ble gjennomført for snaut 10 år siden. Etter dette har det skjedd store endringer i rammebetingelsene for arbeidet med samfunnssikkerhet i Norge:

- Tenkningen rundt sivilt beredskap er en annen i dag enn for 10 år siden
- Trusselbildet har endret seg
- Utviklingen i samfunnet har gått svært raskt de siste årene.

Dette kapittelet peker på de viktigste utviklingstrekkene innen rammebetingelsene for samfunnssikkerhet. Disse rammebetingelsene stod sentrale i BAS-prioriteringen av samfunnsviktige funksjoner, og de vil også være viktige parametre for å kunne peke på hva som er samfunnsviktige funksjoner og kritisk infrastruktur i dag.

4.1 Fra totalforsvarskonseptet til samfunnssikkerhet

Totalforsvarskonseptet var en ramme rundt de første BAS-prosjektene. Konseptet ble utviklet med utgangspunkt i lærdommene etter andre verdenskrig, og bestod av to pilarer: det militære forsvaret og det sivile beredskap. Hovedtanken bak konseptet var at alle landets ressurser, både sivile og militære, offentlig og private i fellesskap, skulle bidra til forsvaret av landet ved krise eller krig.

Tidligere innebar totalforsvarskonseptet et sterkt fokus på hva sivilsamfunnet kunne gjøre for å understøtte Forsvarets militære organisasjon og dens ressursbehov under en krisesituasjon. I dag er det mange som legger mer vekt på hva Forsvaret kan gjøre for å støtte det sivile samfunnet i krisesituasjoner. Men det er på sin plass å peke på at det gjensidige avhengighetsforholdet mellom Forsvaret og sivil sektor fremdeles er til stede, og at Forsvaret i økende grad er i ferd med å bli avhengig av sivile ressurser som en konsekvens av omstillingsarbeidet som nå pågår (3). Forsvaret vil ikke være noen isolert organisasjon som fungerer uavhengig av sivilsamfunnet når tjenester settes bort til private leverandører og nye former for privat-offentlig samarbeid og avhengighet tvinger seg frem.

De siste årene har totalforsvaret som begrep fått redusert betydning. St.meld. nr.17 (2001-2002) «*Samfunnsikkerhet - Veien til et mindre sårbart samfunn*» representerte et veiskille i så måte (4). Her ble totalforsvaret presentert som en del av begrepet samfunnssikkerhet, og det ble omfortolket og betegnet som sivilmilitært samarbeid. I disse dager pågår det en prosess for å forankre denne begrepsforståelsen, og det kan bl.a. henvises til St.meld. nr. 39 (2003-2004) «*Om samfunnssikkerhet og sivilt-militært samarbeid*» for å få eksemplifisert innholdet i begrepene (5).

Det finnes en rekke eksempler på sivilmilitært samarbeid i fredstid og under operasjoner i utlandet. Forsvaret støtter sivilsamfunnet gjennom den daglige redningstjenesten, hjelp under naturkatastrofer, ABCR[2]-beskyttelse, vakthold, beskyttelse av viktige objekter osv. Det sivile samfunnet støtter Forsvaret med bl.a. forsyninger, transportkapasitet og kompetanse som Forsvaret selv ikke har. Ved store kriser nasjonalt finnes det også et sivilmilitært beredskapsplanverk som nylig har vært til revisjon og som kan tas i bruk. I tillegg øves det på sivilmilitær krisehåndtering, både innen enkeltsektorer i samfunnet og på nasjonalstrategisk nivå.

4.2 Prinsippet om ansvar, likhet og nærhet

Disse prinsippene står helt sentralt innenfor sivilt beredskap. Den som har ansvaret innen et område i fredstid, skal også ha det i krise eller i krig. Det skal være minst mulig forskjell mellom normaldrift og krisedrift, og krisen skal håndteres på så lavt nivå og så nært kriseområdet som mulig. Begrunnelsen for denne tilnærmingen er at kriser skal håndteres uten for store omstillinger som bidrar til å øke usikkerhet og fragmentere ansvar.

På dette området har ikke endringene vært veldig store fra 1997 til i dag, selv om prinsippene kanskje ble presisert noe klarere enn tidligere i forbindelse med arbeidet i Sårbarhetsutvalget.

4.3 Trusselbildet

Med erfaringene fra andre verdenskrig friskt i minnet ble totalforsvarskonseptet naturlig nok utviklet for å kunne håndtere en invasjonstrussel mot Norge. I dag er det vanskeligere å spesifisere de dimensjonerende scenariene for arbeidet med samfunnssikkerhet og sivilmilitært samarbeid og ikke minst hvem som har ansvaret for å håndtere ulike trusler. Dette vil også gi føringer for hvilke

[2] Atom, biologisk, kjemisk og radiologisk. Begrepet ABCR referer til truslene fra disse virkemidlene /våpnene.

samfunnsfunksjoner som er viktige for krisehåndteringen.

En utfordring er at krigsbegrepet er problematisk i dagens trusselbilde. Sett fra en folkerettslig synsvinkel er krig å forstå som enhver bruk av militær makt mot en annen stat på en slik måte at det krenker den statlige suverenitet, i praksis angrep som rammer en annen stats territorium eller borgere. Krigens funksjon er altså å regulere forholdet mellom suverene stater.

En slik tilnærming harmonerer i stadig mindre grad med de politiske og militære realiteter. Den utvikling som de senere år mer enn noe annet har bidratt til å sprenge dette bildet er fremveksten av internasjonal terrorisme. Terrorisme kan defineres som politisk motivert voldsanvendelse fra ikke-statlige aktører mot personer eller eiendom, med sikte på legge press myndigheter gjennom å skape frykt i befolkningen. Internasjonal terrorisme er i tillegg karakterisert ved at den er grenseoverskridende, og dermed kan utfordringen bare i begrenset grad håndteres av statenes indre sikkerhetsinstitusjoner. Tradisjonelle militære maktmidler har begrenset relevans siden terroraktører ikke er stater, men i en folkerettslig forstand er å betrakte som private aktører. Man har da beveget seg fra et symmetrisk trusselbilde mellom stater til et mer uklart trusselbilde som er asymmetrisk langs flere dimensjoner –politisk, moralsk, teknologisk og kulturelt.

I tillegg er ikke den sikkerhetspolitiske dimensjonen og rikets sikkerhet lenger de eneste parametrene for arbeidet med sikkerhet, stabilitet og sivilmilitært samarbeid. Ulike økonomiske, miljømessige og ressursmessige forhold må også trekkes frem som relevante.

Hvilke utfordringer kan man i dag se for seg på norsk jord? Akuttscenarier som naturkatastrofer, miljøkatastrofer og storulykker inntreffer mer eller mindre regelmessig, og er en viktig del av det totale trusselbildet. Når det gjelder sikkerhetspolitiske utfordringer er trusselbildet blant annet beskrevet i St.meld. nr. 39 (2003-2004) (5). En sentral forskjell sammenlignet med tidligere er vektleggingen av faren for krig i Norge. Selv om krigsfaren var i ferd med å bli justert ned etter slutten av den kalde krigen, snakket man på midten av 90-tallet fortsatt om muligheten for et omfattende russisk angrep mot Norge på lang sikt. I de nye trusselvurderingene er faren for denne typen scenarier i praksis avskrevet. Selv om Russland fremdeles har betydelig militær kapasitet i våre nærområder, vises det kun til raskt oppstående gråsonesituasjoner eller sikkerhetspolitiske kriser som mulige konfliktsituasjoner. Begrepet «invasjon» er ikke lenger et begrep som brukes.

I stedet har terrortrusselen fått økt betydning. Dette er ikke overraskende etter de siste årenes terroraksjoner, spesielt angrepene mot USA 11. september 2001 og i Madrid 11. mars 2004. Videre har faren for angrep mot informasjonssystemer blitt fremhevet som følge av vår økende avhengighet av IKT-systemer og Internett.

Dreiningen mot kortere og mer akutte trusler gir interessante utfordringer når det gjelder tidsaspektene for beredskapsarbeidet. Overfor invasjonstrusselen ble det forutsatt 3-6 måneders varslingstider. Slike tider er det vanskelig å snakke om i dagens trusselbilde. Å tenke på «det umulige og usannsynlige» blir da en oppgave i seg selv for å bidra til et mest mulig robust samfunn, og bruk av scenarier blir viktig både for forsvarsplanleggingen og for den videre utvikling av det sivile beredskap. Det er en illusjon å tro at man kan få like lett aksept for sikkerhetstenkning mot store, men lite sannsynlige utfordringene som de dagligdagse. Men dersom kriseorganiseringen skal være effektiv, må også fredsorganiseringen ta høyde for større påkjenninger der normal drift vil være vanskelig å opprettholde.

4.4 Samfunnsutviklingen de siste ti år

Det er selvfølgelig ikke mulig å gi et fullstendig bilde av et tiårs samfunnsutvikling i løpet av noen korte setninger. Dette avsnittet gir noen stikkordsmessige betraktninger rundt forskjellen mellom 90-tallet og dagens situasjon.

Flere samfunnsviktige funksjoner har vært utsatt for deregulering og privatiseringsprosesser de siste årene. Resultatet er at samfunnsfunksjoner som tidligere var rent offentlige virksomheter, nå er privatisert eller i større grad avhengige av private leverandører. Eksempler er:

- Dereguleringen av kraftforsyningen på starten av 90-tallet
- Avmonopoliseringen av telemarkedet i 1998
- Løpende privatisering av transporttjenester
- Større innslag av private tjenesteleverandører i tradisjonell offentlig virksomhet, for eksempel helsetjenester, leveranser til Forsvaret, private vakt- og sikkerhetsløsninger osv.

Parallelt med dette har det vært et økende fokus på bedriftsøkonomiske kriterier når det gjelder utviklingen innen samfunnsviktige funksjoner. I dag er det meste av så vel privat som offentlig virksomhet underlagt strenge krav til kosteffektivitet/kostnytte, gjerne over korte tidsperioder (tid utover et par år er «lang tid» i næringslivet). Det blir da vanskeligere å argumentere for langsiktige investeringer, med mindre den potensielle gevinsten er stor.

Et resultat av dette er at samfunnstjenester nå blir utviklet ut fra rene kommersielle kriterier. Dagens nett for mobiltelefoni er for eksempel ikke dimensjonert for å håndtere store sikkerhetsutfordringer, men tar kun sikte på å gi en tilstrekkelig leveringskvalitet i hverdagen.

Et annet resultat er en sterk grad av spesialisering i den enkelte virksomhet. Funksjoner som ligger utenfor virksomhetenes kjerneområde har blitt satt bort til andre leverandører. Disse har ofte kun salgskontorer i Norge, mens ressurser og kompetanse befinner seg i utlandet. Samtidig reduseres egne lagerbeholdninger. Konsekvensen er at virksomheter som tidligere var autonome nasjonalt nå er avhengige av varer og/eller tjenester fra utlandet for å kunne fungere.

Videre er det sterkere til krav til dynamikk og hurtighet i samfunnets prosesser. Teknologiske endringer skjer raskt og implementeres umiddelbart i tjenester overfor brukerne. Kravene til leveringstider blir stadig sterkere, og kundene forventer gjerne at en tjeneste skal leveres i dag, ikke om to uker.

Store deler av denne omleggingen er muliggjort gjennom en eksplosiv utvikling i bruken av elektroniske kommunikasjonstjenester og IKT-systemer. Internett ble for eksempel en kritisk tjeneste mot slutten av 90-tallet.

I tillegg kan det stilles spørsmål om hvorvidt befolkningens evne til å håndtere kriser har blitt redusert i samme periode. Utviklingen der de enkelte innbyggere og familier blir stadig mindre selvforsynte, og dermed stadig mer avhengige av en nærmest kontinuerlig tilgang på viktige varer og tjenester fra samfunnet, har fortsatt i perioden. Dette dreier seg bl.a. om mulighetene for alternativ tilgang til mat, vann og varme dersom grunnleggende samfunnsfunksjoner svikter.

5 Hva er de kritiske infrastrukturene i dag?

5.1 Begrepsavklaring

Som diskutert i kapittel 2 er ikke begrepene knyttet til samfunnssikkerhet entydige. BAS-arbeidene som det er referert til i kapittel 3 heller ga ikke veldig klare skiller på hva en samfunnsfunksjon er kontra en infrastruktur. I dette kapittelet diskuteres disse begrepene, for å presentere et forslag til hvordan disse kan skilles.

I henhold til tradisjonell BAS-tenkning kan samfunnet deles inn i flere samfunnsfunksjoner. En *samfunnsfunksjon* vil med dette være et produkt eller en tjeneste som gir et betydelig bidrag til samfunnet for å opprettholde et minimums kvalitetsnivå[3] innen følgende områder (9):

- Nasjonal og internasjonal lov og orden
- Befolkningens sikkerhet
- Økonomi
- Befolkningens helse
- Økologisk miljø

For begrepet *infrastruktur* finnes det flere definisjoner. Ordboka Merriam-Webster definerer begrepet slik (6):

«*Infrastructure:*

1. *The underlying foundation or basic framework (as of a system or organization)*
2. *The permanent installations required for military purposes*
3. *The system of public works of a country, state, or region; also : the resources (as personnel, buildings, or equipment) required for an activity* «

Med andre ord dreier infrastruktur seg om de grunnleggende ressurser og hjelpemidler som må være på plass for å opprettholde en aktivitet eller tjeneste. I vår sammenheng vil en infrastruktur være de grunnleggende ressurser som må til for å opprettholde en samfunnsfunksjon.

I forhold til samfunnsdrift blir begrepet infrastruktur ofte knyttet til store teknologiske nettverk. Ottawa by har følgende definisjon på infrastruktur i en slik sammenheng (7):

«*Physical structures that form the foundation for development. Infrastructure includes: wastewater and water works, electric power, communications, transit and transportation facilities, and oil and gas pipelines and associated facilities.*»

Som definisjonen over viser er det vanskelig å skille de kabler og rørledninger som disse nettverkene består av fra bygninger, materiell og ressurser som er nødvendig for å drifte eller opprettholde nettene. Grensegangen mellom infrastruktur og samfunnsfunksjon vil også være uklar. Det er for eksempel vanskelig å si hvor et elektronisk kommunikasjonsnett (infrastruktur) slutter og elektronisk betalingsformidling (samfunnsfunksjon) begynner. Definisjonsmessig vil det også kunne argumenteres for at for eksempel «matforsyning» både er en:

- samfunnsfunksjon, der tjenesten er å sørge for at samfunnet har nok mat

[3] Det finnes ingen klare grenser for hva dette minimumsnivået er. Sannsynligvis vil nivået være avhengig av hvilket scenario som skal håndteres.

– infrastruktur, med et produksjonssystem innen landbruk, fiskeri, matvareindustri etc, et distribusjonssystem ut til butikker basert på transporttjenester osv.

Dette trenger likevel ikke å være noe problem, så lenge man klarer å identifisere og spesifisere de en egen kategori av grunnleggende infrastrukturer som all samfunnsvirksomhet er avhengig av. Dette kan da kalles de *kritiske infrastrukturer*. Ut fra diskusjonen over må dette være de nettverkene som brukes innen alle samfunnsfunksjoner for å ivareta basisbehovene til befolkningen og virksomhetene (f.eks. knyttet til vann, varme og energi).

5.2 Kritiske samfunnsfunksjoner og infrastrukturer i dagens samfunn

For å identifisere kritisk infrastruktur er en løsning å benytte en modell som ofte brukes innen elektronisk kommunikasjon. Denne ser på elektronisk kommunikasjon som delt i tre lag:

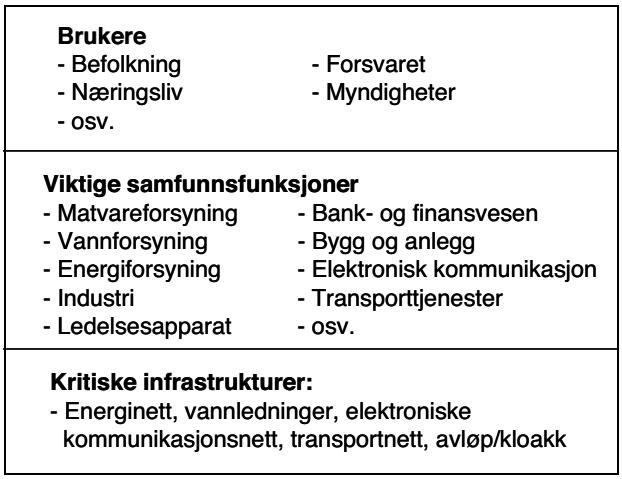
– Et grunnleggende transportnett (telekabler, radiolinjer osv.), som formidler elektronisk trafikk mellom brukere som er geografisk adskilt
– Tjenestenett, som benytter det underliggende transportnettet til å gi brukerne mer raffinerte og funksjonelle teletjenester (for eksempel fasttelefoni, internettjenester, mobiltelefoni)
– Brukerne, som anvender teletjenester

Dersom samme modell anvendes på samfunnet, kan vi si følgende:

– Det finnes noen «transportnettverk» som alle beboere og virksomheter i samfunnet er avhengige av. Dette kan kalles de «kritiske infrastrukturer», som ivaretar samfunnets grunnleggende behov for varme, vann, kommunikasjon osv.
– Mange tjenester i samfunnet er avhengige av de underliggende transportnettene for å gi behovene til befolkning og virksomheter. På overordnet nivå kan disse tjenestene kalles «samfunnsfunksjoner».
– Brukerne i samfunnet, det være seg befolkningen, næringslivet, myndighetene osv., benytter tjenester innen disse samfunnsfunksjonene.

Denne tilnærmingen kan eksemplifiseres som følger:

– Blant de kritiske infrastrukturene finnes nett for overføring av energi (for eksempel strømnett, rørledninger for overføring av olje/gass), nett for elektronisk kommunikasjon, nett for ulike transporttjenester (veg, luft, bane, sjø), ledningsnett for vann og avløp/kloakk. *Disse nettene, sammen med bygninger, materiell og ressurser som er nødvendig for driften av dem, utgjør kritiske infrastrukturer i dagens samfunn.*
– Blant samfunnsfunksjonene finnes tjenester som bank- og finansvesen, helsevesen osv. Alle disse funksjonene er grunnleggende avhengige av de kritiske infrastrukturene. I tillegg kan de ha egne infrastrukturelementer som er bygd for å gi befolkningen best mulig tjenester. Dette kan bl.a. være minibankterminaler knyttet til bankene, sykehus i helsevesenet osv.



Figur 1.1 Samfunnet som tjenestemodell

Dette er skissert i figur 1.1.

5.3 Knutepunkter i nettverkene?

De kritiske infrastrukturene utgjøres altså av nettverk. Innenfor disse kan det identifiseres noder som er viktige for nettverkenes totale funksjonalitet ut fra ulike parametre – relativ betydning i forholdt til systemets totalleveranse, betydning for lokale/regionale leveranser, behovene til Forsvarets/sivilt beredskaps behov osv. Dette er ikke analysert her, men eksempler på slike knutepunkter er:

– Driftssentraler innen kraftforsyningen og elektronisk kommunikasjon
– Transformatorstasjoner inn til byområder
– Trafikkstyringssentraler
– Terminaler på transportsiden

Det er imidlertid vanskelig å konkretisere hva som er de «viktigste» knutepunktene, ikke minst på grunn av sterke gjensidige avhengigheter mellom infrastrukturene. Et godt eksempel på det er den såkalte Østfoldundersøkelsen innen kraftforsynin-

gen, som ble gjennomført for å vurdere muligheten for sonevis utkobling i situasjoner med stor kraftmangel (det ble forutsatt at bare 25% av kraftforsyningen til området var tilgjengelig)[4] . Erfaringene derfra var blant annet at ulike virksomheter var så tett sammenvevd at svikt innen en kritisk infrastruktur fort ville ramme øvrig samfunnsvirksomhet. En analyse av knutepunkter som kun ser på enkeltsektorer, uten å ta hensyn til gjensidige avhengigheter med andre funksjoner, vil derfor ikke nødvendigvis peke ut de mest kritiske punktene for samfunnet som helhet.

En slags konkretisering av knutepunkter kan leses ut av Sikkerhetsloven og tilhørende Objektsikkerhetsforskrift. Her finnes det lister over objekter som skal ha særlig beskyttelse ut fra hensynet til rikets sikkerhet og andre vitale samfunnsinteresser. Det kan imidlertid stilles et spørsmål ved denne listens relevans, sett ut fra dens opprinnelse i forhold til dagens trusselbilde (se kapittel 4.3) og den generelle utviklingen i samfunnet (se kapittel 4.4). Listen er i hovedsak preget av faren for fysiske angrep, og den har ikke tatt særlig høyde for konsekvensene av IKT-utviklingen og nettverkstenkning.

Det kan også nevnes at Sikkerhetsloven kun gjelder statlig virksomhet, noe som er en svakhet i når tendensen er at stadig flere statlige oppgaver overføres til privat sektor og/eller blir organisert ut fra markedsøkonomiske prinsipper. Nye metoder må da tas i bruk for å identifisere og klassifisere kritiske objekter og systemer. En mulig fremgangsmåte er anvendelse av grafteori for å identifisere knutepunktene/nodene i et nettverk og deres relasjoner til andre noder (10). En annen fremgangsmåte er å opparbeide god systemforståelse og identifisere kritiske objekter ut fra ulike kriterier, f.eks. deres andel av systemets totale produksjonskapasitet, deres funksjon/rolle og kritikalitet for systemets helhet.

I appendiks A er det gitt et eksempel på én tilnærming for hvordan slike sentrale objekter/systemer kan identifiseres.

5.4 Kritisk infrastruktur – vår definisjon kontra andres forståelse

Som tidligere nevnt er ikke bruken av begrepet «kritisk infrastruktur» konsistent, verken i Norge eller internasjonalt.

I USA er det nærliggende å kikke på The President's Commission on Critical Infrastructure Protection (PCCIP) (8). De definerte kritisk infrastruktur som:

«*an infrastructure that is so vital that its incapacitation or destruction would have a debilitating impact on defense or economic and the national critical infrastructures*»

Dette er kanskje ikke veldig i uoverensstemmelse med den tilnærmingen som er skissert i kapittel 5.2. Problemet oppstår når PCCIP begynner å liste opp hva som er de kritiske infrastrukturene. I tillegg til åpenbare valg som transport, kraftforsyning og elektronisk kommunikasjon, omtales også følgende som kritisk infrastruktur:

- Emergency preparedness, mao. nødetater og redningstjeneste
- Government services, mao. myndighetsnivå og -tjenester som må til for å dekke befolkningens behov og interesser

Ut fra vårt forslag til definisjon vil ikke dette være kritisk infrastruktur. Men det vil åpenbart være samfunnsfunksjoner som er viktige både i hverdagen og for krisehåndtering.

En annen innvending mot tilnærmingen i kapittel 5.2 er at dette er basert på en strengt teknologisk forståelse av samfunnets virkemåte. Sosiale, verdimessige og kulturelle forhold har da lett for å bli ignorert, for eksempel:

- et effektivt ledelsesapparat
- en velfungerende lovgivning
- et felles verdisyn i samfunnet
- god språkforståelse (felles språk er det beste)

Vår definisjon av kritisk infrastruktur som ensbetydende med grunnleggende teknologiske nettverk kan derfor vise seg å være for snever. Imidlertid tror vi at utgangspunktet med å se på infrastrukturer kontra tjenester kan vise seg å være fruktbar for å avklare begreper og sortere problemstillinger innen dette komplekse området. Så får man eventuelt vurdere om det er infrastrukturene eller samfunnsfunksjonene man ønsker å analysere.

6 Avslutning

BAS-forskningen har hatt som utgangspunkt at samfunnet skal kunne håndtere store påkjenninger i form av kriser uten å bryte fullstendig sammen. Samfunnet må kunne «tåle en støyt», og reduksjon av samfunnets totale sårbarhet er et viktig hjelpemiddel for å sikre dette. For at dette skal kunne være mulig er det viktig å kunne identifisere

[4] Fra arbeidsseminar 4/10-2004 i BAS5-prosjektet, DSB, Oslo; Direktoratet for samfunnssikkerhet og beredskap 2005. Nasjonal sårbarhets og beredskapsrapport 2005

og rangere de viktigste infrastrukturene, samfunnsfunksjonene og knutepunktene i et moderne samfunn.

Notatet forsøker å definere begrepene «samfunnsfunksjoner» og «kritisk infrastruktur». Den prinsipielle forskjellen mellom disse begrepene er at kritisk infrastruktur er de nettverk som er grunnlaget for all annen samfunnsvirksomhet, mens samfunnsfunksjoner er tjenester som benytter de kritiske infrastrukturene for å dekke behovene til befolkningen, virksomheter og aktører i samfunnet. De kritiske infrastrukturene utgjøres av følgende nett, sammen med bygninger, materiell, personell og ressurser som er nødvendig for driften av dem:

- Nett for overføring/distribusjon av energi,
- Nett for elektronisk kommunikasjon
- Nett for transport av gods og personer (veg, luft, bane, sjø)
- Vannledningsnett
- Avløp/kloakknett

Det understrekes likevel at dette ikke er noen endelig liste, og at det ikke er gjort noen ny innbyrdes rangering av disse infrastrukturene. I tillegg innebærer dette en snever fortolkning av begrepet «kritisk infrastruktur», som til dels avviker fra det man ser internasjonalt. Disse forholdene vil være gjenstand for mer arbeid i løpet av BAS5-prosjektet.

Undervedlegg 1

A – Identifikasjon av kritiske punkter innen kritisk infrastruktur

Tabell 1 presenterer et eksempel på oppdeling av kritiske infrastrukturer som kan bidra til å identifisere de viktigste knutepunktene innenfor dem.

En innvending mot en slik statisk og hierarkisk oppdeling er at den ikke tar særlig hensyn til den dynamiske utviklingen innen hver infrastruktur. Den utelukker også ressurser som personell, materiell og kompetanse, og ser ikke på gjensidige avhengigheter mellom nettverkene. Denne måten å tenke på må derfor suppleres med andre metoder, slik at en tar høyde for alle relevante forhold.

Tabellen er heller ikke særlig kvalitetssikret iht. terminologien som gjelder innen den enkelte kritiske infrastruktur. *Den presenteres derfor bare som et eksempel på hvordan dette kan gjøres, ikke som en fasit på hvordan det bør gjøres.*

Tabell 1.1 Inndeling av kritisk infrastruktur

Kritisk infrastruktur	Tjenester	Noder	Nettelementer	Drift
Elektroniske kommunikasjonsnett	Fasttelefoni	Telesentraler/svitsjer (på ulike nivå) Koblingsbokser Hussentraler	Transportnett Aksessnett	Driftssentraler
	Mobiltelefoni	Mobile switching center Basestasjonskontroller Basestasjoner	Transportnett	Driftssentraler
	Internett	NIXer Domenenavnservere Rutere	Transportnett	
Energinett	Kraftforsyning	Produksjonsanlegg Transformatorstasjoner (av ulik størrelse) Koblingsanlegg	Sentralnett Fordelingsnett	Landssentral Regionale sentraler
	Drivstoffforsyning	Plattformer (inkl flytende) Raffinerier Bensinstasjoner	Rørledninger	Kontrollsentre
Transportnett	Vegtransport	Godsterminaler Persontterminaler Kombinerte terminaler	Europaveger Riksveger Fylkesveger Kommunale veger Private veger	Vegtrafikksentral
	Lufttransport	Lufthavner (med og uten internasjonal trafikk	Stamnett Kortbanenett	Luftkontrollsentral
	Jernbanetransport	Matestasjoner Jernbanestasjoner	Fyr	Trafikkstyringsentral
	Sjøtransport	Havner (nasjonale, kommunale, fiskeri, private) Fyr	Sjøleder	Skipstrafikksentral
Vann- og avløpsnett	Vannforsyning	Magasiner Vanntårn Renseanlegg Distribusjonspunkt/ forgreining	Hovedledningsnett Distribusjonsnett	Driftssentral
	Kloakk og avløp	Pumpestasjoner Renseanlegg Oppsamlingsbasseng	Ledningsnett	Driftssentral

Litteratur

1. Fridheim H et al (1997): Viktige samfunnsfunksjoner, FFI/RAPPORT-97/01458, Forsvarets forskningsinstitutt (Begrenset)
2. Justis- og politidepartementet (1993-94): St.meld. nr. 48 (1993-94): Langtidsplanen for det sivile beredskap 1995-98
3. Forsvarsdepartementet (2002-2003): St.prp. nr. 42 (2002-2003): Den videre moderniseringen av Forsvaret i perioden 2005-2008
4. Justis- og politidepartementet (2001-2002): St.meld. nr.17 (2001-2002): Samfunnssikkerhet - Veien til et mindre sårbart samfunn
5. Justis- og politidepartementet (2003-2004): St.meld. nr. 39 (2003-2004): Om samfunnssikkerhet og sivilt-militært samarbeid
6. Merriam-Webster online: http://www.webster.com/cgi-bin/dictionary?book=Dictionary&va=infrastructure
7. City of Ottawa hjemmeside: http://www.ottawa.ca
8. The Presidential Commission on Critical Infrastructure Protection (1997): Final report
9. Hagen J (2004): Beskyttelse av samfunnskritisk informasjonsinfrastruktur - Oppsummering av kjente studier ved starten av BAS5, FFI/NOTAT-2004/02712, Unntatt offentlighet
10. Audestad J (2005): E-bomber eller e-granater - Om IKT og sårbarhet, notat skrevet for BAS5-prosjektet (draft)

Vedlegg 2

Notat – om definisjonen av kritisk infrastruktur

Kjetil Sørli, Direktoratet for samfunnssikkerhet og beredskap,
Enhet for analyse og utredning 19. juli 2005

1 Innledning

Utvalg for sikring av landets kritiske infrastruktur (ISU) har bedt DSB ved enhet for analyse og utredning om innspill til utformingen av en definisjon av kritisk infrastruktur. Utvalget har så langt laget en arbeidsdefinisjon tilpasset norske forhold. Det vil bli hevdet at en annen tilnærming enn arbeidsdefinisjon kan gi et bedre utgangspunkt for en endelig definisjon. Det vil bli hevdet at en annen tilnærming kan være mer intuitiv ved at den tar utgangspunkt i samfunnets grunnleggende verdier.

2 Hvorfor en definisjon?

Hensikten med en definisjon av kritisk infrastruktur er å gi en ramme for, og hjelpe leseren til å forstå hva kritisk infrastruktur er. I seg selv er det en ambisiøs oppgave å beskrive et komplekst område på én eller noen få setninger. Begrensingene er store. En definisjon gjør ikke nødvendigvis leseren i stand til å vurdere om noe konkret er kritisk infrastruktur eller ikke. Til det trengs det en egen metode. Derimot skal en definisjon gi en intuitiv forståelse av hva kritisk infrastruktur er når det arbeides med saksfeltet på et strategisk nivå. Det arbeides for tiden med å utarbeide en egen metode for å identifisere og rangere kritiske samfunnsfunksjoner innenfor forskningsprosjektet BAS5 ved FFI. Metoden vil foreligge i løpet av høsten 2005.[1]

3 Noen definisjoner

Internasjonalt eksisterer det svært mange definisjoner. I USA er det sågar identifisert åtte forskjellige definisjoner i perioden 1983-2004.[2] NATO har sin egen definisjon, og EU-kommisjonen arbeider for tiden med utarbeidelse av en egen definisjon innenfor rammen av EPCIP (European Programme for Critical Infrastructure Protection). Felles for de som presenteres her, er at det er skapt en helhetlig definisjon ut fra én setning. Felles er også at fokus i definisjonene er på konsekvensene for samfunnet ved bortfall og at infrastrukturen er vesentlig for at samfunnet skal fungere. Bruken av kriterier i definisjonen er også fremtredende.

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

USA har følgende definisjon:
Critical infrastructure are systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

NATOs definisjon er som følger:
Critical infrastructure is those facilities, services and information systems which are so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economy, public health and safety and the effective functioning of the government.

EU har en foreløpig arbeidsdefinisjon:
Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security

[1] Merknad februar 2006. Siden notatet ble skrevet er tidspunkt endret til 2006.

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

or economic well-being of citizens or the effective functioning of governments in the Member States.

ISUs arbeidsdefinisjon er som følger:
Kritisk infrastruktur defineres som de objekter, systemer og tjenester som er så viktige for samfunnet at dere manglende funksjonalitet eller ødeleggelse vil medføre svekkelse av rikets sikkerhet, alvorlig svekkelse av den nasjonale økonomi, alvorlig svekkelse av statens myndighetsutøvelse, betydelig tap av liv og helse og/eller betydelig tap av den nasjonale trygghetsfølelse.

De overnevnte definisjonene er bygget opp likt i tre deler. Hvis vi bruker ISUs definisjon som eksempel, så blir det:
1. Kritisk infrastruktur = objekter, systemer, tjenester
2. hvis manglende funksjonalitet eller ødeleggelse vil det
3. medføre svekkelse av rikets sikkerhet, alvorlig svekkelse av den nasjonale økonomi, alvorlig svekkelse av statens myndighetsutøvelse, betydelig tap av liv og helse og/eller betydelig tap av den nasjonale trygghetsfølelse.

Første del etablerer hva infrastruktur er (objekter, systemer, tjenester). Andre del fastslår at bortfall er den aktive faktor. Tredje del lister opp ett sett med grunnleggende verdier/samfunnsfunksjoner(rikets sikkerhet, nasjonal økonomi, statlig myndighetsutøvelse) og kriterier (tap av liv og helse, tap av nasjonal trygghetsfølelse).

4 En annen tilnærming?

Tilnærmingen gjør at brukeren tar utgangspunkt i infrastrukturen og vurderer den opp mot et sett med kriterier, verdier og funksjoner ut fra hva manglende funksjonalitet eller ødeleggelse vil bety. En måte forstå definisjonen er at den stiller spørsmålet: Hvilken infrastruktur sikrer de nevnte verdiene, samfunnsfunksjonene og kriteriene? Med en slik tilnærming kan man for eksempel stille spørsmålet om TV-sendenettet er kritisk infrastruktur. Ut fra ISUs arbeidsdefinisjon vil man stille spørsmålet om manglende funksjonalitet eller ødeleggelse av TV-sendenettet vil medføre *svekkelse av rikets sikkerhet, alvorlig svekkelse av den nasjonale økonomi, alvorlig svekkelse av statens myndighetsutøvelse, betydelig tap av liv og helse og/eller betydlig tap av den nasjonale trygghetsfølelse.* Hvis man får ja på en eller flere, så betyr det at TV-sendenettet er kritisk infrastruktur. Slik kan man fortsette: Medfører manglende funksjonalitet eller ødeleggelse av radio-sendenettet, jernbanelinjer, en passasjerbåt etc *svekkelse av rikets sikkerhet, alvorlig svekkelse av den nasjonale økonomi, alvorlig svekkelse av statens myndighetsutøvelse, betydelig tap av liv og helse og/eller betydlig tap av den nasjonale trygghetsfølelse.* Ved en slik tilnærming blir det en utfordring å velge ut det store antall potensielle objekter, systemer og tjenester som skal testes ut mot verdiene, funksjonene og kriteriene. Dette kan være en omfattende, tungvint og ikke intuitiv tilnærming.

En annen tilnærming er å ta utgangspunkt i samfunnets grunnleggende verdier, utlede hvilke samfunnsfunksjoner som understøtter disse, og ut fra dette intuitivt få en forståelse for hva kritisk infrastruktur er. La oss derfor først søke å identifisere samfunnets grunnleggende verdier, før vi ser videre på kritiske samfunnsfunksjoner.

4.1 Samfunnets grunnleggende verdier

Begrepet viser til verdier som er grunnleggende for å opprettholde samfunnet. I utgangspunktet det et svært omfattende begrep som er vanskelig å avgrense. Det foreligger heller ingen omforent definisjon som presiserer det. Å fylle begrepet med innhold er derfor en subjektiv vurdering preget av hva man ønsker å bruke det til. Forhold som politikk, ideologi og trusseloppfatning bidrar til å forme det.[3] I denne sammenheng er det naturlig å ta utgangspunkt i begrepet slik det er omtalt i dokumenter knyttet til forsvar og samfunnssikkerhet.

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

> Samfunnet skal sikres mot utfordringer mot sentrale samfunnsverdier som liv,
>
> folkehelse og velferd, livsmiljøet, det demokratiske system og dets lovlige institusjoner, nasjonal styringsevne og suverenitet, landets territoriale integritet, materiell og økonomisk trygghet og kulturelle verdier. [4]
>
> ...
>
> Risiko uttrykker fare for tap av viktige verdier som følge av uønskede hendelser. Viktige verdier kan for eksempel være liv og helse,

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

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

> miljø, økonomi og gjennomføring av kritiske samfunnstjenester. [5]
>
> ...
>
> Utvalget legger til grunn at en krise er en hendelse som har potensiale til å true viktige verdier og svekke en organisasjons evne til å utføre viktige funksjoner. [6]

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

> I tillegg til stats-, samfunns- og menneskelig sikkerhet, er det å beskytte velferd, miljø og økonomisk trygghet for det norske folk, grunnleggende norske sikkerhetsinteresser. [...] Videre inngår enkelte grunnleggende verdier som viktige komponenter blant Norges sentrale sikkerhetsinteresser. [...] Norske sikkerhetsinteresser berøres derfor av utfordringer som kan true den internasjonale rettsorden, menneskerettighetene, demokrati, rettsstatens prinsipper, økonomisk trygghet og livsmiljøet.[7]

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

Totalförsvarets forskningsinstitut (FOI) i Sverige beskriver samfunnets grunnleggende verdier som respekt for menneskers verdighet, frihet, demokrati, likhet, rettsstatsprinsippet og menneskerettigheter. De grunnleggende verdiene er felles vurderinger som holder samfunnet sammen. Verdiene holdes oppe av og realiseres gjennom det som blir omtalt som samfunnets vitale interesser.[8] De er:

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

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

De tre nevnte dokumentene identifiserer at noen verdier er viktigere enn andre for et samfunn. De er såkalte grunnleggende verdier og interesser for et samfunn. Dette for å skille dem fra begreper som materielle verdier, økonomiske verdier, kulturelle verdier og lignende. I tillegg kan samfunnsverdier omhandle enkelte som ikke er like relevante i denne sammenheng. Dette kan være samfunnsverdier som å vise toleranse og religionsfrihet. De sistnevnte er eksempler på at en diskusjon om samfunnet grunnleggende verdier vil bevege seg i gråsoner og er gjenstand for subjektive vurderinger. Det er derfor en utfordring å være presis og relevant. Et forsøk på å avgrense for vårt formål, kan som tidligere nevnt, være å omtale samfunnets grunnleggende verdier ut fra forsvar og samfunnssikkerhet, selv om også en slik avgrensing vil åpne for gråsoner og subjektive vurderinger, ikke minst sett på bakgrunn av at begrepet samfunnssikkerhet ikke er et omforent begrep.

4.2 Kritiske samfunnsfunksjoner

Kritiske samfunnsfunksjoner (ev. samfunnskritiske funksjoner) kan bli brukt for å beskrive de funksjonene som drifter samfunnet, og som samfunnet er svært avhengig av for å fungere. Ved bortfall stopper varer og tjenester som befolkningen er avhengig av. På et overordnet nivå er enkelte så kritiske for samfunnet at de omtales som bærebjelker. Bortfall av bærebjelkene vil merkes umiddelbart, og omfatter funksjoner som kraftforsyning, telekommunikasjon, ledelse/informasjon og forsyning av rent vann og ernæring.[9] Renovasjon kan også omtales som en samfunnskritisk funksjon, men bortfall får konsekvenser først på lengre sikt og er derfor ikke en bærebjelke. Hvor kritisk en funksjon er kan også være situasjonsbestemt, eksempelvis funksjonene territorialforsvar og nasjonale beredskapssystemer. Det er først ved gitte situasjoner slike funksjoner er kritiske for samfunnet.

Leveranse av en samfunnskritisk funksjoner er avhengig av tilgang til gitte *ressurser, objekter, systemer og tjenester*. Eksempelvis er funksjonen strøm-

---

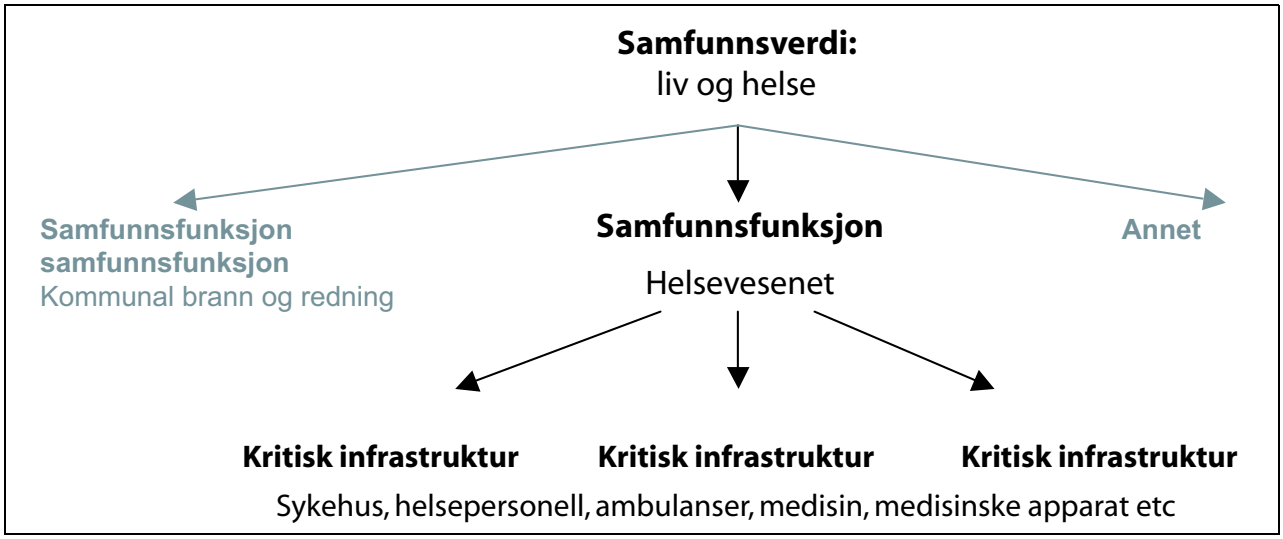
5 St.prp. nr. 42 (2003–2004). Den videre moderniseringen av Forsvaret i perioden 2005–2008.

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

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

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

9 Hæsken O M, Olsen T G, Fridheim H: Beskyttelse av samfunnet (BAS) - Sluttrapport, FFI/RAPPORT-97/01459; Aven, Terje. Boysen, Marit. Njå, Ove. Olsen, Kjell Harald. Sandve, Kjell (2004). Samfunnssikkerhet. Universitetsforlaget; Fridheim H, Hæsken O M, Olsen T G, Balke T, Ensrud M_K: Viktige samfunnsfunksjoner, FFI/RAPPORT-97/01458 (Begrenset)



Figur 2.1

forsyning i Norge avhengig av vann (ressurser), damanlegg (objekter), datakontrollsystemer (systemer) og softwareleverandører (tjenester). Ressursene, objektene, systemene og tjenestene kan omtales som kritisk infrastruktur. På den måten er kritisk infrastruktur den infrastrukturen som samfunnets kritiske funksjoner er avhengig av for å fungere.

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

Samfunnets behov – blir fylt av en funksjon – består av infrastruktur – kan deles i ressurser, objekter, systemer og tjenester.

Fremgangsmåten gir en logisk tilnærming for å vurdere hva som er mest kritisk for samfunnet med utgangspunkt i funksjoner og behov. På den annen side gir den ingen helhetlig tilnærming til hvilken av funksjonene som er mest sårbare og utsatte for bortfall. Sluttrapporten til BAS4 ga en illustrasjon på det. Transport er en kritisk funksjon for samfunnet, men på grunn av stort tilbud, ulike transportformer og redundans ble den ikke vurdert som *sårbar*. Derimot ble den vurdert som *utsatt* for enkelte scenarier så som terrorhandlinger.[10]

5 En tilnærming basert på samfunnets grunnleggende verdier

For å ramme inn de grunnleggende behov og funksjoner kommer samfunnet grunnleggende verdier. Vi har tidligere etablert enkelte av dem, og de kan summeres til å gjelde:

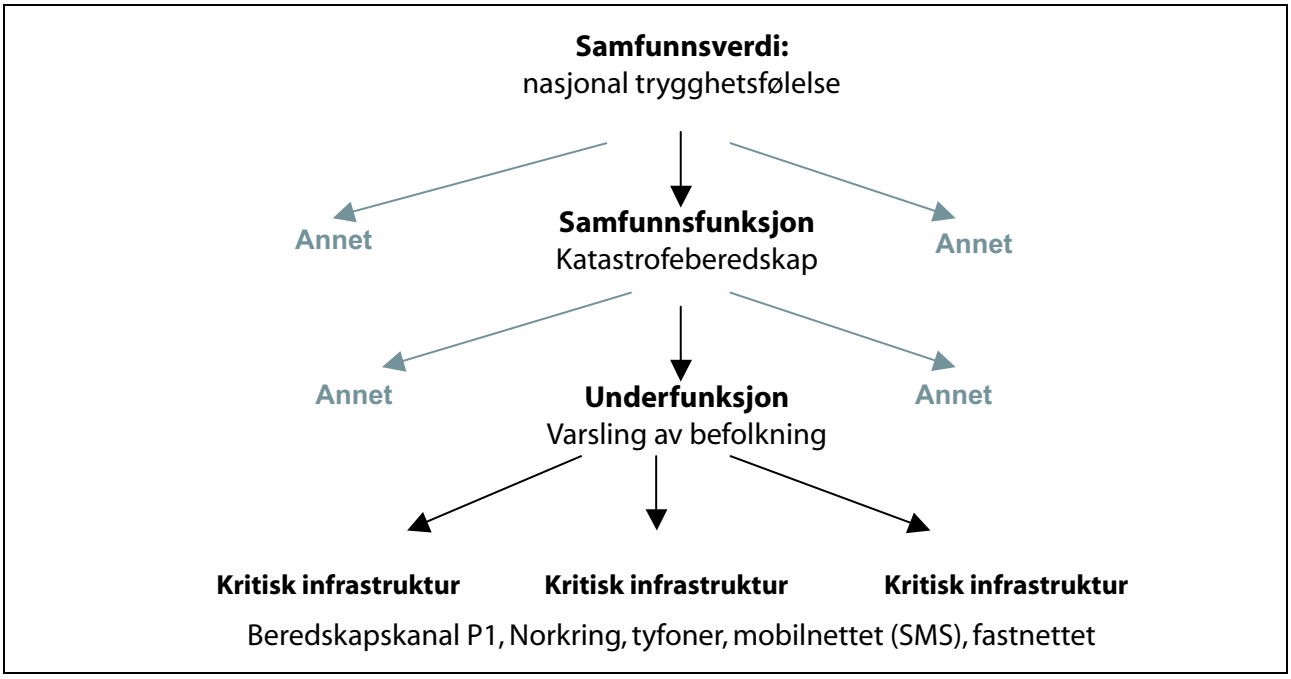
- fred og nasjonal selvstendighet
- en demokratisk rettsstat
- en god samfunnsøkonomi
- velferd
- liv og helse
- livsmiljøet
- nasjonal trygghetsfølelse

Vi får da en logisk kjede, hvor sluttproduktet er kritisk infrastruktur. For eksempel [figur 2.1]:

Legg merke til at en samfunnsverdi er delt opp i flere funksjoner som vist over. En samfunnsfunksjon kan også deles opp i underfunksjoner, som vist i figuren under[figur 2.2]:

Ved en slik tilnærming får vi en diskusjon om hvilke verdier som er samfunnets grunnleggende verdier; de som det er mest kritisk å bevare. Det som blir omtalt som samfunnets grunnleggende verdier blir i denne sammenheng sett opp mot samfunnssikkerhet og forsvar. Det som følger under kommer da som en logisk følge, og vi får en mer intuitiv tilnærming til hva kritisk infrastruktur er.

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



Figur 2.2

6 Hva da med definisjonen av kritisk infrastruktur?

Vi må ha fokus på hva samfunnets grunnleggende verdier er i definisjonen, hvilke funksjoner som sikrer disse, og hvilken infrastruktur som gjør det mulig. Definisjonen må med andre ord ta utgangspunkt i verdier, ikke infrastruktur. Slik arbeidsdefinisjonen fremstår nå stiller den spørsmålet: Hvilken infrastruktur sikrer de nevnte kriterier, funksjoner, verdier? Noe som kan omtales som å være en *nedenfra og opp-tilnærming*. Ved å være eksplisitt i å bruke verdier er vi mer presise og stiller spørsmålet: Hvilke verdier og funksjoner er de mest grunnleggende for samfunnet, og hvilken infrastruktur sikrer dem? Dette kan fremstilles som en *ovenfra og ned-tilnærming*. Ved å ta utgangspunkt i verdier, beholder man også det strategiske overblikket uten å gå i for mange detaljer med en gang. *Ved utformingen av en definisjon, blir derfor utfordringen å velge ut samfunnets grunnleggende verdier, og få en diskusjon knyttet til dette, ikke om en infrastruktur er kritisk eller ikke ut fra et sett med kriterier*. Som tidligere nevnt er en definisjon ikke tilstrekkelig til å identifisere kritisk infrastruktur. Til det trengs det en egen metode.

Forsøksvis vil en definisjon av kritisk infrastruktur som tar utgangspunkt i samfunnets grunnleggende verdier se slik ut:

Kritisk infrastruktur er de objekter, systemer, tjenester og ressurser som sikrer samfunnets grunnleggende verdier. De er fred og nasjonal selvstendighet, en demokratisk rettsstat,en god samfunnsøkonomi, velferd til befolkningen, liv og helse, livsmiljøet og en nasjonal trygghetsfølelse.

Legg merke til at ressurser er lagt til utvalgets arbeidsdefinisjon sammen med objekter, systemer og tjenester. Det ut fra en forståelse om at en ressurs, som for eksempel råolje og vann, er deler av den kritiske infrastrukturen.

Definisjonen er da bygget opp på følgende måte:

1. Kritisk infrastruktur er de objekter, systemer, tjenester og ressurser
2. som understøtter samfunnets grunnleggende verdier
3. Samfunnets grunnleggende verdier er fred og nasjonal selvstendighet, en demokratisk rettsstat,en god samfunnsøkonomi, velferd til befolkningen, liv og helse, livsmiljøet og nasjonal trygghetsfølelse

7 Konklusjon

Hensikten med teksten er ikke å presentere en autorativ definisjon, men å snu diskusjonen til å omhandle hva samfunnets grunnleggende verdier er, hvilke funksjoner som understøtter disse og hvilken infrastruktur som ligger i bunn for å realisere verdiene og funksjonene. ISUs arbeidsdefinisjon slik den fremstår nå kan hevdes å forsøke å

gape over for mye: Ved å liste opp ett sett med kriterier/funksjoner/verdier i definisjonen, gir den inntrykk av å gi svar på noe som kun en større metode kan gi svar på. Ved å fokusere på samfunnets grunnleggende verdier gir en definisjon et bedre utgangspunkt for å definere kritisk infrastruktur på et strategisk nivå, uten å gi inntrykk av å være et verktøy for å identifisere kritisk infrastruktur. En definisjon på noen få setninger gir en pekepinn. Den leder tankene på rett vei og gir en intuitiv forståelse av hva kritisk infrastruktur er når det arbeides med saksfeltet på et strategisk nivå

Vedlegg 3

Sårbarhet i kritisk infrastruktur – utfordringer

Innledende utredning om kritisk infrastruktur til Utvalg for sikring av landets kritiske infrastruktur

Kjetil Sørli, Direktoratet for samfunnssikkerhet og beredskap,
Enhet for analyse og utredning

17. januar 2005
(Revidert febr. 2005 og med oppdatert tabell per februar 2006)

1 Sårbarhet i kritisk infrastruktur - utfordringer

1.1 Innledning

Kritisk infrastruktur er fundamentet for samfunnets evne til å fungere både i normale situasjoner og i situasjoner der samfunnet utsettes for ekstraordinære påkjenninger. Ved svikt i kritisk infrastruktur er samfunnet ikke i stand til opprettholde den leveranse av varer og tjenester som befolkningen er avhengige av.[1] Det finnes flere definisjoner av begrepet, men i kjernen ligger noen svært viktige samfunnsfunksjoner, også omtalt som bærebjelkene i samfunnet.[2] Bærebjelkene kan deles opp i følgende:

- Energi- og kraftforsyning
- Informasjons og kommunikasjonsteknologi (IKT)
- Ledelse og informasjon
- Tilgang til rent vann og ernæring
- Helsetjenester
- Transport

Felles er at det ved alvorlig svikt i en eller flere av disse raskt vil oppleves massive forstyrrelser i samfunnet.[3] De har dermed et stort sårbarhetspotensiale. Felles er også at de i større eller mindre grad er gjensidig avhengige av hverandre og har en sektorovergripende karakter. Kritisk infrastruktur er imidlertid mer enn bare bærebjelkene. Kritisk infrastruktur finnes også innen områder hvor lengre tids avbrudd vil få store konsekvenser for samfunnet.

Norge var tidlig ute med forskning på sårbarheter i kritisk infrastruktur.[4] Forskningen har bidratt med å legge grunnlaget for sårbarhetsregulerende tiltak fra myndighetene. Det gjelder både i forhold til organisering, lovgivning og styrking av beredskapsressurser. Store deler av tidligere forskning er fremdeles relevant. Utredningen har derfor ett overordnet blikk på forskningsstatus så langt. Samtidig er samfunnet i kontinuerlig endring med hensyn til teknologi, organisasjon, politikk og trusler. Det vises derfor til temaer og fremtidsutfordringer som det hevdes det er viktig å få mer kunnskap om. Ut over dette har utredningen en kort oversikt over ansvar, oppgaver og arbeidsfordeling på myndighetssiden. Det vil ikke bli gitt en bred omtale av sårbarheter i samfunnskritisk infrastruktur i dag eller sårbarhetsreduserende tiltak myn-

[1] Av andre definisjoner kan følgende nevnes. Canada: Critical infrastructure consists of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada (www.ocipep.gc.ca). USA: Critical infrastructure are systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (The USA Patriot Act of 2001 (P.L. 107-56)). Danmark: [Kritisk infrastruktur] kan forstås som de elementer i et overordnet system (samfund), der er så vitale, at forstyrrelse og nedbrud af bare en enkelt af dem ville kunne true selve systemets funktionsduelighed. (National Sårbarhedsudredning, Udvalget for National Sårbarhedsudredning. Beredskabsstyrelsen 2004.) Sverige: Med samhällsviktig infrastruktur avses grundläggande system i samhället som är väsentliga för att samhället skall fungera och som direkt eller indirekt används av flertalet invånare. (KBM, planeringsprocessen 2003:7. Samhällets krisberedskap 2005 - Planeringsinriktning. Krisberedskapsmyndigheten.)

[2] Hæsken, Ole Morten et al. 1997: Beskyttelse av samfunnet (BAS) – sluttrapport, FFI/RAPPORT -97/01459, Forsvarets forskningsinstitutt.

[3] Hæsken, Ole Morten et al. 1997: Beskyttelse av samfunnet (BAS) – sluttrapport, FFI/RAPPORT -97/01459, Forsvarets forskningsinstitutt.

[4] Forskningsserien BAS – Beskyttelse Av Samfunnet – startet i 1994.

dighetenes har iverksatt de siste årene. DSBs anliggende i denne sammenheng er å gjøre opp en status på hva som er kjent om sårbarheter i samfunnskritisk infrastruktur og hvor veien burde gå videre.

1.2 Identifisering og prioritering av kritisk infrastruktur

Det er ikke etablert et helhetlig sett med kriterier for identifisering og prioritering av kritisk infrastruktur. En vanlig, men noe utilstrekkelig tilnærming, er å gå gjennom tidligere lister over kritisk infrastruktur og justere dem opp mot det aktuelle behovet der og da.[5] Dette vanskeliggjør en helhetlig prioritering mellom det viktige og uviktige. Statiske lister fanger heller ikke opp endringer i samfunnet.

Det er to overordnede elementer i en helhetlig tilnærming for utvelgelse og prioritering av kritisk infrastruktur. For det første må de kritiske sektorene identifiseres og prioriteres på et overordnet nivå ut fra et sett med utvalgskriterier. For det andre må sektorene operasjonaliseres ned til håndterbare størrelser, også her med hjelp av utvalgskriterier. Det er først på et detaljert nivå kompleksiteten og de gjensidige avhengighetene trer frem. Det blir gitt et eksempel på en slik prosess senere i utredningen i omtalen av den såkalte Østfoldundersøkelsen, hvor Østfold Energi brukte et halvt år på å kartlegge konsekvensene av kraftrasjonering i distribusjonsnettet i Østfold fylke.

Utvalgsprosessen er dessuten sektoravhengig. Eksempelvis er utfordringene annerledes for helsesektoren enn den er for transportsektoren. Utvalgsprosessen er også situasjonsbestemt. Kraftrasjonering på grunn av overforbruk i en streng kuldeperiode er annerledes enn kraftrasjonering etter bortfall av store produksjonsenheter om sommeren. Likeledes er det ved kraftrasjonering mer hensiktsmessig å prioritere strøm til et vannverk uten nødstrøm enn til et sykehus med tilstrekkelig nødstrøm. I en slik situasjon er rent vann mer kritisk for sykehuset enn ekstern kraftforsyning. Likevel ligger det sektorovergripende konstanter der, uavhengig av sektor og situasjon. Dette gjelder særlig i forhold til bærebjelkene i samfunnet. Utvalgsprosessen innebærer også å være i kontakt på et svært detaljert nivå med de virksomheter det berører samt andre eksperter på fagområdet.

For å identifisere sårbarheter i kritisk infrastruktur er Charles Perrows teori om systemulykker en fruktbar tilnærming.[6] En av hans hovedteorier er at mestring av tett koblede systemer krever sentralisert styring. Et tett koblet system vil ikke fungere uten sentralisert styring og forstyrrelser vil hurtig berøre resten av systemet. Ut fra et slikt perspektiv vil de tett koblede systemene være mer sårbare fordi helheten er avhengig av at «hjernen» fungerer. Perrows teori fungerer dermed som et verktøy for å identifisere infrastruktur hvor toleransen for avbrudd er svært små. For eksempel er strømforsyning langt mer sårbar enn drift av renovasjon. Begge har en kritisk funksjon i samfunnet, men mens strømforsyning er avhengig av noen få kontrollsentraler for å fungere, er det mulig å drifte renovasjon desentralisert. På samme måte er jernbane og lufttrafikk i Norge avhengig av styring fra driftsentraler i sanntid, mens busstrafikk kan operere uten en sentralisert styring, eller i hvert fall med langt lavere krav til sentralisert kontroll og styring i sanntid. Identifisering og kartlegging kan omtales som en første grunnleggende fase. Ut over dette vil det være nødvendig å vurdere hvilket skadepotensiale og hvilke risikoer sårbarhetene utgjør, gjøre prioriteringer og å fange opp eventuelle endringer som kan inntreffe over tid. Det mangler per i dag en god metode for å dekke alle aspektene av dette, særlig i forhold til å identifisere og prioritere.

1.3 Ansvar, oppgaver og arbeidsfordeling på myndighetssiden

Samfunnssikkerhets- og beredskapsarbeidet overfor kritisk infrastruktur er organisert ved at det departementet som har ansvar for en sektor til daglig også har ansvaret ved en krisesituasjon. Beredskapsorganiseringen følger dermed ansvarsprin-

[5] Eksempler på lister se, NOU 2000:24, Et sårbart samfunn, http://odin.dep.no/jd/norsk/dok/andre_dok/utredninger/012001-020005/dok-bn.html;
Canada: Public Safety and Emergency Preparedness Canada, http://www.ocipep.gc.ca/info_pro/fact_sheets/general/CIP_NCIAP_e.asp;
USA: National Strategy for the Physical Protection of Critical Infrastructures and Key Assets 2003, http://www.whitehouse.gov/pcipb/physical.html
USA: Critical Infrastructure and Key Assets: Definition and Identification, 2004, CRS Report for Congress, http://www.fas.org/sgp/crs/RL32631.pdf
Beredskapsstyrelsens Nationale sårbarhedsudredning 2004, http://www.beredskabsstyrelsen.dk/info/rapport/

[6] Perrow, Charles. 1999. Normal Accidents. Living with High Risk Technologies, Princeton University Press.

sippet i tillegg til prinsippene om nærhet og likhet.[7] Ut over dette har Justis- og politidepartementet et samordnings- og tilsynsansvar og en særlig initiativplikt ved kriser. Det innebærer et ansvar for å utarbeide overordnede retningslinjer, koordinere og fremme proposisjoner og meldinger til Stortinget, tilrettelegge rammebetingelser, ta initiativ, være pådriver, avklare ansvarsforhold i gråsoner og treffe prinsipielle avgjørelser på samfunnssikkerhets- og beredskapsområdet. Statsministerens kontor kan dessuten ta initiativ til å fastsette en særskilt organisering av krisehåndteringen. Hvis normale beslutningssystemer ikke fungerer på grunn av ekstraordinære sikkerhetspolitiske omstendigheter, er det utarbeidet egne krisehåndteringssystemer.

Sektorvis ansvar for beredskap og/eller forebygging innen samfunnskritiske sektorer og områder kan fremstilles på følgende måte i tabellform[8]

[7] Ansvarsprinsippet betyr at den som har et ansvar i en normal situasjon også har ansvar i tilfelle ekstraordinære hendelser. Likhetsprinsippet betyr at daglig organisasjon skal være mest mulig lik organisasjon under kriser. Nærhetsprinsippet betyr at kriser skal håndteres på lavest mulig nivå. St.meld. nr. 39 (2003–2004), Samfunnssikkerhet og sivilt-militært samarbeid.

[8] Tabellen er revidert per februar 2006.

Tabell 3.1 Myndighetenes ansvar for beredskap og/eller forebygging i kritisk infrastruktur og kritiske samfunnsfunksjoner

Kritisk infrastruktur	Departement	Underliggende etat
Elektrisk kraft	Olje- og energidepartementet	Norges vassdrags- og energidirektorat
	Justis- og politidepartementet	Direktoratet for samfunnssikkerhet og beredskap
Elektronisk kommunikasjon	Sektordepartementene	
	Samferdselsdepartementet	Post- og teletilsynet
	Forsvarsdepartementet	Nasjonal sikkerhetsmyndighet
	Justis- og politidepartementet	
	Fornyings- og administrasjonsdepartementet	
Transport	Samferdselsdepartementet	Luftfartstilsynet
		Jernbanetilsynet
		Vegdirektoratet
	Nærings- og handelsdepartementet	Sjøfartsdirektoratet
	Fiskeri- og kystdepartementet	Kystdirektoratet/Kystverket
	Justis- og politidepartementet	Direktoratet for samfunnssikkerhet og beredskap (transport av farlig gods)
Olje og gass	Olje- og energidepartementet	Oljedirektoratet
	Arbeids- og inkluderingsdepartementet	Petroleumstilsynet
Vann og avløp	Helse- og omsorgsdepartementet	Mattilsynet
		Sosial- og helsedirektoratet
		Helsetilsynet
		Nasjonalt folkehelseinstitutt
		Kommunene
	Miljøverndepartementet	Statens forurensningstilsyn
		Fylkesmennene
		Kommunene
	Olje- og energidepartementet	Norges vassdrags- og energidirektorat
	Justis- og politidepartementet	Direktoratet for samfunnssikkerhet og beredskap
Satellittbasert infrastruktur	Nærings- og handelsdepartementet	Norsk romsenter

Tabell 3.1 Myndighetenes ansvar for beredskap og/eller forebygging i kritisk infrastruktur og kritiske samfunnsfunksjoner

Kritiske samfunns-funksjoner	Departement	Underliggende etat
Bank og finans	Finansdepartementet	Kredittilsynet Norges Bank
Matforsyning	Landbruks- og matdepartementet	Mattilsynet Statens landbruksforvaltning
	Nærings- og handelsdepartementet	
	Fiskeri- og kystdepartementet	Mattilsynet
	Helse- og omsorgsdepartementet	Mattilsynet Sosial- og helsedirektoratet Helsetilsynet Nasjonal folkehelseinstitutt
Helse, sosial og trygde-tjenester	Helse- og omsorgsdepartementet	Helsetilsynet Sosial- og helsedirektoratet Nasjonalt folkehelseinstitutt
	Arbeids- og inkluderingsdepartementet	Sosial- og helsedirektoratet Rikstrygdeverket Arbeids- og velferdsetaten (NAV) sommeren 2006
Politi	Justis- og politidepartementet	Politidirektoratet
Nød- og redningstjeneste	Justis- og politidepartementet	Politidirektoratet Direktoratet for samfunnssikkerhet og beredskap Hovedredningssentralene Næringslivets sikkerhetsorganisasjon (Industrivern)
	Helse- og omsorgsdepartementet	Sosial- og helsedirektoratet Helsetilsynet Kommunene (Brann- og redningsvesen)
Nasjonal kriseledelse	Sektordepartementene	
	Justis- og politidepartementet	Politidirektoratet Direktoratet for samfunnssikkerhet og beredskap Hovedredningssentralene
	Kultur- og kirkedepartementet	NRK
Storting og Regjering	Sektordepartementene Statsministerens kontor	
	Fornyings- og administrasjons-departementet	Departementenes servicesenter (sentraladministrasjonen) Stortingets administrasjon Riksrevisjonen
Domstolene	Justis- og politidepartementet	Domstoladministrasjonen (Tingretten) (Lagmannsretten) (Høyesterett)[1]
Forsvar	Forsvarsdepartementet	Forsvarets militære organisasjon Forsvarsbygg Nasjonal sikkerhetsmyndighet
Miljøovervåkning	Miljøverndepartementet	
Renovasjon		Kommunene

[1] Domstolene er ikke underlagt Justis- og politidepartementet, men er tatt med på listen for oversiktens skyld.

Det fragmenterte ansvaret tilsier et sterkt fokus på Statsministeres kontor og Justis- og politidepartementets samordnende rolle, og at det i forbindelse med omorganiseringen av departementer og underliggende etater den senere tid bør gjennomføres en tverrsektoriell analyse for å avdekke uavklarte beredskapsmessige roller. Dette må også relateres til utfordringer på beredskapssiden knyttet til deregulering og privatisering av virksomheter som spiller en rolle for samfunnets sikkerhet. Innenfor en slik analyse vil Politiet, Forsvaret, redningstjenesten og det regionale og kommunale apparatet også inngå. I denne sammenheng fremstår det som en særlig utfordring å oppdatere lovstrukturen i forhold til å ha en sektorovergripende tilnærming innenfor samfunnssikkerhet, beredskap og forsvar.

Transportsektoren har de senere år gjennomført tiltak for å beskytte kritisk infrastruktur. Luftsikkerheten ble styrket etter innføringen av ny forskrift i mai 2004.[9] Forskriften krever bedre sikring av fly og økt kontroll av blant annet passasjerer, bagasje, flybesetninger, lufthavnansatte, frakt og post. Sikkerhetskontrollen omfatter både innenlands og utenlands rute- og chartertrafikk. For norske lufthavner gjelder dermed de samme sikkerhetskravene som for lufthavnene i EU. Skip og havner fikk styrket sikkerhet med innføring av EUs og FNs regler for havnesikkerhet.[10] De inneholder en rekke myndighetskrav og krav til konkrete sikkerhetstiltak som skal iverksettes om bord på skip i internasjonal fart og i havneanlegg som betjener slike skip. Målet er å forhindre terroranslag mot internasjonal skipsfart.

Flere tiltak i andre sektorer er under utarbeidelse. Eksempelvis i telesektoren arbeider Post- og teletilsynet med skjerpede sikkerhetskrav til leverandørene. I dag er det slik at Ekomlovens bestemmelser om krav til sikkerhet i utgangspunktet omfatter alle leverandører av telefoni- og kommunikasjonstjenester.[11] Til og med 2005 er det i tillegg inngått særlige avtaler med Telenor om spesielle sikkerhetstiltak. Fra og med 2006 vil alle leverandører med IKT infrastruktur av betydning og andre leverandører med leveranser til brukere med samfunnskritisk funksjon bli omfattet av slike avtaler. Sikkerhetskravene omfatter blant annet tiltak innen fysisk og logisk sikring av kommunikasjonssystemer, krav om beredskapsplanlegging og prioritering av ressurser. Videre gjennomføres det kriseøvelser i regi av Post- og teletilsynet, der hensikten er å koordinere ressursutnyttelse på tvers av leverandørgrensene i en krisesituasjon.[12] Krav om nasjonal autonomi på produksjon og leveranse av teletjenester er under utredning. Prioritetsordning som muliggjør at særlig viktige brukere kan få prioritet på mobiltelefontjenester i en krisesituasjon er under utredning med assistanse fra Telenor Mobil, NetCom og Direktoratet for samfunnssikkerhet og beredskap.

I Forsvarsdepartementet utarbeides det nye retningslinjer for objektsikkerhet. Sikkerhetslovens bestemmelser om objektsikkerhet ble sammen med det øvrige regelverket for informasjonssikkerhet og personellsikkerhet iverksatt 1. juli 2001. Bestemmelsene om objektsikkerhet i loven er for kortfattede til å fungere som veileder for offentligheten. Forsvarsdepartementet som regelverksforvalter for sikkerhetsloven arbeider nå med å endre loven på dette punkt slik at det skal bli mulig å få til en tverrsektoriell utvelgelse, klassifisering og defensiv beskyttelse av objekter som er skjermingsverdige av hensyn til rikets sikkerhet og selvstendighet og andre vitale nasjonale sikkerhetsinteresser. Loven definerer objekt som eiendom. Dette kan være materiell, bygninger, gjenstander, transportmidler med mer som kan være direkte mål for eller midler til å gjennomføre sabotasje eller terrorhandlinger.

1.4 Forskning og utredning

Det vil i løpet av 2005 pågå flere større forskningsprosjekter og utredninger på området kritisk infrastruktur. Ved Forsvarets forskningsinstitutt (FFI) startet BAS5 om sårbarhet i samfunnskritiske IKT-systemer opp høsten 2004. I oktober 2004 ble det etablert et utvalg for sikring av landets kritiske infrastruktur med fokus på omstilling og deregulering i virksomheter med kritisk infrastruktur. Ved Norges teknisk-naturvitenskapelige universitet (NTNU) og Stiftelsen for Industriell og Teknisk Forskning ved Norges tekniske høgskole (SINTEF) og ved Universitetet i Stavanger (UiS) og Senter for Risikostyring og Samfunnssikkerhet (SEROS) er det flere pågående prosjekter som er relevante. Det vil i det følgende bli fokusert på dette arbeidet.

1.4.1 BAS – Beskyttelse av samfunnet

Det mest omfattende og helhetlige arbeidet som er gjort i Norge om sårbarhet i kritisk infrastruktur

[9] Forskrift om forebyggelse av anslag mot sikkerheten i luftfarten.

[10] The international convention for the Safety Of Life At Sea (SOLAS-konvensjonen) og International Ship and Port Facility Security Code (ISPS-koden)

[11] Lov om elektronisk kommunikasjon.

[12] Første øvelse var i 2003.

og samfunnskritiske funksjoner er i de såkalte BAS-forskningsprosjektene ved Forsvarets forskningsinstitutt (FFI). Forskningen har på flere områder vært en premissleverandør for myndighetene.

BAS-prosjektene startet i 1994 som et samarbeid mellom FFI, Justis- og politidepartementet, det daværende Direktoratet for sivilt beredskap og relevante fagdepartementer. Bakgrunnen var erkjennelsen om endringer i de sikkerhetspolitiske utfordringene for samfunnet, og hadde som utgangspunkt at den sivile beredskapssektor hadde behov for et mer helhetlig grunnlag for ressursallokering og et bedre system for langsiktige planlegging.[13] Prosjektseriens langsiktige mål var og er å bidra til et gjennomarbeidet konsept for beskyttelse av samfunnet, samt støtte opp under en løpende prioritering av sårbarhetsreduserende tiltak. I studiene har det inngått sårbarhetsanalyser av ulike sektorer, studier av tilsiktede og utilsiktede trusler mot samfunnet og kosteffektivitetsanalyser av sårbarhetsregulerende og skadebøtende tiltak. BAS har så langt omfattet følgende prosjekter:

- 1994-1997 Samfunnets sårbarhet og organiseringen av beredskap (BAS1)
- 1997-1999 Sårbarhet i offentlig telekommunikasjon (BAS2)
- 1999-2001 Sårbarhet i kraftforsyningen (BAS3)
- 2001-2003 Sårbarhet i transportsektoren (BAS4)
- 2003 Sårbarhet i vannforsyningen (SIV)
- 2004-2006 Sårbarhet i samfunnskritiske IKT-systemer (BAS5)

En rekke problemstillinger har vært formative for prosjektene: Hvor sårbart er samfunnet og de ulike sektorene, hvilke trusler står samfunnet overfor, er beredskapen tilpasset trusselbildet og utfordringene, hvilke tiltak bidrar til å redusere sårbarheten, hva koster beredskap og beskyttelsestiltak og hvordan få mest mulig beredskap ut av hver krone?

1.4.1.1 Samfunnets sårbarhet og organiseringen av beredskap (BAS1)

I BAS1 på midten av 1990-tallet ble det klart at det moderne samfunnet generelt er sårbart, men at det er store forskjeller mellom ulike samfunnsfunksjoner. Det ble også funnet en stor grad av gjensidige avhengigheter mellom ulike samfunnsfunksjoner og at sårbarheten tenderte til å øke innen kritisk infrastruktur som følge av sentralisering og spesialisering. En gjennomgående trend ble også funnet å være IKT-avhengigheten på alle områder. Inn i dette bildet faller også at personellreduksjoner og effektivisering gir mindre rom for å møte uforutsette hendelser. Overgripende for alle funnene er at internasjonalisering og globalisering gjør det stadig vanskeligere å se på sårbarhet i et isolert nasjonalt perspektiv. Som en konklusjon ble det konstatert at alvorlig svikt vil få store konsekvenser, og at beredskapstiltak bar preg av å være lite tilpasset en endret virkelighet.

1.4.1.2 Sårbarhet i offentlig telekommunikasjon (BAS2)

Som en oppfølgning av BAS1 gjennomførte FFI en undersøkelse med fokus på sårbarhet i telenettet i BAS2 fra 1997 til 1999.[14] FFI fant som hovedtrender at markedshensyn i økende grad var styrende for sektoren og da særlig i forhold som sentralisering og samlokalisering, teknologisk utvikling og kompleksitet, og internasjonalisering og globalisering. FFI fant blant annet at telekommunikasjon legger til rette for å drifte virksomheter utenfor landets grenser. Det ble også observert at det offentlige telenettet var sårbart og hadde liten redundans. Videre ble det funnet at avhengigheten av kommunikasjon er stor og at konsekvensene ved bortfall er store, særlig ved kriser der det er viktig å handle raskt for å redde liv, helse og verdier. På grunnlag av funnene ble det i 1999 anbefalt en økt sikring av telenettet ved å vektlegge beredskapsplanlegging, forsterke informasjonssikkerheten, ha samøvelser, bedre reparasjonsberedskapen samt å innføre redundansrettede tiltak ved å konkret utbedre de verste fysiske sårbarhetene. Resultatene fra BAS2 var med å danne grunnlag for myndighetenes videre arbeid med å minske sårbarheter i telenettet, blant annet vet å gi innspill til Sårbarhetsutvalget og Samferdselsdepartementets revisjon av teleberedskapen..

1.4.1.3 Sårbarhet i kraftforsyningen (BAS3)

I 1999 startet BAS3 med fokus på sårbarhet i kraftforsyningen.[15] Særlig to funn var interessante i et

[13] Hæsken, Ole Morten et al. 1997: Beskyttelse av samfunnet (BAS) – sluttrapport, FFI/RAPPORT -97/01459, Forsvarets forskningsinstitutt.

[14] Hagen, Janne M. et al. 1999: Sårbarhetsreduserende tiltak innen offentlig telekommunikasjon - Sluttrapport, FFI/RAPPORT-99/00242, Forsvarets forskningsinstitutt (Begrenset). Hagen, Janne M, Nystuen, Kjell Olav. 1999: Beskyttelse av samfunnet med vekt på offentlig telekommunikasjon, FFI-RAPPORT-99/00240. Forsvarets forskningsinstitutt.

samfunnsperspektiv. For det første at sårbarheten i kraftforsyningen øker, og for det andre at befolkningens avhengighet av strøm øker. Prosjektet kom frem til at den fysiske infrastrukturen er relativt godt dimensjonert, men at et ensidig fokus på kosteffektiv drift fører til at sårbarheten øker. Forbruket har tatt igjen produksjonskapasiteten, og kraftsystemet kjøres på grensen av kapasiteten med en delvis foreldet infrastruktur. Det ble pekt på at enkle feil kan gi store konsekvenser. Senere ble dette bekreftet i 2003 ved strømutfallene i Nord-Amerika, England, Danmark og Sverige og Italia.[16] Prosjektet fant videre at reparasjonsberedskapen var svak, og at det var for lite fokus på de store utfordringene blant annet ved at kravene til beskyttelse var gammelmodige. Stigende sårbarhet ble også observert i kraftindustriens økende avhengigheten av IKT-systemer. Norsk kraftforsyning styres fra et fåtall driftssentraler med fjernstyring via avanserte IT-systemer, og sammenkopling av ulike datasystemer blant annet mot internett ble funnet å representere en sikkerhetsrisiko.

Konsekvensene av langvarige strømbrudd ble funnet å være at kritiske samfunnsfunksjoner stopper opp og at store deler av befolkningen meget raskt vil få behov for hjelp. Særlig kritisk er det at kraftbortfall i kuldeperioder vil medføre rask nedkjøling av en boligmasse som i stor grad er avhengig av elektrisk strøm for varme. Også krisehåndteringsevnen vil lide i en slik situasjon. På tiltakssiden anbefalte FFI en minimumspakke med bedre IT-sikring, en økt reetableringsevne og bedre sikring av viktige objekter. Det ble også anbefalt at marginene i systemet må økes, for eksempel med nybygging, sikring av importert kraft og fortsatte sparetiltak på forbruket.

1.4.1.4 Sårbarhet i transportsektoren (BAS4)

BAS4-prosjektet ble etablert i 2001 med fokus på sårbarhet innen transportsektoren.[17] FFI fant en rekke samfunnsmessige endringer som påvirket transportsektoren, blant annet i forhold til at transporttjenester har gått fra å være et knapphetsgode til at vi i dag har et overskudd. Sektoren har også i stor grad gått fra å være nasjonal til internasjonal, med en økende markedsdominans blant de store selskapene. I perioden som prosjektet løp ble også terrortrusselen aktualisert, og det ble iverksatt studier som så transportsektoren opp mot den nye trusselen. Statistikk om tidligere terrorhendelser fra hele verden ble sammenstilt, og resultatene viste at det innen transportsektoren var transport på veg som var mest utsatt, men at Norge og Skandinavia har vært lite utsatt i forhold til andre deler av verden. Samtidig ble det vist til at dette kan endre seg, og da særlig i forhold til Norges engasjement i andre konflikter, i forhold til spredning av kompetanse på IKT-siden og i forhold til en større villighet blant terrorister til å bruke masseødeleggelsesvåpen. Den generelle sårbarheten ble funnet å være lav på grunn av mangfold og redundans i de forskjellige transportformene. Likevel ble det gjort oppmerksom på at sektoren er sårbar overfor terrorhandlinger fordi den er tilgjengelig, synlig og attraktiv som mål.

1.4.1.5 Sårbarhet i vannforsyningen (SIV)

I 2003 kom resultatene av en mindre studie om sårbarhet i vannforsyningen.[18] Hovedmålet var å avdekke potensielle trusler og svakheter, og foreslå tiltak for å redusere sårbarheten. Rapporten viste at norsk vannforsyning inneholder et mangfold og en variasjon som gjør det mindre relevant å gi noen generelle anbefalinger til prioritering av enkelttiltak. Det er samspillet mellom de ulike tiltakene, så som tekniske, operasjonelle, vedlikeholdsmessige, kunnskapsmessige og øvelsesmessige som avgjør den helhetlige sikkerheten i vannforsyningen. Hvert vannverk må ses på som unikt og risikoen vurderes lokalt. Også sårbarhet opp mot terrorisme, beredskapsløsninger, ekstremt vær, konkurranseutsetting og privatisering ble vurdert. Av interessante funn i denne sammenhengen er at det ble funnet å være lett tilgang til mange anlegg. I studien blir det fremhevet at faren for alvorlige terroranslag mot vannforsyningen i Norge vurderes som meget liten, men at andre typer fysiske sabotasjeaksjoner er mer sannsynlige. Ekstremt vær vil trolig inntreffe stadig hyppigere. De fleste vannverk kan kjøres manuelt i en periode med bortfall av IKT-system, men større

[15] Fridheim, Håvard et al. 2001: Sårbarhetsreduserende tiltak innen kraftforsyningen - Gradert sluttrapport etter BAS3, FFI/RAPPORT-2001/02383, Forsvarets forskningsinstitutt (Begrenset). Fridheim, Håvard et al. 2001: En sårbar kraftforsyning - Sluttrapport etter BAS3, FFI/RAPPORT-2001/02381, Forsvarets forskningsinstitutt.

[16] I Norge ble store deler av Hordaland og nordre deler av Rogaland mørklagt som resultat av feil i en linjeskjøt på ledningen fra Sauda til Nesflaten 13. februar 2004. Strømbruddet varte kun 40 minutter, men rammet om lag 200 000 personer.

[17] Hagen, Janne et al. 2003: Beskyttelse av samfunnet med fokus på transportsektoren, FFI/RAPPORT-2003/00929. Forsvarets forskningsinstitutt.

[18] Bartnes, Jørgen et al. 2003: Sårbarhet i vannforsyningen, Rapport nr. 27.730.081/R1. Scandpower Risk Management AS. Rapporten ble utarbeidet i samarbeid mellom Aquateam AS, Forsvarets forskningsinstitutt, Hjellnes Cowi AS og Scandpower Risk Management AS.

vannverk blir mer og mer avhengige av IKT-systemer når det gjelder prosesstyring, overvåking m.v. Det ble også funnet mangel på redundans, utfordringer knyttet til kompetanse og rekruttering, og at fremtidig konkurranseutsetting og privatisering kan gjøre at beredskap ikke blir prioritert. Regelverket knyttet til vannforsyning er oppfattet som noe overlappende, og det etterlyses en klarere organisering av beredskap på nasjonalt og regionalt nivå. SIV-studien avdekket også at kun halvparten av landets vannverk hadde utarbeidet en beredskapsplan og at bare 10 % hadde gjennomført øvelser de siste tre årene. Videre ble det avdekket begrensninger med hensyn til analysekapasitet og muligheter i forhold til spesialiserte analysetjenester for å identifisere agens i vann. Som en videreføring av SIV er det bl.a. igangsatt et prosjekt som tar sikte på å utarbeide et bransjespesifikt veiledningsmateriell for vannforsyning. Hensikten er gi vannverkene og deres rådgivere et bedre hjelpemiddel i arbeidet med vurdering av sårbarhet, utarbeidelse av beredskapsplaner, avklaringer av forholdet til samfunnet omkring (herunder overordnet operativ beredskap), gjennomføring av beredskapsøvelser m.v.

1.4.1.6 Sårbarhet i samfunnskritiske IKT-systemer (BAS5)

Høsten 2004 startet det så langt siste prosjektet i BAS-serien, BAS5. Prosjektet kom etter at Direktoratet for samfunnssikkerhet og beredskap (DSB) og Nasjonal sikkerhetsmyndighet (NSM) ble gitt i oppdrag av Justis- og politidepartementet (JD) å initiere et forskningsprosjekt for å undersøke hvordan sårbarhet i IKT-systemer kan påvirke viktige nasjonale samfunnsinteresser og -funksjoner. Forsvarets forskningsinstitutt utfører prosjektet som vil vare i om lag 2 år. I tillegg ble det innledet et samarbeid med Universitetet i Stavanger, Høgskolen på Gjøvik og Norges teknisk-naturvitenskapelige universitet i Trondheim om prosjektgjennomføringen.

Bakgrunnen for prosjektet er at nesten all oppmerksomhet på IKT-sikkerhet er rettet mot dagligdagse hendelser. Eksempler på dette er virusangrep og lokal driftsstand. Det er derfor naturlig for myndighetene å stille spørsmål om konsekvensene ved ekstraordinære hendelser. Dette er særlig viktig sett på bakgrunn av at vi er vitne til en akselererende bruk av IKT i samfunnskritiske systemer. Sårbarhetspotensialet kan derfor sies å hatt en dramatisk økning de siste årene. Også på trusselsiden er det skjedd endringer ved at det i dag bygges opp kompetanse og kunnskap for på sikt kunne ramme en nasjon gjennom dataangrep. Vi ser at slagmarken er i ferd med å utvides til også å omfatte samfunnskritiske IKT-systemer. Målsetningen er å komme med konkrete forslag til tiltak for å redusere sårbarhet, og videre at forslagene skal kunne danne grunnlag for myndighetenes videre arbeid med å skape et robust samfunn. Målsettingen er videre å utvikle og anvende en risiko- og sårbarhetsmetode på samfunnsviktige IKT-systemer, utvikle og anvende en metodikk for å rangere tiltak som reduserer sårbarheten og utvikle og anvende en metode for å rangere kritiske IKT-systemer og samfunnsfunksjoner.

BAS5 er organisert som et spleiselag. Norges forskningsråd er en tung bidragsyter ved siden av DSB. I tillegg bidrar departementer og underlagte etater med i prosjektet med arbeidsinnsats og finansiering. Også FFI har gått inn med midler i prosjektet. Oppdragsmiljøet omfatter så langt:

- Direktoratet for samfunnssikkerhet og beredskap
- Nasjonal sikkerhetsmyndighet
- Justis- og politidepartementet
- Forsvarets sikkerhetsavdeling
- Oljedirektoratet
- Norges vassdrags- og energidirektorat
- Moderniseringsdepartementet
- Post- og teletilsynet
- Samferdselsdepartementet
- Sosial- og helsedirektoratet
- Kredittilsynet
- Norges forskningsråd
- Statnett

1.4.2 NTNU og SINTEF

NTNU har en teknologisk og naturvitenskapelig hovedprofil. Samtidig har universitetet et bredt fagtilbud i medisin, samfunnsvitenskap, humaniora og kunstfag. NTNU vektlegger tverrfaglighet i forskning og undervisning. Stiftelsen SINTEF består av åtte forskningsinstitutter, og i SINTEF-gruppen inngår også fire forskningsaksjeselskaper.[19] SINTEFs visjon er teknologi for et bedre samfunn. SINTEF samarbeider nært med NTNU og Universitetet i Oslo (UiO). Personell fra NTNU arbeider på SINTEF-prosjekter, mens SINTEF-ansatte underviser ved NTNU. Fellesskapet innebærer en utstrakt, felles bruk av laboratorier og utstyr.

Ved NTNU og SINTEF foregår det mye forskning som direkte omhandler eller grenser opp mot sårbarheter i kritisk infrastruktur. Det gjelder

[19] SINTEF-gruppen er Skandinavias største uavhengige forskingsorganisasjon, med ca. 1800 ansatte og en samlet omsetning på om lag. 1,7 mrd kr. (2003).

innenfor områder som transport, kraftforsyning, vannforsyning og IKT. I det følgende vil de mest aktuelle studiene bli presentert.

1.4.2.1 Sårbarhet i transport

Innenfor landbasert transport på veg og bane spenner aktiviteten blant annet over følgende tema:

- Ulykkesdata og risiko i vegnett, erfaringstall for ulykkesrisiko, effekter av tiltak, metodikk for å evaluere nye tiltak, sårbarhetsanalyser for vegnettet, risiko og krisehåndtering i veg- og jernbanetunneler
- Trafikksikkerhet som funksjon av drift og vedlikehold av vegnettet, herunder vinterdrift, dekketilstand og fartsgrenser
- Sikringssystemer for jernbane, herunder vurdering av sikkerhet og interoperabilitet
- Holdninger, kjøreatferd og sikkerhetskultur, herunder trafikantenes fysiske forutsetninger samt holdninger og atferd hos spesielle trafikkantgrupper
- Lovgivning, kontroll og sanksjoner, herunder evaluering av aksjoner og tiltak som prikkbelastning, sammenhenger mellom deregulering og trafikksikkerhet med mer.

Det er et stort potensial for å bedre sikkerheten innenfor landbasert transport så vel ved tiltak rettet mot de enkelte elementene (trafikantene, kjøretøyene, transportsystemet) som ved tiltak av mer generell karakter. Det er ellers en stor utfordring å avklare hvordan trafikksikkerheten skal veies mot andre hensyn som økonomi, miljøforhold og lignende ved evaluering av aktuelle tiltak.

Omfanget av forsknings- og utviklingsaktiviteten på disse områdene beløper seg til 10-15 mill kr. pr. år. Forskningsprogrammet Risiko og sikkerhet i transportsektoren (RISIT) og nullvisjonssatsingen til Statens vegvesen utgjør for tiden et viktig grunnlag for aktivitetene ved NTNU og SINTEF på dette feltet. Forskningsaktiviteten finansieres ellers av en rekke ulike oppdragsgivere både i inn- og utland.

Av andre stikkord kan nevnes:

- Deregulering innenfor jernbane – hva er beste praksis innenfor EU?
- Deregulering og transportsikkerhet innenfor veg, bane, luft og sjø; en kunnskapsoversikt.
- Etablering og oppfølging av sikkerhetskritiske funksjoner innenfor Jernbaneverkets trafikkstyring .
- Katastrofepotensialet ved uønskede hendelser innenfor transport; hvilke faktorer avgjør om en hendelse utvikler seg til en storulykke?

1.4.2.2 Sårbarhet i kraftforsyningen

SINTEF har nylig gjennomført en analyse av sårbarheten i den nordiske kraftforsyningen på oppdrag fra Nordisk Ministerråd med tittelen *Vulnerability of the Nordic Power System.*[20] Formålet med studien var å identifisere faktiske og mulige hendelser i kraftsystemet som kan lede til alvorlige konsekvenser for samfunnet, og foreslå tiltak for å redusere og håndtere kritiske situasjoner. Tre sett av basishendelser er analysert: energiknapphet i tørrår, effektknapphet ved streng kulde og nettsammenbrudd. Disse kan hver for seg eller i kombinasjon føre til tre typer uønskede hendelser: Ekstreme priser, rasjonering og omfattende utfall[21] av strømforsyningen. Disse hendelser klassifiseres i henhold til alvorlighetsgraden. Sannsynligheten for hendelsene og alvorlighetsgraden bestemmer sammen risikoen, som deles inn i tre nivåer: i) lav risiko, som ikke krever tiltak, ii) medium risiko, hvor tiltak bør vurderes med hensyn til kostnader og iii) høy risiko, som anses som uakseptabelt og følgelig krever tiltak.

Resultatet av analysen viser at sannsynligheten for energiknapphet er på medium nivå for dagens system. Sannsynligheten for en situasjon som i vinteren 2002/03 eller verre er estimert til én gang hvert tiende år. Hvis en antar at produksjonskapasiteten utvides i takt med forbruksøkningen vil risikonivået være tilsvarende i 2010. Uten en slik økning i produksjonskapasiteten vil risikoen for ekstreme priser øke betydelig.

Med hensyn til effektknapphet tilsier analysen at risikonivået er lavt, delvis fordi det allerede har vært iverksatt en rekke tiltak av systemoperatørene. Imidlertid forventes dette å forverres til medium risiko mot 2010, fordi produksjonsøkningen primært skjer på anlegg med et lavere effektbidrag enn dagens produksjonssystem.

Også med hensyn til omfattende utfall anses risikonivået å være medium. Risikoen ligger primært i muligheten for større utfall i Sør-Skandinavia. Slike utfall vil alltid omfatte mange mennesker og dermed ha store konsekvenser. Denne situasjonen er imidlertid ikke vesentlig endret etter liberaliseringen. Det er ingen direkte indikasjoner på at dette vil forverres mot 2010, men det er en viss bekymring med hensyn til endringer i vedlikeholdsrutiner og tilgang på kvalifisert personell.

Rapporten anbefaler en rekke tiltak, deriblant reduksjon av usikkerheten i fremtidige reguleringstiltak, økning av elastisiteten i etterspørselen,

[20] Doorman, Gerard et al. 2004: Vulnerability of the Nordic Power System. TR A5962. SINTEF.
[21] Også omtalt som blackout.

reduksjon av virkningen av høye priser til utsatte grupper, forbedring og harmonisering av rammebetingelser for nettutbygging innenfor Norden, forbedret systemovervåkning, vern og trening av driftspersonale og sterkere satsing på forskning.

1.4.2.3 Sårbarhet i vannforsyning

SINTEF har de siste årene arbeidet mye med forfallsproblematikk i vannledningsnettet og hvordan dette påvirker påliteligheten til vannledningsnettet. Det er utviklet flere typer simuleringsmodeller for dette. SINTEF har også et stort internasjonalt nettverk på området og har bl.a. ledet EU-prosjektet *Computer Aided REhabilitation of Water Networks* (CARE-W) som omhandlet rehabiliteringsplanlegging av vannforsyningsnett. De største norske kommunene har vært med på dette arbeidet. Tre ulike modeller for å analysere sårbarheten i vannforsyningssystem er blitt utviklet og inngår i prosjektet. CARE-W var ferdig januar 2004. 15 forskningsinstitusjoner og 13 sluttbrukere/kommuner over hele Europa deltok i prosjektet.[22] Dette er verktøy som er nyttig for å tallfeste hvor sårbar vannforsyningen er, og hvilke tiltak som kan settes inn for å øke sikkerheten. Systematisk bruk av pålitelighetsmodeller for vannforsyning er et nyttig tiltak for å tallfeste sårbarheten i vannforsyningsnettet og for å kunne vurdere avbøtende tiltak på nettet.

På oppdrag fra Kommunal- og regionaldepartementet (KRD) har SINTEF også utført arbeidet med VARFIN – Utredning om informasjonssystem og finansieringsregime for vann. og avløpssektoren.[23] Et av delmålene med prosjektet var å vurdere hvorvidt det finansieringsregime som er innført på kraftnettsiden, kan overføres til VA.[24] Det ligger her en stor utfordring i å sikre at sårbarheten ikke økes ved deregulering. Tiltak for å opprettholde sikkerheten innen vannforsyning er beskrevet i rapporten. I St.prp. nr. 64 (2003-2004) Om lokaldemokrati, velferd og økonomi i kommunesektoren 2005 er VARFIN-utredningen m.m. drøftet, og KRD signaliserer der oppstart av arbeidet med å utvikle et nasjonalt informasjonssystem for VA-sektoren. Vurdering av alternativt finansieringsregime til dagens selvkostregime utsettes til man har høstet erfaringer med et nasjonalt informasjonssystem (benchmarking).

SINTEF utfører også forskning innenfor vannbehandling, eksempelvis i forhold til parasitter og virus i drikkevann.

1.4.2.4 Sårbarhet innenfor IKT

Forskningsrådets program IKT Sikkerhet og sårbarhet (IKT SoS) går fra 2004 til 2007. Programmet vil prioritere prosjekter der resultatet av FoU fra et informasjonssikkerhetssyn bidrar til å:

- Gjøre systemer og infrastruktur for elektronisk informasjonsutveksling robust og sikker.
- Utvikle innbyggeres og virksomheters holdninger slik at det bygges en sikkerhetskultur rundt bruk og utvikling av informasjonssystemer og elektronisk informasjonsutveksling .
- Etablere nye tjenester og produkter der sikkerhetsteknologi muliggjør nye måter å arbeide på, nye forretningsmodeller eller høyere effektivitet og god brukervennlighet.
- Utvikle, vedlikeholde og håndheve lover og forskrifter slik at de fremstår og kan anvendes på en enkel og oversiktlig måte.
- Muliggjøre deteksjon og sporing av sikkerhetshendelser med pålitelige og effektive metoder.
- Redusere kostnadene forbundet med etablering av riktig informasjonssikkerhet for målgruppen.

De prosjekter som SINTEF / NTNU er involvert i og som hittil er godkjent av Forskningsrådet via IKT SoS-programmet er:

- iAccess - Aksesskontroll i helsesystemer.
- IRMA - Hendelsesrapportering og oppfølging av IKT sikkerhetsbrudd via videreutvikling av sikkerhetskultur i olje og gass-sektoren.
- TID - TIDS stempling og oppfølging IKT hendelser i etterkant.

Andre godkjente prosjekter der NTNU / SINTEF spiller en rolle er:

- SWAP - Sikker Trådløs kommunikasjon for bærbare PCer.
- BAS5 – via FFI – Sårbarhet i samfunnskritiske IKT-systemer.
- Rapportering av Sikkerhetsbrudd i prosesstyring (SCADA[25]) knyttet til elektrisitetsforsyning, og annen infrastruktur.
- Enforce - Oppfølging av IKT politikk.
- Ambasec - Dynamisk modellering av sikkerhetskultur.
- Legal Inf. Security Regulations – Utvikling av Informasjonssikkerhet via lovverket.
- Gjennomføring av konferansen Safecomp 2005.

[22] http://www2.unife.it/care-w/

[23] Sjøvold, Frøydis et al. 2003: VARFIN - Utredning om informasjonssystem og finansieringsregime for VA-sektoren. STF50 A03302. SINTEF. http://odin.dep.no/filarkiv/195904/VARFIN_Endelig_sluttrapport.pdf

[24] VA – Vann og Avløp

[25] Supervisory Control And Data Acquisition.

1.4.2.5 Sikkerhet og sårbarhet generelt

SINTEF Teknologi og samfunn har definert Sikkerhet og sårbarhet som et utviklingsområde. Målsettingen er å videreutvikle kompetanseområdet sikkerhet og sårbarhet gjennom internasjonalt samarbeid i store EU-prosjekt. Som et ledd i dette er SINTEF blant annet. koordinator i EU prosjektsøknaden *Water for billions* hvor risiko og sårbarhet er en egen arbeidspakke. Søknaden er levert til 1. gangs evaluering oktober 2004.

Av andre prosjekter som er rapportert, kan stikkordmessig nevnes:

- Fem perspektiver på organisatoriske ulykker og fleksible organisasjoner.
- Slank og sårbar? Om verdien av organisatorisk redundans.
- Feiltoleranse, barrierer og sårbarhet innen petroleumsnæringen.
- Risiko på tvers – en gjennomgående og helhetlig strategi for risikovurdering innen HMS-området.

Informasjons- og systemsikkerhet er et satsningsområde i SINTEF IKT. Avdelingen har arbeidet med sikringssystemer for jernbane i 25-30 år og er utnevnt til Teknisk kontrollorgan i henhold til EU-direktiv 96/48. Det satses også på videreutvikling og etablering av samarbeidsrelasjoner til relevante institutter og bedrifter i Europa og USA.

NTNU har i flere år samarbeidet med Nasjonal Sikkerhetsmyndighet (NSM) og tidligere Forsvarets Overkommando, Sikkerhetsstaben (FO/S) om utvikling av metoder for risiko- og sårbarhetsanalyser av informasjon og følsomme objekter.

NTNU tilbyr en rekke kurs i risiko- og sårbarhetsanalyse og i informasjonssikkerhet. NTNU har startet et omfattende forskningsprogram innenfor informasjonssikkerhet.[26]

NTNU har etablert et internt nettverk for forskning og undervisning innenfor Risiko- og sårbarhetsstudier (ROSS).[27] ROSS-nettverket har videre status som *Marie Curie Training Site* innenfor risiko og sårbarhet. Dette betyr at EU har vurdert ROSS som et egnet miljø for doktorgradsutdanning i Europa.

1.4.3 UiS og SEROS

Forskningen ved sikkerhetsmiljøet ved Universitetet i Stavanger (UiS[28]) og ved Senter for Risikostyring og Samfunnssikkerhet (SEROS[29]) har som formål å bidra til å bygge et sikrere og mer robust samfunn. Ved å arbeide for å utvikle ny metodikk og kompetanse innen fagområdet risikostyring og samfunnssikkerhet ønsker miljøet å bidra til å redusere menneskelige, miljømessige og økonomiske tap i samfunnet. Kompetanse samles spesielt fra fagområdene risikoanalyse og risikostyring med fokus på ulykker, skader og tap, økonomisk risikostyring med fokus på kontraktsformer, markedsanalyser og prosjektstyring og samfunnssikkerhet med fokus på samfunnsplanlegging, beredskap, krisehåndtering og sikkerhetsledelse. Mye av den forskningsaktivitet som foregår har direkte eller indirekte relevans for kritisk infrastruktur, enten ved forskning på sårbarhet i systemer eller i forskning innen trusler mot systemene. I tillegg utarbeides det årlig masteroppgaver av både samfunnsvitenskapelig og teknisk karakter hvor ulike sikkerhetsaspekter ved kritisk infrastruktur studeres og analyseres.

Følgende forskning på kritisk infrastruktur foregår ved UiS og SEROS:

- Transportsektoren (vei, båt, jernbane, fly)
- Informasjonssikkerhet (IT)
- Helsesektoren
- Sårbarhet i samfunnskritisk IKT (BAS 5)

1.4.3.1 Transportsektoren

Prosjektet Risikoanalyse- og styring under Forskningsrådets program Risiko og sikkerhet i transportsektoren (RISIT), er utviklet av det samfunnssikkerhetsfaglige miljøet ved Høgskolen i Stavanger og Rogalandsforskning. De overordnede målsettinger er å utvikle egnet metodikk for risikoanalyse og å utvikle kunnskap og en hensiktsmessig tenkning om hvordan slike analyser skal brukes i en plan- og beslutningskontekst. Spesielt inngår kopling mellom risikoanalyser og kost/nytte-vurderinger og risikoakseptkriterier.

Det samfunnssikkerhetsfaglige miljøet ved UiS er videre involvert i et prosjekt for Vegdirektoratet der temaet er «organisering av trafikksikkerhetsarbeidet i fylkeskommuner og kommuner - virkning på trafikksikkerheten.» Målet er å finne ut om

[26] Mer informasjon om programmet finnes på: http://www.item.ntnu.no/infosik/

[27] Mer informasjon om ROSS-aktivitetene ved NTNU finnes på http://www.ntnu.no/ross

[28] Høgskolen i Stavanger (HiS) ble ved årskiftet 2004/2005 Universitetet i Stavanger (UiS)

[29] SEROS er et nasjonalt forskningsmiljø bestående av samfunnsvitere, ingeniører og økonomer fra Høgskolen i Stavanger og Rogalandsforskning som arbeider aktivt mot næringsliv og forvaltning for å utvikle ny metodikk og kompetanse innen fagområdet risikostyring og samfunnssikkerhet.

organiseringen har betydning for trafikksikkerhetsarbeidet i både fylkene og kommunene.

Det er søkt om støtte til et forskningsprosjekt med fokus på risikoutfordringer knyttet til samtidige endringsprosesser i norsk transportsektor. Dette er, med forbehold om innvilging fra Norges forskningsråd, et fremtidig forskningsprosjekt innen luftfart, jernbane og sjøtransport med oppstart medio 2005.

Samfunnssikkerhetsmiljøet har to doktorgradsstipendiater som forsker på sikkerhet inn mot transportsektoren. Det ene prosjektet, transportsikkerhet og risiko, ser primært på aktørene innefor transportsystemet med fokus på forebygging av ulykker gjennom optimal risikostyring. Det andre prosjektet – Robuste organisasjoner, slakk og sikkerhet – fokuserer på hvordan man kan være i stand til å utvikle mer robuste organisasjoner, organisasjoner som har evnen til å håndtere feil og uventede hendelser. Prosjektets empiriske arbeid vil i første fase foregå innenfor luftfartsbransjen, men vil muligens utvides med helsesektoren.

1.4.3.2 Helsesektoren

UiS har inngått avtale med Helse Vest vedrørende et forskningsprogram innen håndtering av feil og avvik i helsesektoren. Dette er et 3-årig forskningsprogram innen pasientsikkerhet med studier i Helse Stavanger, oppstart 2005.

1.4.3.3 Informasjonssikkerhet

Samfunnssikkerhetsmiljøet har et doktorgradsprosjekt innen analyse av informasjonssikkerhetshendelser med fokus på blant annet hvordan varierte typer dataangrep fører til ulike konsekvenser for varierte bransjer i samfunnet, for eksempel bank/finans og helse. Studiet vil se på type angriper, metodikk og konsekvens, samt dra implikasjoner av dette til videre forebyggende arbeid.

1.4.3.4 Andre forskningsprosjekter og teoriutvikling ved UiS og SEROS

Miljøet innen risikostyring utvikler metoder for analyse av barrierer og risiko (BORA-prosjektet) i tillegg til utvikling av prinsipper, metoder og modeller for beslutningstaking under usikkerhet, der risiko og sårbarhet er sentrale problemstillinger. Ut over dette foregår det en fortløpende teoriutvikling ved UiS og SEROS innen håndtering av risiko, risikovurderinger, risikoanalyser, beslutningsanalyser og beslutningsstøtte. Denne forskningen er ikke sektorspesifikk, men kan brukes inn mot studier av flere bransjer og sektorer i samfunnet.

Det forskes også på erfaringsoverføring og organisatorisk læring i beredskapsorganisasjoner.[30]

Kurset Samfunnsplanlegging og Sikkerhet II, ved mastergradsstudiet i samfunnssikkerhet, omhandler sårbarhet i infrastruktur. Følgende temaer blir tatt opp som dagsseminarer: Vann, avløp, renovasjon, kraftforsyning, transportsektoren, IKT og sikkerhet, og arealplanlegging for et mer robust samfunn.

UIS og SEROS er også involvert i BAS 5 om sårbarhet i samfunnskritiske IKT-systemer.

1.4.4 Østfoldundersøkelsen

I forbindelse med den anstrengte kraftsituasjonen våren 2003 ble landets energiverk pålagt å revidere sine planer for kraftrasjonering ved utkobling. Østfold Energi reviderte og utarbeidet rasjoneringsplanene våren 2003 for et område som dekker 2/3 av Østfold.[31] Det ble gjennomført en detaljert undersøkelse av virkningen på samfunnet og laget planer for rasjonering med roterende sonevise strømutkobling basert på dette. Det ble avdekket overraskende mange alvorlige samfunnsmessige konsekvenser.

Da rasjoneringsplanen ble laget, ble samfunnsfunksjonene veid opp mot hverandre som beskrevet i rasjoneringsforskriften etter følgende prioritet:

1. Liv og helse
2. Vital samfunnsmessig infrastruktur
3. Næringsliv, økonomiske interesser

Alle kraftledninger som kan utkobles ved fjernstyring, ble kartlagt helt ned til den enkelte adresse på så å si alle samfunnskritiske funksjoner. Tidlig viste problemet seg å være at strømnettet ikke er konstruert med tanke på rasjonering ved utkobling. Utgangspunktet for arbeidet ble derfor at rasjonering nesten er umulig, men dersom vi likevel må, hva gjør vi da?

For at rasjoneringen skulle ha noen virkning skulle kun 25 % av forbruket være fast innkoblet. Resten skulle kobles ut flere timer hvert døgn. Unntaket er at noen få viktige samfunnsfunksjoner får strøm hele døgnet. Nettet er imidlertid ikke bygget opp med tanke på strømrasjonering. Dersom vannverket skal ha strøm, får et meget stort område med «gratispassasjerer» rundt vannverket

[30] Studier i oljeselskap og profesjonelle redningsteam, det vil si politi/brann/AMK.

[31] Undersøkelsen ble foretatt av Carl Georg Abel, da ansatt ved Østfold Energi, nå ansatt ved NVE.

også strøm. Tilsvarende med trykkforsterkere for drikkevannet, kloakkpumper, telefonsentraler, sykehus, sykehjem, bakerier, politistasjoner, brannstasjoner, radio- og TV-sendere, basestasjoner for navigasjonssystemer, fyrlykter, tollstasjoner og så videre. Mye av dette må derfor likevel kobles ut dersom rasjoneringen skal ha noen effekt. Konsekvensene blir derfor også store.

Det er flere tusen lokale brytere geografisk spredd rundt om i hele fylket. De må kobles ut og inn manuelt på forskjellige steder mange ganger hvert døgn. I praksis er dette ikke mulig. For at rasjonering ved roterende sonevise utkoblinger rent praktisk skal kunne gjennomføres, må utkoblingen skje med fjernstyrte brytere ut fra halvstore transformatorstasjoner hvor hver bryter leverer strøm til et relativt stort geografisk område. Dette gir gratispassasjerer. Det er også slik at hvert område må være utkoblet mange timer ved rasjonering, ellers tas det oppsparte igjen ved innkobling, hvor alle elektriske apparater starter samtidig og drar mye strøm i startfasen.

De konkrete problemstillinger var mange. For eksempel ble det funnet at dersom alle sykehus, legevakter, sykehjem og ambulansestasjoner skulle ha fast forsyning, blir i praksis all strøm brukt opp på grunn av gratispassasjerene. Rent praktisk er det umulig å drive et sykehus uten strøm, men helt umulig uten rent vann, vaskeritjenester og mat. Det er også slik at noen sykehus kun har panelovner til oppvarming. For sykehjem ble det funnet at flere av institusjonene ikke kan få fast strømforsyning ved en slik rasjonering. Rent drikkevann til resten av befolkningen er også kritisk. Ved trykkbortfall vil det sive noe avløpsvann inn i vannrørene, og det kan dermed bryte ut epidemier. Dersom det leveres vann, men uten avløpspumper i drift, går avløpsvann i overløp til gater og kjellere. Uten fast forsyning av strøm må også meierier stoppe på grunn av bakterievekst, kjølelager på slakterier blir for varme, bakerier rekker ikke å få varmet opp bakerovnen og mat i butikkenes kjøledisker må kastes. Med sonevise utkoblinger vil også skipstrafikken måtte stanse når fyr, skipsledsbelysning og radarovervåkning er uten strøm. Togtrafikken får kjørestrøm sentralt, men strøm til bommer og signalanlegg tas ut lokalt, og på hver strekning vil det alltid være ett område som er utkoblet.

Telenettets konstruksjon forutsetter en normal strømforsyning. Bare de aller viktigste sentraler har dieselaggregat. Noen sentraler har batterireserve, men mange har ingen reservestrøm i det hele tatt. Mobilnettet slås raskt ut ved strømbrudd. Batteri løser heller ikke alle problemer. Å lade opp store nødstrømsanlegg for noen få timers drift, tar flere døgn. Dersom anleggene bare har strøm få timer før neste utkobling, lades heller ikke batteriene helt opp, og de ødelegges fort.

Industrien får også store problemer. Smelteovner ødelegges, ekstrudere og prosesser tettes og kontrakter brytes.

Elverkenes bemanning og utstyr er tilpasset en normalsituasjon. Ved rasjonering må det kobles i flere titalls brytere hver time hele døgnet, noe som krever store arbeidsressurser. Svært mange av disse bryterne har ligget fast inne i mange år, og det er ikke sikkert at de virker. De er heller ikke konstruert for å kobles flere ganger i døgnet.

Merk at til forskjell fra fullstendig utfall[32] vil det ved roterende utkoblinger alltid være noe som virker. For eksempel er det alltid en bensinstasjon som har strøm i nærheten. Østfold har 53.000 barn i skoler, barnehage og skolefritidsordninger. Ved manglende oppvarming må skoler stenges, noe som vil påføre småbarnsfamilier store praktiske problemer. Det må sannsynligvis løses ved at foreldre er hjemme fra arbeidet. Østfold har ikke storbyenes utfordringer med lange veitunneler som krever ventilasjon, stor avhengighet av strøm til lysregulering for å unngå trafikkaos og avhengighet av T-bane.

I Østfold representerer et titalls store bedrifter om lag halvparten av alt strømforbruk i hele fylket. Dersom myndighetene kan beordre utkobling av noen få bedrifter, ville derfor hele samfunnet ellers skånes.

Det kan se ut som at det er svakheter i forhold til lovverket ved at kommunene ikke er pålagt å ha nødstrøm til alle vannverk og kritiske trykkøkningsstasjoner. Likedan har ikke sykehusene nødstrømsanlegg som kan klare full drift. Tilsvarende konklusjon kom frem i et forprosjekt utført av DSB hvor det fremgår at nødstrømsforsyningen på sykehus har en gjennomgående lav pålitelighet.[33]

Etter at Østfoldundersøkelsen ble gjennomført har bevissthetsnivået blitt hevet. Blant annet har det vært gjennomført flere øvelser på overordnet nivå, og problemstillingene er derved kommet på dagsordenen. Østfoldundersøkelsen gir også en god illustrasjon på hvor avhengig samfunnets sikkerhet er av en stabil strømforsyning, og på at vi må operasjonalisere oss ned på et svært detaljert nivå før vi kan gjøre reelle prioriteringer.

[32] Utfall er også omtalt som blackout.
[33] Forprosjekt om nødstrømforsyning til norske somatiske sykehus, DSB 2004.

1.4.5 OECD

Organisasjonen for økonomisk samarbeid og utvikling (OECD) sin rapport *Emerging Systemic Risks in the 21st Century - An agenda for Action* (OECD, 2003) blir fulgt opp gjennom et nytt prosjekt: *Risk Management Policies in Selected OECD Countries.* Norge deltar i dette prosjektet med et *Case Study* som omhandler nasjonal organisering av tiltak med hensyn til IKT-sikkerhet. Målet med dette er dels å gi bidrag til generelle retningslinjer fra OECD med hensyn til risikostyring, dels å bidra til norsk policy på området IKT-sikkerhet.

1.4.6 Sårbarhetsutvalget fra 2000

I september 1999 ble det såkalte sårbarhetsutvalget nedsatt for å utrede det moderne samfunnets sårbarhet med sikte på å styrke samfunnets sikkerhet og beredskap.[34] Rapporten ble ferdig juli 2000. Utvalget konkluderte blant annet med at samfunnet er langt mer sårbart enn tidligere, og at svikt i noen få grunnpilarer og funksjoner i samfunnet kan resultere i kritiske problemet for samfunnet som helhet. Tap av telekommunikasjon og energiforsyning vil få særlig store konsekvenser. Utvalget viste videre til at andre aspekter som bidrar til økt sårbarhet kommer som følge av teknologiske endringer, økende kompleksitet i samfunnet, økende krav til effektivitet og kostnadsreduserende tiltak, redusert antall personell i viktige samfunnssektorer og økende privatisering av offentlige tjenester. Utvalget tok også for seg utfordringer knyttet til terrorisme. Utvalgets arbeid la et grunnlag for vår forståelse for sårbarheter i samfunnskritisk infrastruktur, og har bidratt med grunnlagsmateriale for flere av de tiltak vi har sett i de senere år.

1.4.7 Utvalg for sikring av landets kritiske infrastruktur

I oktober 2004 ble det nedsatt et utvalg for sikring av landets kritiske infrastruktur. Utvalget skal kartlegge virksomheter som antas å ha betydning for rikets sikkerhet og vitale nasjonale interesser. Videre skal utvalget kartlegge de virkemidler som brukes for å sikre nasjonale interesser når offentlige virksomheter privatiseres. Eksempler på områder som utvalgets vurdering skal omfatte er kraftsektoren, telesektoren, vannforsyningen og tilsvarende. Utvalgets rapport skal være ferdig til august 2005.[35]

[34] NOU 2000:24, Et sårbart samfunn, http://odin.dep.no/jd/norsk/dok/andre_dok/utredninger/012001-020005/dok-bn.html;

1.5 Trender og utviklingstendenser

Det er så langt gjort rede for større forsknings- og utredningsarbeid på sårbarhet i kritisk infrastruktur, blant annet på trender og utviklingstendenser som påvirker samfunnets sårbarhet. Dette er trender knyttet til globalisering, gjensidig avhengigheter, IKT-avhengighet, sentralisering, kraftavhengighet, omstilling, deregulering og privatisering. Mange av trendene er godt dokumentert i tidligere arbeider, og det vil i det følgende bli fokusert på tre temaer som DSB vil hevde krever større oppmerksomhet fremover i forbindelse med sårbarheter i kritisk infrastruktur. For det første deregulering og bortsetting[36], for det andre bruken av IKT i samfunnskritiske funksjoner og for det tredje globalisering. Felles for de tre er at de er sektorovergripende. Utfordringene er dermed av en slik karakter at de også må løses sektorovergripende.

1.5.1 Deregulering og bortsetting

Deregulering av kritisk infrastruktur er en del av en internasjonal trend, og er en politisk styrt prosess for videreutvikling av samfunnet. Deregulering og privatisering innebærer å innføre eller skjerpe konkurransen innenfor en sektor, og betyr at offentlige myndigheter overfører kontroll fra én sentral myndighet til en eller flere aktører som

[35] Utvalget gis følgende mandat:
- Utvalget skal kartlegge de virkemidler som brukes for å sikre rikets sikkerhet og vitale nasjonale interesser når offentlige virksomheter privatiseres. Utvalget skal kartlegge virksomheter som antas å ha betydning for rikets sikkerhet og vitale nasjonale interesser. Utvalget skal videre kartlegge de virkemidler som i dag brukes for å sikre rikets sikkerhet og vitale nasjonale interesser i forhold til virksomheter som ikke er offentlige, eller organiserte som selvstendige rettssubjekter helt eller delvis eid av det offentlige.
- Det vises i Sem-erklæringen til at begrunnelser for direkte offentlig eierskap kan være å ivareta økonomisk virksomhet markedet ellers ikke kan løse, for eksempel særlige infrastrukturoppgaver. På denne bakgrunn skal utvalget vurdere hva slags infrastruktur Staten bør eie helt eller delvis. Denne vurderingen skal avgrenses til infrastruktur der særlig viktige hensyn ikke kan ivaretas på annen måte.
- Med utgangspunkt i den samlede oversikt som er fremskaffet gjennom mandatets punkt 1 skal utvalget vurdere hvilke virkemidler som kan være aktuelle å bruke for å ivareta rikets sikkerhet og vitale nasjonale interesser i forhold til virksomheter som privatiseres eller som er i privat eie.
- Ved vurderingen av virkemidler skal utvalget også ta i betraktning om bruk av enkelte virkemidler representerer så vidt store inngrep overfor den tiltakene retter seg mot at bruken av virkemidler må frarås, eller at særskilt lovhjemmel kreves.
- Forholdet til konkurransemessige og øvrige hensyn skal inngå som en del av utvalgets vurderinger.
- Utvalget skal vurdere de økonomiske og administrative konsekvenser av sine forslag. Minst ett forslag skal baseres på uendret ressursbruk, jf. utredningsinstruksen pkt. 3.1.
- Utvalgets rapport skal være Justis- og politidepartementet i hende innen 01.08.2005.

opererer etter markedsøkonomiske prinsipper. Virksomheter med beredskapsoppgaver dereguleres også, blant annet virksomheter som på grunn av deres økonomiske viktighet eller på grunn av deres kritiske funksjon for samfunnet kan sies å utgjøre en del av nasjonens vitale interesser. Overfor disse virksomhetene er det behov for å sikre at beredskapsoppgavene kan ivaretas på en hensiktsmessig måte. Et annet trekk i denne sammenheng er at eierstrukturen i selskaper kan fremstå med uklar nasjonalitet og at eierkonstellasjoner i prinsippet kan endres raskt. Det er også en utfordring at utviklingen går så hurtig at myndighetsorganer blir hengende etter både organisatorisk og i forhold til lovgivningen. Ved slike anledninger handler det ofte om manglende evne til å kommunisere et samfunnsansvar overfor aktører hvis fremste prioritet er å sikre inntjening. Summert opp på engelsk kan det omtales som at *the business of business is business and nothing else*.

Inn i dette bildet kommer også bortsetting. Hensikten med bortsetting er å fokusere på egne kjerneområder i en virksomhet ved å sette ut aktiviteter som er definert som perifere. Det kan være drifting av IKT-systemer, vedlikehold, regnskap og så videre. Som resultat kan driften bli mer kosteffektiv, men samtidig gjør virksomheten seg avhengig av andre virksomheter for tjenester som er sentrale for opprettholdelse av egen drift. Manglende forståelse og nærhet til driftskritiske løsninger i egen virksomhet kan derfor skape en sårbarhet overfor uforutsette hendelser. Bildet kompliseres ytterligere ved at sentrale tjenester kan bortsettes uavhengig av geografi, og det kan derfor oppstå situasjoner hvor samfunnskritiske funksjoner er avhengig av tjenester utført utenfor landets grenser, og dermed utenfor nasjonal kontroll. Sårbarheten øker i takt med kompleksiteten.

Samfunnssikkerhet og beredskapsspørsmål knyttet til deregulering og bortsetting i forskjellige sektorer er svært komplekse og uensartede, og DSB ser det derfor som viktig å opprettholde en høy utrednings- og forskningsinnsats med et sektorovergripende blikk på området.

1.5.2 Sårbarhet og IKT i kritisk infrastruktur

Et annet sektorovergripende utviklingstrekk som DSB ønsker å trekke frem er teknologiutvikling innenfor IKT. Som med globalisering er den en viktig del av samfunns- og velstandsutviklingen. Samtidig stiller den samfunnet overfor ett sett med nye sårbarhetsutfordringer. Det skyldes at befolkningens velferd i økende grad er avhengig av teknologiske løsninger som er koblet sammen i nettverk. På de fleste sektorer bryter samfunnskritiske tjenester sammen uten tilgjengelighet til IKT. Den potensielle sårbarheten og skadepotensialet er derfor særdeles høy.

Et gjennomgående trekk er datanettverkenes tendens til å klumpe seg sammen rundt knutepunkter.[37] Fordi det mangler oversikt over punktene og hvor sårbare de er, står samfunnet overfor en strukturell sårbarhet som er vanskelig å håndtere. Knutepunktene i datanettverk er av forskjellig karakter. Det kan være knutepunkter av informasjon, programvare eller maskinvare. Når det gjelder det sistnevnte er det i Norge flere knutepunkter, blant annet de såkalte NIXene som er samtrafikkpunkter for IP-trafikk i Norge.[38] Mye av internettrafikken går gjennom disse punktene, og en svikt vil få uoversiktlige konsekvenser.

En annen side er at ny teknologi legger til rette for å effektivisere drift ved å sentralisere tjenester. Dette gir samtidig enkeltpersoner stor makt til å forårsake skade, enten den er tilsiktet eller utilsiktet. Teknologien muliggjør på mange måter at liten tue velter stort lass, også innenfor kritisk infrastruktur. Det er dermed en sårbarhet i denne sammenhengen at makt til å forårsake sårbarhet og skade forsvinner innover, bort fra systemnivå ned til individnivå. Det setter ekstra krav til opplæring, kontroll med tilgang og håndtering av innsideproblematikk.

Innenfor kritiske samfunnsfunksjoner vokser også sårbarhetspotensialet etter hvert som prosesser som tidligere ble kontrollert innenfor lukkede systemer, i økende grad kobles til internett. Eksempelvis styrings- og prosessystemer som blir koblet opp mot administrative systemer, som igjen blir koblet opp mot internett for å imøtekomme publikums behov for informasjon. Det er også vekst i teknologiske løsninger hvor eksempelvis driftspersonale plassert utenfor eget nettverk har behov for å knytte seg direkte opp mot egne prosessystemer, og hvor internett er koblingen mellom bruker og det interne nettverket. Denne utviklingen kommer hovedsakelig som et resultat av krav til økt effektivitet.

En sektor hvor dette de senere år er blitt tydelig, er i olje- og gassektoren med såkalte eDriftsløsninger. eDrift er en samlebetegnelse for et driftskonsept der ny informasjons- og kommunikasjonsteknologi og sanntidsdata utnyttes for å opti-

[36] Outsourcing

[37] Barabási, Albert-László. 2002. Linked: How Everything Is Connected to Everything Else and What It Means, 2002.

[38] NIX – Norwegian Internet eXchange

malisere operasjoner på sokkelen. eDrift blir omtalt som et tredje effektivitetssprang for olje- og gassindustrien.[39] eDrift skal bidra til å redusere kostnadsnivået, akselerere produksjonen, øke utvinningsgraden og bedre HMS-resultatene.[40] Flere eDrift-konsepter er i drift hos forskjellige selskaper og flere er på vei. Sleipner B fjernopereres fra Sleipner A, Hod fra Valhall, Huldra fra Veslefrikk og Tambar fra Ula. På Ekofisk har ConocoPhillips avbemannet to plattformer, installert én ubemannet plattform og lagt planer for fjernoperasjon av nye, opprinnelig bemannede enheter. Dessuten skal de nye undervannsinstallasjonene til Ormen Lange og Snøhvit fjernopereres fra landanlegg. Det er også mulig å fjernoperere store deler av produksjonsanlegget på Troll A fra landanlegget på Kollsnes. eDrifts-konseptet vil akselerere og forsterke utviklingen.[41]

Det er knyttet store forventinger til eDrift. Samtidig åpner utviklingen opp for nye sårbarheter i en samfunnskritisk sektor. Eksempelvis vil et typisk kontrollsenter på land ha flere leverandørdrevne støttesentre som opererer geografisk uavhengig av kontrollsenteret. Støttesentrene har behov for å koble seg på ved for eksempel feilretting, og det vil som regel skje ved hjelp av internettbasert kommunikasjon. Kritiske styringssystemer får da en fysisk tilkobling mot utenverden via internett. Offshoreinstallasjonene er også sårbare overfor driftstans hos de landbaserte kontrollsentrene ved strømstans, brann og lignende. Ut over dette er det en generell betraktning at økende kompleksitet i tekniske systemer og datasystemer samt nye grensesnitt mellom menneske og maskin er faktorer som i tillegg øker risikoen for feil og åpner for utilsiktede konsekvenser og nye sårbarheter.

I USA er det i forlengelsen av slike utfordringer kommet frem en særlig bekymring overfor beskyttelse av SCADA-systemer, senest i forbindelse strømutfallet august 2003 som rammet store deler av det nordøstlige USA og det sørlige Canada.[42] Et SCADA-nettverk består av sammenkoblede IKT-systemer og programvare som utfører en rekke funksjoner spredt utover forskjellig industri og kritisk infrastruktur. De amerikanske SCADA-systemene var i utgangspunktet konstruert for å operere i isolerte nettverk med tanke på funksjonalitet, ikke sikkerhet.[43] I USA er de nå i økende grad enten direkte eller indirekte koblet til internett blant annet fordi driftspersonell har behov for å overvåke de SCADA-tilkoblede systemene utenfor det interne nettverket. Dette øker risikoen for uautorisert tilgang til systemenes kontrollmekanismer. I USA og Canada er opprettelsen av et eget SCADA-sikkerhetsprogram under vurdering for å sikre en helhetlig tilnærming til både den fysiske og logiske sikkerheten i slike systemer.[44] SCADA-systemer er av interesse i vår sammenheng fordi de også i Norge er nødvendige for driften av samfunnskritiske funksjoner.

Sårbarheten i IKT-systemer kan illustreres ved hendelsen i Sverige i mai 2004, da dataormen Sasser slo ut et stort antall PCer på sykehus i Västra Götaland og Lund. Ormen slo blant annet ut tilgangen til røntgenbilder og elektroniske pasientjournaler. Resultatet var at pasienter ble flyttet eller omdirigert til andre sykehus. Likevel kan ikke episoden karakteriseres som kritisk. Ingen pasienter led skade og Sasser fikk ingen alvorlige konsekvenser for mulighetene til å gi individuell hjelp til trengende pasienter. Hendelsen avslørte derimot hvor sårbar en organisasjon er når den er avhengig av IT-systemer på døgnkontinuerlig basis.[45] Dette var en lavtrusselhendelse som ikke var spesifikt rettet mot noe enkelt mål. Det er derimot naturlig å anta at et høykapasitetsangrep rettet mot svenske sykehus kan få helt andre og dramatiske konsekvenser. Det er også naturlig å anta at et høykapasitetsangrep også kan skje mot norske sykehus, selv om de mest kritisk systemene ikke er tilgjenglige via åpne systemer som internett. Ormen fikk da også noen få, men mindre konsekvenser for norsk helsevesen ved at lokalsykehuset i Orkdal hadde driftsproblemer med de pasientadministrative systemene, de elektroniske pasientjournalene

[39] I Nordsjøen har det med jevne mellomrom oppstått sprang i utviklingen som har medført større effektivitet i operasjonene. Det snakkes gjerne om 3 sprang: Første effektiviseringssprang kom på 1980-tallet med nytt boreutstyr, nye utvinningsmetoder og 2D-utstyr. Andre effektiviseringssprang kom på 1990-tallet med horisontale brønner, undervannsenheter, flytende produksjonsenheter og 3D-seismikk. Tredje effektiviseringssprang som er aktuelt nå innebærer såkalt eDrift med intelligente «nedihullssensorer», forbedret retningsboring, operasjonssentre for sanntids datautnyttelse, fjernovervåking og –styring..

[40] eDrift på norsk sokkel – det tredje effektivitetsspranget, OLF-rapport 2003. http://www.olf.no/?18389.pdf

[41] eDrift på norsk sokkel – det tredje effektivitetsspranget, OLF-rapport 2003. http://www.olf.no/?18389.pdf

[42] SCADA står for Supervisory Control And Data Acquisition. SCADA-systemer muliggjør fjernovervåkning og fjernstyring, eksempelvis innen offshore, vann, elektrisitet, kloakk og andre kritiske infrastrukturer.

[43] Assessment and Remediation of Vulnerabilities in SCADA and Process Control Systems, Internet Security Systems, 03/03. www.iss.net

[44] Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, U.S.-Canada Power System Outage Task Force, April 2004.

[45] Lindberg, Bertil, Kartläggning och bedömning av konsekvenser av Sasser-masken i samhället, rapport 2004-06-23, Krisberedskapsmyndigheten Sverige

samt laboratorie- og røntgensystemet på grunn av Sasser.

Tilsvarende ble det amerikanske kjernekraftverket David-Besse i Ohio rammet av Slammerormen i januar 2003. Anlegget var for anledningen avstengt, men angrepet fra Slammer satte et viktig overvåkningssystem ut av drift i nærmere fem timer.[46] Årsaken var delvis en feilimplementert forbindelse inn i anleggets datanettverk, og delvis at en datamaskin uten virusbeskyttelse ble feilaktig ansett å være frittstående fra anlegget og dermed ikke hadde behov for beskyttelse. Det fantes redundante, analoge reservesystemer som var upåvirket av ormen, men driftsoperatørene fikk en betraktelig økt arbeidsbelastning. Også denne episoden var en lavtrusselhendelse som ikke var rettet mot noe enkelt mål.

På bakgrunn av slike erkjennelser er det grunn til å reise spørsmål med om sikkerheten er godt nok ivaretatt når driften av samfunnskritiske funksjoner får en kobling opp mot internett. Dette gjelder overfor lavkapasitetstrusler som Slammer og Sasser, men gjør seg i særlig grad gjeldene overfor den mer ukjente delen av trusselspekteret hvor ondsinnede aktører med høy kapasitet fatter interesse. Det må tilføyes at det er iverksatt logiske sikringstiltak mellom de systemene som kontrollerer og styrer prosessene innen samfunnskritiske områder og de administrative og publikumsrettede tjenestene. Det er likevel knyttet en viss usikkerhet til hvor effektive disse er, noe eksemplene ovenfor viser. Det finnes per i dag ingen oversikt over hvor utbredt koblingen mellom prosessystemer og åpne datanettverk er for de forskjellige kritiske samfunnssektorene, men utviklingen så langt tilsier at dette er et område i vekst.

Uavhengig av om de mest kritiske systemene er godt nok sikret, vil også en svikt i de administrative og publikumsrettede tjenestene være problematisk for samfunnet som helhet. Bortfall av tjenester knyttet til ordrebestilling, fakturering, vareflyt, nettbanktjenester, IP-telefoni og lignende vil få store konsekvenser meget raskt. I løpet av få år er slike tjenester blitt vesentlige i befolkningens daglige gjøremål. Det er forventet at avhengigheten vil øke i årene som kommer.

[46] Christiansson, Henrik. Värdering av IT-säkerhetsanalysemetoder inom samhällsviktig infrastruktur, Rapport FOI R 1350 SE, Totalförsvarets forskningsinstitut, Sverige, 2004; Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, U.S.-Canada Power System Outage Task Force, April 2004.

1.5.3 Internasjonale trender

Felles for det som er tatt opp er at det har trekk koblet til globalisering. Globaliseringen gir en rekke fordeler blant annet økt velferd og et større kulturelt mangfold, men det åpner samtidig opp for økt sårbarhet. Norsk produksjon og tjenesteyting blir i økende grad vevd sammen med og blir avhengig av resten av verden. Dette går også den andre veien, særlig i forhold til andre lands avhengighet av vår olje- og gassproduksjon. Produksjonsstopp i Norge betyr stopp i leveransene til mottagerland. Globalisering gjør oss dermed ikke bare potensielt mer sårbar, den bidrar også til andres sårbarhet. Et nytt trekk de senere år finner vi i koblingen mellom globalisering og avanserte IKT-løsninger. Samfunnskritiske funksjoner kan nå i økende grad bli kontrollert av driftssentraler utenfor landets grenser. Dette gjelder særlig på finans- og energisektoren, men også til en viss grad transportsektoren. Vi ser at makt til å motarbeide sårbarhet forsvinner utover, bort fra nasjonalstaten. En forsterkende effekt er at befolkningen i økende grad er avhengig av disse tjenestene for å løse dagligdagse utfordringer. Avhengigheten er blant annet fundert i at befolkningen er mindre robust overfor uforutsette hendelser i dag enn tidligere. Dette gjelder særlig i de større byene.

1.6 Kunnskapsbehov

1.6.1 Tilrettelegging for kunnskapsutvikling

Samfunnets raske endringstakt tilsier fortsatt fokus på forskning og utredning om sårbarhet i kritisk infrastruktur. For det første bør det opprettes et eget forskningsprogram i Norges forskningsråd med fokus på samfunnssikkerhet. En utredningsgruppe er nå etablert i regi av Norges forskningsråd. Hensikten med en slik løsning er å sikre en helhetlig tilnærming som involverer mange. For det andre bør det finansieres et permanent miljø for forskning om samfunnets sårbarhet for eksempel ved Forsvarets forskningsinstitutt. Som tidligere vist har FFI siden 1994 vært ledende på forskning om samfunnets sårbarhet med BAS-prosjektene. Likevel fremstår det som en utfordring at BAS-prosjektene finansieres ad-hoc fra prosjekt til prosjekt og at miljøet står i fare for å forvitre mellom hvert prosjekt. Det er også et aspekt at de sikkerhetspolitiske utfordringene i dag er av mer sivil enn militær karakter. Økt fokus ved FFI på sivil sårbarhetsforskning vil styrke den sivile kompetansen, og skape et permanent miljø som ser militære og sivile utfordringer i sammenheng. For det tredje vil det fortsatt være behov for å starte tidsav-

grensede forskningsprosjekter med ad-hoc midler. Det ligger i sakens natur at hendelser som utfordrer samfunnets sikkerhet dukker opp uten varsel. Det må ligge inne en kapasitet for kortere analyser av hendelser ut over det myndighetene selv er i stand til å utføre.

DSB anser at en slik tredelt tilnærming for å tilrettelegge for kunnskapsproduksjon innen sårbarhet i kritisk infrastruktur, vil bidra til balanse mellom myndighetenes behov for anvendt forskning og forskningsmiljøenes behov for en fri og uavhengig rolle. Samtidig vil det bidra til å etablere en langsiktighet som vil motvirke at kunnskapsforvaltningen i for stor grad blir hendelsesorientert.

1.6.2 Sentrale temaer

DSB understreker behovet for en sektorovergripende tilnærming overfor sårbarheter i SCADA-systemer og andre prosesstyringssystemer i samfunnskritisk infrastruktur. Fordi de samfunnskritiske funksjonene er en del av globaliseringen, og fordi endringene skjer i et høyt tempo, anser DSB at globalisering er en sektorovergripende utfordring hvor kunnskapstilfanget må økes. Dette gjelder særlig i forhold til nasjonalstatens relevans og styringsmulighet. Større samarbeid ut over grensene er nødvendig. Det gjelder både i forhold til kunnskapsutvikling, men også i forhold til det operative samarbeidet. Vi mangler også kunnskap om sårbarhet overfor terrorisme sett opp mot samfunnskritisk infrastruktur.

1.7 Oppsummering og anbefalinger

Norge var tidlig ute med bevissthet omkring sårbarhet i kritisk infrastruktur. I 1994 startet BAS-forskningen ved FFI. Det også større miljøer ved Universitetet i Stavanger og Norges teknisk-naturvitenskapelige universitet som arbeider med sårbarheter i kritisk infrastruktur. I 2000 ble bevisstheten om det sårbare samfunn løftet opp til et politisk nivå med sårbarhetsutvalgets rapport.[47] Samtidig er samfunnet i konstant endring, og det ligger en utfordring i å tilpasse seg disse endringene. Denne utredningen har hatt som fokus de overordnede sektorovergripende utfordringene, både i forhold til det vi vet, og i forhold til hvor vi burde gå videre for å redusere sårbarheter.

Oppsummert anbefaler DSB følgende:

- At det etableres et sektorovergripende sett med kriterier for identifisering og rangering av samfunnskritisk infrastruktur. Det pågår et arbeid i BAS5 på dette.
- At det i forbindelse med omorganisering av myndighetsansvar og dereguleringer gjennomføres en helhetlig analyse om tverrsektorielle konsekvenser i forhold til forebygging og beredskap i samfunnskritisk infrastruktur.
  - Innenfor dette at det ses nærmere på konsekvensene for lovverket innenfor samfunnssikkerhet.
- At det holdes et særlig fokus på tre områder hvor myndighetene har behov for ytterligere kunnskap:
  - Bruk av IKT i samfunnskritiske funksjoner, med et særlig blikk på sektorovergripende utfordringer for SCADA og prosesstyringssystemer
  - Sektorovergripende konsekvenser for beredskap og samfunnssikkerhet ved deregulering av samfunnskritiske sektorer og virksomheter
  - Sektorovergripende konsekvenser av globalisering for samfunnskritisk infrastruktur
- At det legges til rette for kunnskapsforvaltning i Norge ut fra:
  - Å opprette et eget forskningsprogram i Norges forskningsråd med fokus på samfunnssikkerhet.
  - At det sikres finansiering for å opprette et permanent forskningsmiljø ved FFI med fokus på samfunnets sårbarhet
  - At det sikres kapasitet til ad-hoc analyser av samfunnets sårbarhet

[47] NOU 2000:24, Et sårbart samfunn, http://odin.dep.no/jd/norsk/dok/andre_dok/utredninger/012001-020005/dok-bn.html.

Vedlegg 4

Notat – Et blikk på begrepet samfunnssikkerhet for å operasjonalisere «nasjonal trygghetsfølelse»

Kjetil Sørli, Direktoratet for samfunnssikkerhet og beredskap
Enhet for analyse og utredning 8. august 2005

1 Et blikk på begrepet samfunnssikkerhet for å operasjonalisere «nasjonal tryggetsfølelse»

Begrepet «nasjonal trygghetsfølelse» er et sentralt begrep for Infrastrukturutvalget. Som et innspill til å operasjonalisere begrepet, vil dette notatet ta for seg et annet begrep, nemlig samfunnssikkerhet. Hensikten med å dra inn samfunnssikkerhetsbegrepet er at det er et parallelt begrep, om enn ikke fullt ut synonymt; en høy grad av samfunnssikkerhet er en forutsetning for den nasjonale trygghetsfølelsen. Hva samfunnssikkerhet er, er derfor førende for hva vi definerer som nasjonal trygghetsfølgelse. Det er også et poeng å ta for seg samfunnssikkerhetsbegrepet fordi det i motsetning til «nasjonal tryggetsfølelse», har vært i bruk noen år, og at det er knyttet diskusjoner og uenighet til hva samfunnssikkerhet egentlig er. Et blikk på denne diskusjonen kan avhjelpe med å begrepsfeste og operasjonalisere «nasjonal tryggetsfølgelse». Teksten er hentet fra en kommende FFI-rapport.[1]

1.1 Samfunnssikkerhet vs Totalforsvaret vs Homeland Security

Som en del av å tolke og definere samfunnskritiske funksjoner og kritisk infrastruktur, er én vinkling å se på begrepsapparatet knyttet til utviklingen av risikosamfunnet[2] slik det fremstår i Norge. De siste årene har samfunnssikkerhet etablert seg som et eget begrep i Norge og dels i andre skandinaviske land for å definere potensiell risiko mot samfunnet. Begrepet har imidlertid ikke satt seg ennå, noe som har sammenheng med at det finnes flere fortolkninger. Utviklingen av begrepet henger nøye sammen med fremveksten av risikosamfunnet, slutten av den kalde krigen, oppblomstringen av regionale konflikter og sikkerhetsutviklingen etter 11. september 2001. Det finnes i dag minst tre hovedbegreper som bør ses i forhold til hverandre:

- Homeland Security
- Totalforsvar
- Samfunnssikkerhet

1.1.1 Homeland Security

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

> Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. [3]

Etter denne definisjonen er begrepet Homeland Security fokusert på terrortrusselen. Departement of Homeland Security (DHS) har imidlertid underlagte etater som også arbeider med andre forhold enn terrorisme. Federal Emergency Mana-

[1] Teksten er hentet fra en FFI-rapport som vil foreligge høsten 2005 skrevet av Kjetil Sørli (DSB). Deler av teksten er også hentet fra ikke-utgitte tekster til bruk i Nasjonal sårbarhets- og beredskapsrapport 2004 fra DSB. Stein Henriksen (DSB) har skrevet utvalgte deler av nevnte tekst.

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

[3] National Strategy for Homeland Security, Office of Homeland Security, juli 2002

gement Agency[4] (FEMA) har for eksempel også prioritet på risiko knyttet til naturkatastrofer, transport av farlig gods, forebygging, beredskapsplanlegging, krisehåndtering og normalisering etter kriser.

1.1.2 Totalforsvar

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

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

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

1.1.3 Samfunnssikkerhet

Samfunnssikkerhetsbegrepet er nytt, og det foregår ennå en prosess med hensyn til å feste begrepsinnholdet. En tilnærming til begrepet er å vise til Stortingsmelding 39 (2003 – 2004) om samfunnssikkerhet og sivilt-militær samarbeid[5] og hva slags temaer som tas opp der:

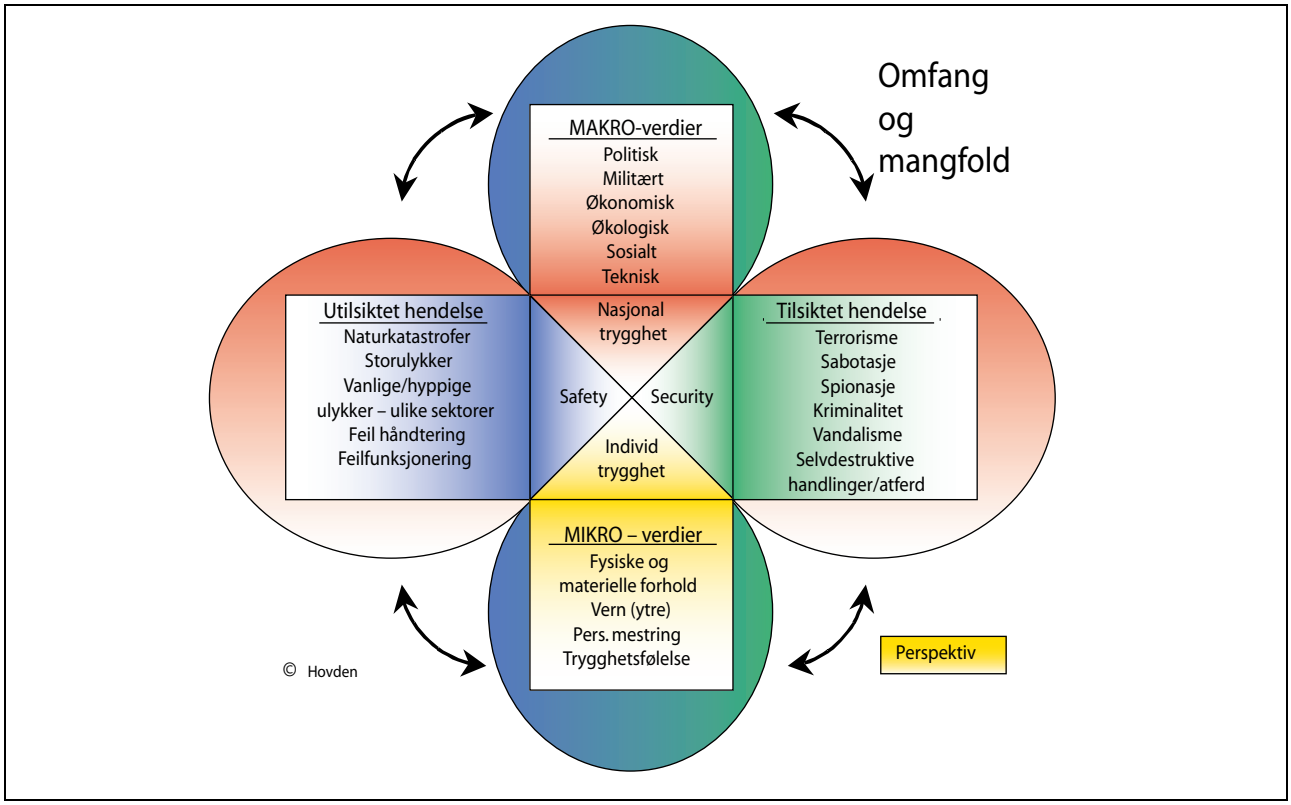
- Omdefinering av sivilt-militært samarbeid innen totalforsvarskonseptet og en rekke andre områder
- Politi og Forsvar i kampen mot terrorismen – hvem gjør hva?
- Oppgradering av Politiets kapasiteter
- Omdefinering av militære roller, særlig Heimevernet
- Etterretningssamordning
- Samarbeid om internasjonal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

Det kan ut fra dette hevdes å være en viss bredde i begrepet samfunnssikkerhet, og en tilsvarende avgrensingsutfordring. Det som med sikkerhet kan hevdes, er at begrepet ikke er festet til noe bestemt scenario av typen krig eller terror, men omfatter alle potensielle krisescenarier. Ettersom begrepet knapt kan avgrenses tematisk/fenomenologisk, må det søkes etter en «terskel», det vil si man må tilnærme seg et skille for eksempel mellom det som kan betraktes som et samfunnsproblem, som er relevant for begrepet, og det som kan betraktes som et individuelt problem, som er mindre relevant. Et forsøk på det kan illustreres i figuren nedenfor [Figur 4.1].

Figuren illustrerer forholdet mellom nasjonal sikkerhet, sikkerhet for individet, *safety* og *security*. Figuren viser bredden og omfanget av risiko og sårbarhet for samfunnet og individet generelt. Den vertikale aksen viser noen av utfordringene med å koble forskjellige lag i risikohåndtering, med andre ord koblingene mellom det globale, internasjonale, nasjonale, regionale, lokale og individuelle med hensyn til å håndtere risiko. Den horisontale

[4] A Nation Prepared, Federal Emergency Management Agency Strategic Plan, Fiscal Years 2003 – 2008

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



Figur 4.1 The vertical macro-micro perspective on risk management combined with types of hazards/ threats and events (Hovden, 1998).

aksen dekker alt fra naturkatastrofer og menneskeskapte ulykker til tilsiktede handlinger så som terror. Figuren gir dermed en oversikt over forhold som kan falle innenfor samfunnssikkerhetsbegrepet.

Definisjonen av samfunnssikkerhet er ikke entydig, men kan deles i tre; en bred og omfattende definisjon, en snever definisjon og en politisk definisjon som beveger seg mellom de to andre, avhengig av det politiske sakskartet.

1.1.3.1 Bred definisjon

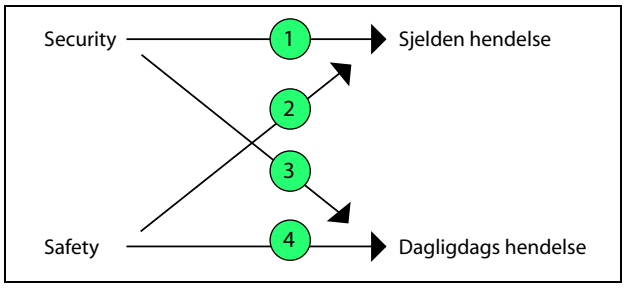
I den brede definisjonen er samfunnssikkerhet for det første å kunne forebygge og håndtere ekstraordinære hendelser. For det andre er samfunnssikkerhet å ha ressurser til å forebygge og håndtere dagligdagse hendelser. Det er dermed ressursene til å håndtere som er i fokus, ikke hendelsen i seg selv. For eksempel truer ikke én enkelt brann samfunnets sikkerhet, men hvis samfunnet ikke har ressurser til å håndtere branner vil samfunnets sikkerhet være truet. For det tredje er samfunnssikkerhet å forhindre at mindre hendelser blir så mange at det går ut over samfunnet. For eksempel innebærer dødsulykker i trafikken store personlige og samfunnsmessige omkostninger, men det truer ikke samfunnets sikkerhet i seg selv. Hvis antallet dødsulykker i trafikken derimot stiger til et antall hvor det påvirker samfunnets daglige drift svært negativt, vil det true samfunnssikkerheten.

Fellesnevneren i forhold til en bred definisjon som omfatter de tre aspektene, er at det på en eller annen måte har å gjøre med samfunnets mulighet til minimalisere alle tenkelige risikoer. Det kan argumenteres for at en bred definisjon av begrepet gjør det upresist og vanskelig å bruke, og da særlig i forhold til en politisk virkelighet hvor det alltid vil være et spørsmål om å prioritere.

Spennet i begrepsinnholdet kan også illustreres med figuren nedenfor [Figur 4.2]:

1.1.3.2 Snever definisjon

Den andre og mer snevre definisjonen har fokus på at samfunnssikkerhet handler om å forhindre eller avdempe effektene av ekstraordinære hendelser som i tillegg krever ressurser ut over det vanlige. Her er de dagligdagse hendelsene ekskludert, det vil i hovedsak si den nederste delen av Hovdens firkløver og punkt 3 og 4 i figur?. Hensikten med å spisse begrepet er å forhindre at de dagligdagse hendelsene tar all fokus fra de ekstraordinære, slik



Figur 4.2 : Samfunnssikkerhet

Sjelden tilsiktet hendelse (security 1) f. eks terror
Sjelden utilsiktet hendelse (safety 2)
f. eks stor naturkatastrofe
Dagligdags tilsiktet hendelse (security 3)
f. eks hverdagskriminalitet
Dagligdags utilsiktet hendelse (safety 4)
f. eks trafikkulykke

at samfunnet dermed står i fare for glemme disse. Innenfor en slik definisjon har ekstraordinære hendelser fokus fordi de har et meget stort skadepotensial. Det kan også hevdes at det er en forventing i befolkningen om at myndighetene er i stand til å håndtere det ekstraordinære, og at bevisstheten dermed må være høy fra myndighetsorganer.

Hovden hevder i denne sammenheng at i forhold til å håndtere samfunnets sårbarhet, så er dagligdagse hendelser så som trafikkulykker, hverdagskriminalitet og liknende ekskludert. Videre skriver han at innenfor rammen av samfunnets sårbarhet er problemstillingene vanligvis relatert til overlevelse og gjenoppretting av vitale samfunnsfunksjoner, med andre ord trusler mot infrastruktur knyttet til energiforsyning, IKT, pandemier og liknende.[6] Hovden legger seg således på en snever definisjon av begrepet samfunnssikkerhet.

1.1.3.3 Politisk definisjon

Den tredje definisjonen av samfunnssikkerhet er den politiske. I St. meld. nr. 17 (2001-2002) står det følgende:

> Samfunnssikkerhet brukes i denne meldingen for å beskrive den evne samfunnet som sådan har til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for påkjenninger.[7]

Samfunnssikkerhetsbegrepet brukes bredt og dekker sikkerhet mot hele spekteret av utfordringer, fra begrensede, naturskapte hendelser, via større krisesituasjoner som representerer omfattende fare for liv, helse, miljø og materielle verdier, til sikkerhetsutfordringer som truer nasjonens selvstendighet eller eksistens.

I St. meld. nr. 39 (2003-2004) står det følgende:

> Regjeringen vil understreke at det grunnleggende mål for alt samfunnssikkerhetsarbeid er å forebygge at uønskede hendelser inntreffer og minimalisere konsekvensene når slike situasjoner skulle oppstå. [...] Arbeidet med forebyggende brannvern er en viktig del av samfunnssikkerhetsarbeidet. [...] I samfunnssikkerhetsarbeidet er det nødvendig å vie oppmerksomhet til mulige negative konsekvensene av et endret klima.[8]

Det er ikke lenger ekstraordinære hendelser, men uønskede hendelser som ligger til grunn. Forklaringer på endringen i bruken av begrepet er flere, både organisatoriske og trusselmessige, men viser primært at begrepet er under endring, og at det lar seg påvirke av den politiske virkeligheten.

St.meld. nr. 37 (2004–2005) fra mai 2005 omtaler samfunnssikkerhet på følgende måte:

> Samfunnssikkerhet dreier seg om å ivareta sivilbefolkningens trygghet og sikre sentrale samfunnsfunksjoner og viktig infrastruktur mot angrep og annen skade i situasjoner der statens grunnleggende interesser ikke er truet. Samtidig har utviklingen medført et økt fokus på menneskelig sikkerhet der menneskerettighetene og ikke minst retten til liv og personlig trygghet står i sentrum.
>
> [...]
>
> Sentralt i dagens samfunnssikkerhetsarbeid er beskyttelse av sivilbefolkningen og vitale samfunnsinteresser i situasjoner hvor det ikke foreligger en tradisjonell militær trussel.
>
> [...]
>
> De sikkerhetspolitiske rammene, og da særlig utviklingen i internasjonal terrorisme, har fått økt betydning for samfunnssikkerheten. En rekke risikofaktorer, som faren for smittsomme sykdommer, naturhendelser og store ulykker har også fått økt betydning for sikkerhets- og beredskapsarbeidet nasjonalt.
>
> [...]
>
> Brannvesenet er en vesentlig ressurs på samfunnssikkerhetsområdet. Et velfungerende brannvesen er av grunnleggende betydning for

[6] Hovden, Jan 2004. Coping with Vulnerabilities and the Modern society. Det sikkerhetspolitiske bibliotek 5-2004. Den norske Atlanterhavskomité.

[7] St.meld. 17 (2001-2002). Samfunnssikkerhet. Veien til et mindre sårbar samfunn.

[8] St.meld. nr. 39 (2003–2004). Samfunnssikkerhet og siviltmilitært samarbeid.

samfunnets evne til å kunne håndtere også ekstraordinære hendelser. [9]

Her er det sikring av sentrale samfunnsfunksjoner og viktig infrastruktur som blir vektlagt. Også den nye sikkerhetspolitiske situasjonen blir trukket frem. Samtidig blir det vist til retten til liv og personlig trygghet. Omtalen av begrepet, slik det fremstår her, kan derfor hevdes å ha en tyngde mot å trygge samfunnet og ikke så mye individet. Både tilsiktede og utilsiktede hendelser er trukket frem.

1.1.3.4 Konsensus om begrepet

25. og 26. oktober 2004 ble det avhold et seminar arrangert i samarbeid mellom DSB, Norsk teknisk-naturvitenskapelige universitet (NTNU) og Universitetet i Stavanger (UiS), hvor begrepet samfunnssikkerhet ble drøftet. På bakgrunn av dette ble det utgitt et manus skrevet av Bjørn Ivar Kruke og Odd Einar Olsen ved UiS og Jan Hovden ved NTNU med forsøk på en begrepsfestning.[10] I den ble det slått fast følgende. For at en hendelse skal true samfunnssikkerheten, må den falle inn under én eller flere av følgende kriterier: (1) Ekstraordinære påkjenninger og tap, (2) kompleksitet og gjensidig avhengighet og (3) tillit til vitale samfunnsfunksjoner. Listen er ikke ment å være uttømmende, og det blir vist til at det alltid vil være gråsoner. Det blir videre hevdet at enhver uønsket hendelse i seg selv ikke er et anslag mot samfunnssikkerheten. Vanlige ulykker i trafikk, arbeid, hjem og fritid, samt vold og kriminelle handlinger, håndteres daglig på en rutinemessig måte i samfunnet. Forfatterne legger seg således opp til en snever definisjon av begrepet samfunnssikkerhet.

1.1.3.5 SAMRISK (Samfunnssikkerhet og risikoforskning)

Norges forskningsråd satte i 2005 ned en gruppe for å utrede behovet for et eget forskningsprogram innen samfunnssikkerhet og risikoforskning (SAMRISK). Deltagerne bestod av personer fra forvaltning og forskning.[11] Utredningsgruppen la følgende definisjon av samfunnssikkerhet til grunn:

> Vi anser at samfunnssikkerhet er relevant for risikohåndtering på alle nivåer i samfunnet, fra internasjonale og nasjonale reguleringer, ned til individets utøvelse av aktiviteter i arbeid, trafikk og fritid. [12]

Samtidig skriver de:

> I forhold til denne [Hovdens figur, figur ?] bør samfunnssikkerhet avgrenses til forhold som påvirker nasjonale institusjoner, normer som regulerer samhandlingen i samfunnet, og kritisk infrastruktur. De såkalte mikroverdier som individuell trygghet og sikkerhet bør inngå i begrepet dersom den involverer en stor samfunnsmessig kostnad og omfatter akuttpregede hendelser.

Gruppen inkluderer også Forsvarets støtte til det sivile samfunn i begrepet, men ekskluderer det som blir omtalt som udiskutable militære situasjoner. Utvalget hevder videre at det er oppstått ulike nyanser rundt begrepet, og at det delvis vil måtte være et eget tema for forskningen å forstå begrepet og gjøre det mer analytisk. SAMRISKs har dermed en bred tilnærming til begrepet.

---

[9] St.meld. nr. 37 (2004–2005). Flodbølgekatastrofen i Sør-Asia og sentral krisehåndtering.

[10] Kruke B.I, Olsen O.E og Hovden J (2005): «Samfunnssikkerhet – forsøk på en begrepsfesting» Rogalandsforskning RF-rapport 2005/035, ISBN: 82-490-0347-0

[11] Følgende ressurspersoner deltok i utredningsgruppen: Professor Jan Hovden, Norges teknisk- naturvitenskapelige universitet (NTNU), leder Professor Tore Bjørgo, Politihøgskolen (PHS), seniorforsker ved Norsk utenrikspolitiske institutt (NUPI) Seniorrådgiver May-Kristin Ensrud, Justis- og politidepartementet (JD) Forsker Janne Hagen, Forsvarets forskningsinstitutt (FFI) Rådgiver Lene Orsten Haugland, Forsvarsdepartementet (FD) Forskningssjef Kjell Haugset, Institutt for energiteknikk (IFE) Professorstipendiat Odd Einar Olsen, Universitetet i Stavanger (UiS) Rådgiver Lise Siverts, Arbeids- og sosialdepartementet (ASD) Avdelingsdirektør Helge Stamnes, Direktoratet for samfunnssikkerhet og beredskap (DSB) Utredningsgruppens sekretær var overingeniør Jan Tobiassen, Nasjonal sikkerhetsmyndighet (NSM). Halvdan Buflod og Tor-Petter Johnsen, Norges forskningsråd, deltok som observatører i utredningsgruppen sine møter.

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

Vedlegg 5

Sikkerhet - Safety/Security

En begrepsutredning
Finn-Erik Vinje

1 Bakgrunn

I utredningen *NOU 2000:24,* med tittelen «Et sårbart samfunn» (254 sider) , redegjør utvalget («Willoch-utvalget») for «samfunnets sårbarhet med sikte på å styrke samfunnets sikkerhet og beredskap» (s. 20). Utvalget har ifølge seg selv lagt til grunn «en bred tilnærming til arbeidet med å kartlegge og drøfte sikkerhets- og beredskapsutfordringer i samfunnet» (s. 22).

I et vedlegg til den nevnte utredningen, kalt «Sentrale begreper og definisjoner» (s. 226), er det foretatt en begrepsbestemmelse av de engelskspråklige betegnelsene *safety* og *security* og trukket opp grenselinjer – uten at det kan ses at utvalget i sin egen tekst selv har brukt disse betegnelsene, enn si holdt seg til den begrepsdistinksjon som er formulert i vedlegget.

I det omtalte vedlegget er *safety* definert slik: «Sikkerhet mot uønskede hendelser som opptrer som følge av en eller flere tilfeldigheter» – og *security* slik: «Sikkerhet mot uønskede hendelser som er resultat av overlegg og planlegging». Forskjellen mellom *safety* og *security* beror altså på om skaden er påført uten motiv (ikke villet) eller med motiv (villet).

Eksempler på *safety*-tiltak er verneutstyr av forskjellig slag. Typiske eksempler på *security*-tiltak er personkontroll, etterretningstiltak o.l. Imidlertid – som det påpekes i *Nasjonal sikkerhetsmyndighets risikovurdering 2004, ugradert versjon* (s. 4) – kan det være flytende overganger mellom *safety* og *security.* Man kan således iblant komme i tvil om en foreteelse skal henføres til den ene eller den andre kategori. *Nasjonal sikkerhetsmyndighets risikovurdering 2004* peker således på at slik tvil kan oppstå f.eks. ved hendelser som er resultat av kunnskapsmangel, slurv eller en generelt likegyldig holdning blant impliserte.

2 Fagspråk og allmennspråk

Jeg går ut fra at *NOU 2000:24* finner støtte i engelskspråklig litteratur om emnet for sin prinsipielle distinksjon – i vedlegget – mellom *safety* og *security.* Men det kan være på sin plass å påpeke at denne distinksjonen er basert på et fagspråklig behov. Stikkprøver i allmennspråklige engelske (engelskspråklige) ordbøker tyder på at betydningsforskjellen mellom *safety* og *security* ikke er så tydelig eller uttalt som man på norsk hold kanskje har hatt tilbøyelighet til å tro. Jeg dokumenterer ikke dette forholdet i noen bredde her, men nøyer meg med å sitere *Webster's Ninth New Collegiate Dictionary* (1987), der *security* har denne hoveddefinisjonen: «the quality or state of being secure». Nøkkelordet i definisjonen er *secure*, og slår man opp på dette ordet, får man det forklart bl.a. slik: «free from danger; free from risk of loss». På tilsvarende måte er *safety* definert under henvisning til adjektivet *safe,* idet *safety* bestemmes slik: «the condition of being safe from undergoing or causing hurt, injury, or loss».

Safety og *security* er adjektivabstrakter, de er avledet på normal måte av henholdsvis *safe* og *secure.* Men det er ikke slik at de to adjektivene i engelsk allmennspråklig praksis er begrepsmessig atskilt på den måten at *safe* opptrer med henblikk på ikke-villede hendelser, og at *secure* opptrer med henblikk på villede hendelser. Begge adjektivene refererer til en tilstand med tilstrekkelig vern mot uønskede hendelser – villede eller ikke-villede.

Lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven) handler om *sikkerhet* svarende til *security* i den ovenfor definerte (snevrere) forstand (dvs. tilsiktede uønskede hendelser/handlinger, f.eks. spionasje, sabotasje, terrorhandlinger). Loven gir selv ingen begrepsbestemmelse. Det heter imidlertid i § 1 at formålet med loven er «å legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvsten-

dighet og andre vitale sikkerhetsinteresser» – men også å «ivareta den enkeltes rettssikkerhet».

3 Et vilkårlig inngrep i vokabularet

Når man på engelsk – og tentativt på norsk – hold opererer med distinksjonen *safety/security* etter de linjer som er trukket opp ovenfor, da har man altså stipulert en begrepsdistinksjon, og – så vidt jeg forstår – funnet aksept for den i diskusjonen om de berørte aspekter av moderne samfunnsliv.

I den språklige tradisjon finner man ikke støtte for en slik distinksjon. Det betyr at man i allmennspråket hittil ikke har følt noe tvingende behov å distingvere i tråd med den ovenfor refererte forskjellen mellom *scurity* og *safety.*

Men dette faktum innskrenker ikke vår handlingsfrihet: Språket er et smidig system,og det er ingenting i veien for å forsøke å etablere en slik distinksjon. Da foretar man altså et vilkårlig inngrep i språkets vokabular og trekke nye grenser mellom leksikalske enheters virkefelt. En slik framgangsmåte er meget alminnelig i en fagspråklig kontekst. Terminologisk nydannelse skjer normalt på denne måten.

En *leksikalsk* definisjon, der man tar sikte på å beskrive den faktiske språkbruken, kan være sann eller falsk. En *stipulativ* definisjon derimot, som er å oppfatte som en forskrift eller regel for ordets bruk, kan være mer eller mindre hensiktsmessig eller adekvat, men den kan ikke plasseres inn på aksen sann – falsk.

Når man i det foreliggende tilfelle har sett behov for å distingvere etter modellen *safety/security*, gjelder det å finne fram til egnede leksikalske størrelser i vårt språk og bestemme deres betydningsomfang ut fra det behov som foreligger.

Ved siden av ordet *sikkerhet* står *trygghet.* De to ordene er synonymer, og de bærer begge betydningen 'det å være sikker/trygg' – uten hensyn til om de uønskede hendelser det henspilles på, er villede eller ikke villede. Man kan eksempelvis finne ordboksbelegg for *trygghet* i vid forstand: Man kan snakke om *trygghet* for stormvinder og flodbølger, men også om *trygghet* for fiendtlig anfall.

I *Nasjonal sikkerhetsmyndighets risikovurdering 2004, ugradert versjon* (s. 4) heter det innledningsvis under tittelen «Security/Safety»: «Norske ord kan ha dobbel betydning. I sikkerhetssammenheng kommer dette til syne ved at både »security« og »safety« kan oversettes med »sikkerhet« på norsk.»

Den siste perioden i foregående sitat («I sikkerhetssammenheng ... på norsk») er en korrekt beskrivelse av norsk språk. Bokstavelig tolket er også den andre perioden («Norske ord kan ha dobbel betydning») korrekt, men den er innholdstom, ja misvisende. Den formidler nemlig det inntrykk at norsk språk skulle stå i en særstilling ved at våre ord «kan ha dobbel betydning». Men norsk språk står ikke i noen særstilling. Alle levende språk har en overveldende mengde dobbelttydige ord – ikke minst engelsk.

4 Sikkerhet som overbegrep (hypernym)

Tilbake til *NOU 2000:24,* «Et sårbart samfunn». Som vi har sett av den begrepsbestemmelse som utvalget foretar (jf. ovenfor), forekommer ordet *sikkerhet* i de to definisjoner utvalget opererer med. *Sikkerhet* er behandlet som det overordnede begrep, og dette blir spesifisert i to retninger ved en attributiv bisetning – a) «som opptrer som følge av en eller flere tilfeldigheter» (*safety*); b) «som er resultat av overlegg og planlegging» (*security*). I lingvistisk sammenheng snakker man i slike tilfeller om *hypernymi;* ordet *sikkerhet* er et *hypernym.*

Utvalget opplyser selv at det har fått i oppdrag å drøfte «sikkerhets- og beredskapsutfordringer i samfunnet» (s. 22) og oppfatter altså *sikkerhet* som overbegrep. Iblant – ved behov – har Willoch-uytvalget spesifisert ordbruken, f.eks. når man på s. 115 i utredningen etablerer begrepet *matvaretrygghet* (ikke helt vellykket definert slik: «hvordan man kan sikre at en trygt kan spise den maten som er tilgjengelig») forskjellig fra *matvaresikkerhet* («som går på at det skal finnes tilstrekkelig med mat på markedet»). Derimot har man i et parallelt kapittel som handler om vannforsyning (s. 118 f.), ikke funnet det hensiktsmessig å etablere en tilsvarende terminologisk distinksjon når det gjelder vannkvalitet og «leveringssikkerhet». Når det dreier seg om hygienisk kvalitet på vannet, anvender man altså ikke begrepet «vanntrygghet» (jf. *matvaretrygghet* ovenfor), men holder seg også da til «sikkerhetsnivå» (s. 121).

Vi slår fast at *NOU 2000:24* i praksis oppfatter *sikkerhet* som overbegrep (hypernym). Del III i utredningen har således den overordnede tittelen «Sektorvise tiltak for økt samfunnssikkerhet», og et underkapittel bærer tittelen «Matvaretrygghet». Ordet *(matvare)trygghet* er et spesialtilfelle av – et underordnet aspekt av – *sikkerhet.* I lingvistisk sammenheng vil man betegne *(matvare)trygghet* som *hyponym* til ordet *sikkerhet* (jf. *hypernym* ovenfor).

5 Sikkerhet og sårbarhet

Sikkerhet danner en begrepsmessig motsetning – et *antonym* – til *sårbarhet,* som ifølge *NOU 2000:24* defineres slik: «Uttrykk for de problemer et system får 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» (s. 226). Om disse problemer er villede eller ikke-villede, er likegyldig for definisjonen av det begrep (*sårbarhet*) som det her dreier seg om. Jf. tittelen på utredningen: «Et sårbart samfunn».

Når *NOU 2000:24* bruker *sikkerhet* som et overordnet begrep (jf.ovenfor), er det i harmoni med etablert norsk allmennspråklig praksis. Ordboksdefinisjonen (*Norsk riksmålsordbok*) av *sikkerhet* er nemlig denne: «trygghet mot fare, angrep, uhell e.l.». Man snakker tradisjonsriktig f.eks. både om «rikets sikkerhet» og om at det gjelder å ta med paraply for *sikkerhets* skyld. Betegnelsen *sikkerhet* har enda bredere referanse: Eksempelvis kan et menneske vise *sikkerhet* i opptreden eller vesen, og penger kan bringes i *sikkerhet.* Osv.

Om ordet *sikkerhet* kan vi dermed konkludere at det er godt egnet som overordnet begrep også i vår sammenheng. Ved å akseptere den ordbruken holder man seg trygt innenfor tradisjonelt forankret språklig praksis. I sammensetninger får man da *sikkerhetstiltak* osv., og en adjektivisk parallelldannelse er *sikkerhetsmessig.*

Spørsmålet er så hvordan man skal innrette seg leksikalt for å spesialisere dette begrepet og betegne de forskjellige aspektene av *sikkerhet,* dvs. med hensyn til den refererte distinksjonen mellom *safety* og *security.*

6 Begrepsmessig differensiering

Før vi går videre, skal jeg si noe generelt om et levende språks ordforråd og språkbrukernes behov for og språkets evne til begrepsmessig differensiering.

Vårt språk har hittil ikke etablert noen leksikalsk distinksjon mellom a) en forsvarstilstand mot uønskede hendelser som er ikke-villede, og som opptrer som følge av tilfeldigheter (*safety*) og b) en forsvarstilstand mot uønskede hendelser som er villede, og som skyldes overlegg (*security*). Grunnen til dette er at denne distinksjonen tydeligvis ikke har imøtekommet noe behov, de norsktalende har ikke i sin språklige praksis følt det som noen nødvendighet å utvikle noe leksikalsk uttrykk for dette forholdet.

Men språket har en overflod av *synonymer* på dette som på andre felter, dvs. ord som betyr (nesten) det samme som et annet. Legg således merke til at *Norsk riksmålsordboks* definisjon av *sikkerhet* lød slik: «trygghet mot fare, angrep, uhell e.l.» (også sitert ovenfor). Ordet *trygghet* inngår altså som hovedord i selve definisjonen av sikkerhet og etablerer de to som synonymer. På tilsvarende måte kan man finne i norske synonymordbøker at *sikkerhet* og *trygghet* er synonymer, likesom adjektivene *sikker* og *trygg.* En *trygghetsalarm* skal etter hensikten inntre både overfor villede og ikke-villede uønskede hendelser.I nynorsk har man tradisjonelt hatt en puristisk motivert motvilje mot ord på *-het,* og *tryggleik* er således et offisielt synonym til *sikkerhet (*jf. Rommetveit: *På godt norsk* (1981)); FNs s*ikkerhetsråd* kalles for øvrig på offisiell nynorsk for *tryggingsrådet.*

Det er et aksiom i lingvistikken at enhver fasett i den menneskelige begrepsdannelse kan få språklig uttrykk, og det gjelder alle språk. Alle levende språk kan uttrykke alt – riktignok mer eller mindre elegant, mer eller mindre kortfattet. Det vil si: Når et behov for ny leksikalsk differensiering er sterkt nok, tilbyr språket muligheter. Iblant kan man ty til noen av språkets eksisterende ord og bestemme seg for å gi dem et nytt innhold og bruke dem på en måte som dekker vårt uttrykksbehov. Man finner da fram til partielle synonymer og *stipulerer* en betydning svarende til uttrykksbehovet, og kodifiserer den nye ordbruken i autoritative tekster (fagspråksordbøker, lærebøker o.a.).

På denne bakgrunn kan man eksempelvis slå fast at når *NOU 2000:24* som nevnt opererer med en betydningsmotsetning mellom *matvaresikkerhet* og *matvaretrygghet*, så baserer man seg på en såkalt *stipulativ definisjon*. Det innebærer at man for bestemte formål oppstiller vilkårlig visse definisjonskjennetegn for eksisterende leksikalske størrelser og bestemmer seg for å bruke – og overtale andre til å bruke – disse størrelser på den måte som definisjonen tilsier.

En annen mulighet er å utnytte mulighetene for å lage splitter nye ord (morfemer), men denne muligheten er meget begrenset. Språket har i virkeligheten en sterk uvilje mot å akseptere nye morfemer. Uavhengig av hvordan verden forandrer seg, og uavhengig av hvor mange nye, merkelige foreteelser som dukker opp i vår omverden og den virkligghet vi lever i, så anvender vi oss i regelen av de samme gamle morfemene – eventuelt i nye kombinasjoner – for å betegne disse nyheter. Bortsett fra innlån fra frememde språk er det således ytterst sjelden at nye morfemer oppstår. Muligens

kan visse forkortelser regnes hit, f.eks. når *bil* oppstår av *automobil.*

7 Trygghet og sikring

Vi ser så nærmere på den aktuelle formuleringsoppgaven som her foreligger. Oppgaven er å finne hensiktsmessige *hyponymer* til *sikkerhet,* ut fra det foreliggende behov. Jeg går altså ut fra at *sikkerhet* er etablert som *hypernym* (overordnet begrep) – på tross av at *lov om forebyggende sikkerhetstjeneste (sikkerhetsloven)* for sitt formål foretar en innsnevring av begrepet *sikkerhet* og lar det gjelde bare villede hendelser. Selv om loven ikke eksplisitt stipulerer en definisjon, framgår den av lovens § 1. Lovens innsnevring av begrepet *sikkerhet* betrakter vi som tekstintern.

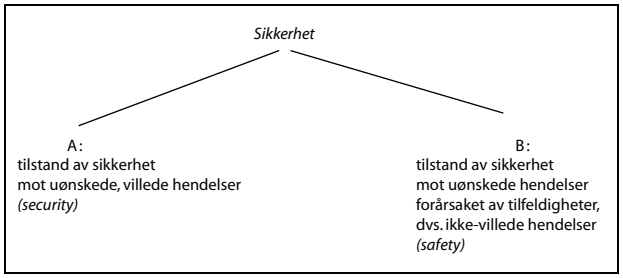
Vi søker altså hensiktsmessige leksikalske størrelser for de begreper som det refereres til under A og B i figur 5.1; vi kan kalle dem henholdsvis *sikkerhet A* og *sikkerhet B*.

Jeg gjentar at en leksikalsk differensiering i henhold til figuren nedenfor vil være en vilkårlig konstruksjon – i den forstand at den ikke er oppstått spontant i allmennspråket og neppe imøtekommer noe presserende behov der.

8 Et forslag

Den leksikalske differensiering vi her taler om (henholdsvis *sikkerhet A,* dvs. *safety* og *sikkerhet B,* dvs. *security*), springer ut av et faglig behov og er som sådan legitim, men man skal altså være klar over at man her *stipulerer* definisjoner til bruk i en bestemt sammenheng. Man kan neppe regne med at distinksjonen kommer til å bli allmennspråklig praksis – iallfall ikke i første omgang.

For øvrig har vi jo allerede konstatert at det kan finnes glidende overganger mellom A og B, slik at det kan være tilfeller der kategoriseringen er usikker.



Figur 5.1

Når man skal stipulere definisjoner og ha rimelige forventninger om at de skal bli akseptert, står man prinsipielt fritt til å fylle de leksikalske størrelser med et innhold som dekker uttrykksbehovet. Men språket er en treg materie, og i praksis må man nødt til å ta hensyn til den eksisterende ordbruken. Man kan altså ikke avvike mye fra den ordbruk som allerede er etablert.

Med dette som utgangspunkt vil jeg foreslå *trygghet* under A (*safety)*. Jeg foretar dermed en betydningsinnskrenkning av den allmennspråklige betegnelsen *trygghet,* idet jeg velger ut som definisjonskriterium ett av de betydningsaspekter som *trygghet* rommer i allmennspråket.

Trygghet volder ingen formelle problemer mht. orddannelse. Ordet inngår uten problemer i sammensetninger: *trygghetstiltak* osv. – og kan lett danne utgangspunkt for en adjektivavledning: *trygghetsmessig.*

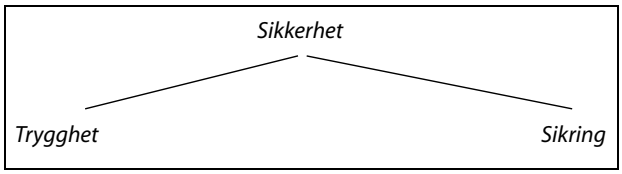
Noe vanskeligere er oppgaven når det gjelder B (*security*) ovenfor.

Det ville utvilsomt vært en fordel om man også under B kunne velge et adjektivabstrakt på *-het*, ettersom dette suffikset tydelig betegner en tilstand eller en egenskap. Men det er vanskelig å finne en slik *-het*-avledning.

Mitt forslag er at man tyr til *sikring,* som riktignok er en avledning av annen type (verbalsubstantiv), men som like fullt kan opptre med tilstandsbetydning i etablert språkbruk. Verbalsubstantiver på *-ing* er oftest verbalabstrakter, dvs. de betegner 'den virksomhet å + verbet'. Mer marginal er tilstandsbetydningen, dvs. betydningen 'det å være sikret', men også denne betydningen ligger altså innenfor avledningstypens muligheter.

Sikring er ordboksbelagt både som verbalabstrakt i betydningen 'det å sikre(s)', og som tilstandsbetegnende substantiv. Det første tilfelle foreligger i f.eks. «bygge festninger til sikring av grensene» og for øvrig også i selve utvalgsnavnet *Utvalg for sikring av landets kritiske infrastruktur.* Som tilstandsbetegnende adjektivavledning opptrer *sikring* i betydningen 'det å være sikret'. Slår man opp i *Norsk riksmålsordbok* på *sikkerhetstjeneste,* finner man at ordet er definert som 'sikringstjeneste'; ordet *sikring* gjøres her til synonym for *sikkerhet.*

Ordet *sikring* møter ingen formelle innvendinger mht. orddannelse. Det inngår uten problemer som sammensetningsledd: f.eks. *sikringstiltak.* Ordet kan dessuten danne utgangspunkt for adjektivavledningen *sikringsmessig.*



Figur 5.2

Ved å akseptere *sikring* som referanse til B har man etablert et betydningshierarki som får språklig uttrykk på følgende måte, se figur 5.2.

Så vidt jeg vet, opererer jeg her med en definisjon av ordparet *trygghet* og *sikring* som ikke finner støtte i litteraturen om emnet. Hver av de to betegnelsene er gitt en stipulativ definisjon, og det foreslås at det blir inngått en avtale om å bruke dem i henhold til definisjonen. Betydningen gir seg altså ikke selv ut fra en alminnelig kunnskap om språket og dets leksikalske enheter.

Slik sett står man overfor en ren skrivebordskonstruksjon. Definisjonene er på vilkårlig måte tilpasset vårt formål, men de er altså ikke uten forbindelse med eksisterende språkbruk. Det vi har gjort, er å er foreta en innsnevring av eksterende leksikalske enheters betydningsomfang.

Uansett – hvis eller når betegnelsene *trygghet* og *sikring* tas i bruk i betydningsdifferensierende hensikt, må man i tekster der disse termene anvendes, redegjøre for den betydning man for hver av de to betegnelsene legger til grunn.

Vedlegg 6

Risikobildet

Notat til infrastrukturutvalget

Rådgiver Bjørnar Davidsen, Seniorrådgiver Bjørn Nilsen,
Nasjonal sikkerhetsmyndighet, April 2005

1 Innledning

Nasjonal sikkerhetsmyndighet er bedt om å gi et innspill til Infrastrukturutvalget som sammenfatter risikobildet med bakgrunn i informasjon fra ulike kilder, herunder Politiets sikkerhetstjeneste og ulike forskningsmiljøer. Det presiseres at risikobildet er komplekst og at dette notatet derfor gir et innblikk i enkelte forhold ved risikobildet. Det er lagt spesiell vekt på å beskrive sårbarheter i forhold til spionasje, sabotasje og terrorhandlinger, hvor konsekvensen av anslag kan innebære en utfordring for vår nasjonale sikkerhet.

2 Generelt om risikobildet i vår tid

Det har i de senere årene vært gjennomført en rekke offentlige utredninger hvor det nye risikobildet Norge står overfor, har vært drøftet. Generelt kan det sies at utviklingen har gått fra en ganske entydig og klart dimensjonerende trussel til et variert og diffust *trusselbilde*. Tidligere var vern om landets suverenitet (territorielt og statsmessig) det sentrale sikkerhetsmessige fokus. Etter den kalde krigens epoke, har den tradisjonelle militære trussel mot Norge blitt sterkt redusert. I St.meld. nr. 17 (2001-2002) Samfunnssikkerhet står det:

> «Vi står overfor et mye bredere og mer diffust trusselbilde enn tidligere, kjennetegnet av glidende overganger mellom det nasjonale og det internasjonale, og mellom fred, krise, væpnet konflikt og krig. Norge kan i økende grad bli trukket inn i konflikter i den lavere del av krisespekteret, og vi kan bli trukket inn i konflikter på en indirekte måte. I sum er de potensielle truslene som vi står overfor som en del av en mer global verden ikke blitt borte – de er flere og mer uoversiktlige.»

Perioden med bortfall av den kalde krigen faller tidsmessig sammen med en annen viktig utvikling, nemlig inngangen til informasjonssamfunnet og globaliseringen som dette fører med seg. Vi har i løpet av de siste to tiårene sett en eksplosiv utvikling innen informasjons- og kommunikasjonsteknologi (IKT). Nye *sårbarhetsområder* har dermed blitt introdusert, selv om teknologien også gir bedre muligheter for å forebygge uønskede hendelser. Ved siden av at denne teknologien etter hvert tas i bruk på stadig flere områder i samfunnet, har fremveksten av et Internett på verdensbasis skapt en helt ny epoke.

Et sentralt kjennetegn ved denne samfunnsutviklingen, er at stabile og fungerende IKT-systemer i stadig økende grad er en forutsetning for at samfunnsmaskineriet skal virke. Det er også slik at måten teknologien tas i bruk på gjør at det er stadig flere tannhjul som griper i hverandre, selv på tvers av sektorer. Samfunnets infrastruktur på nær sagt alle områder drives på en eller annen måte av IKT-systemer.

Det nye trusselbildet har mange fasetter; noen av dem er knyttet nettopp til infrastrukturens avhengighet av IKT. IKT representerer en helt spesiell *verdi* for samfunnet. At samfunnet er blitt så avhengig av fungerende IKT-systemer, gjør at trusler mot disse får en helt ny dimensjon. For 15 år siden ville feil eller sammenbrudd i en datamaskin kun føre til meget begrenset skade. I dag kan en tilsvarende hendelse gi omfattende og kanskje katastrofale virkninger.

Utviklingen har gått så raskt at vi kanskje ikke kan sies å ha full kontroll over situasjonen. Hvor sårbare er vi egentlig? Hvilke trusler vil være dimensjonerende for valg av sikringstiltak? Hvilke er de viktigste truslene i dag, i morgen?

Det kan observeres noen trender som kanskje kan si noe om hva oppmerksomheten bør rettes in mot:

– Det er flere angrep som er koordinerte med økonomiske, politiske eller samfunnskritiske mål

- Server-, klient- og applikasjonsparken i Norge blir mer og mer homogen
- Norske virksomheter er raske til å ta i bruk ny teknologi
- Norge har høy utbredelse av bredbånd
- Teknologi blir brukt på nye måter for å bli hørt; demonstrasjoner, utpressing
- Nye sammenstillinger av angrepstyper blir brukt av organiserte kriminell miljøer – ikke alltid veldig sofistikerte, men enklere angrep
- Det er en nedgang i helgene med antall automatiske angrep mot mål
- Derimot en økning i antall angrep i helgene mot hjemmebrukere, hvor sosial manipulasjon er fremtredende

Organiserte kriminelle bruker kombinasjoner av spam[1], sosial manipulering, id-tyveri, phishing[2] etc. for å kunne angripe for eksempel nettbanker.

De mer langsiktige trendene kjennetegnes ved en angrepsvektor med elementer av nektelsesangrep, koordinert med økonomiske eller politiske mål. En annen langsiktig trend er at norske, samfunnskritiske kontrollsystemer blir koblet opp mot Internett.[3] Det er også en økende motivasjon for økonomisk vinning ved såkalte zero-day-attacks.[4]

Politisk motiverte nektelsesangrep har man sett mye av i enkelte deler av verden (eksempel i Midt-Østen). Denne angrepstypen er vanskelig å spore. Det finnes heller ikke noe internasjonalt lovverk som retter seg mot dette.

Til nå har vi ikke sett at elektroniske informasjonssystemer har vært utsatt for angrep, verken av fysisk eller elektronisk karakter, som med rimelighet kan betegnes som terrorisme. Ikke desto mindre gjør infrastrukturens avhengighet av IKT-systemene disse til et potensielt mål, ikke bare for terroristorganisasjoner. Muligheten til å være proaktiv i forhold til å vurdere truslene, avdekke sårbarhetene og forberede tiltak som kan redusere konsekvensene ved et angrep mot infrastrukturen, må utnyttes.

3 Risikobegrepet

En vanlig forståelse av risikobegrepet er at det utledes av to komponenter; sannsynligheten for at en uønsket hendelse skal skje og hvilke konsekvenser dette kan medføre.

Den tradisjonelle definisjonen av risikobegrepet som et produkt av sannsynlighet for en uønsket hendelse og konsekvensen denne hendelsen gir, blir likevel ikke et hensiktsmessig utgangspunkt når det gjelder for eksempel trusselen som utgjøres av terrorgrupper.

Det kan i stedet være nødvendig å anvende en metode som gir et grunnlag for å si noe om hvilken *mulighet* det er for at en slik trussel skal føre til utløsning av en uønsket hendelse gjennom utnyttelse av sårbarheter.

Det er avdekking av sårbarheter og tiltak for å redusere denne, som kan redusere mulighetene for et vellykket anslag. En kan gå ut fra at for eksempel et informasjonssystem som ikke har god nok beskyttelse i form av brannmurer, vil være mer sårbart overfor angrep og at muligheten for at dette informasjonssystemet rammes dermed vil være større.

Konsekvensene av ondsinnede handlinger kan være så store at de truer rikets sikkerhet og vitale nasjonale interesser. Stortinget vedtok i 1998 Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), som skal sikre at en grunnsikring til enhver tid er på plass for informasjon og objekter av spesiell **verdi** for samfunnet, gjennom blant annet å stille krav til defensive sikkerhetstiltak.

Det er ikke mulig å forutsi med særlig grad av sikkerhet hvor trusselaktører vil angripe. De defensive sikkerhetstiltakene har derfor som utgangspunkt at den samfunnsmessige verdien identifiseres og danner utgangspunkt for tiltakene, slik at tiltak skal være på plass alle steder hvor det finnes en mulighet for anslag som kan medføre betydelige, samfunnsmessige konsekvenser.

Konsekvensvurderingen er styrende ved fastsetting av sikkerhetsmessig verdi på informasjon og objekter. Dess større konsekvens det får dersom informasjon blir kjent for uvedkommende eller et objekt ødelegges for eksempel av terrorister eller

---

1 Uønsket, elektronisk post som sendes ut i store mengder.

2 Forsøk fra tredjepart på å lure et individ, en gruppe, eller en organisasjon til å gi fra seg sensitiv informasjon. Motivet bak phishing er i de fleste tilfeller økonomisk. Begrepet er phishing er ikke nytt. Det ble første gang nevnt på Internett i nyhetsgruppen alt.2600 i januar 1996 og ble da brukt for å omtale handlinger utført av enkelte angripere som stjal America Online (AOL) brukerkonti. En typisk angrepsmetode benyttet i forbindelse med phishing, er bruk av forfalskede e-post meldinger hvor avsenderen utgir seg for å være en pålitelig kilde, eksempelvis en bank eller et kredittkortselskap. E-posten inneholder gjerne en link til et nettsted, hvor brukeren registrerer sine sensitive data. Nettstedet kan i utgangspunktet se helt legitimt ut, men alt er i realiteten en forfalskning designet for å få tak i sensitiv informasjon.

3 Konfidensialitet kan ivaretas ved eksempelvis bruk av Virtual Private Network (VPN), som gir kryptert forbindelse på Internett. Problemet kan imidlertid bli manglende tilgjengelighet. Dersom en Internet Service Provider (ISP) får problemer med sin leveranse av Internett, kan det ta tid å få rettet opp feilen. Dette kan, i de tilfeller hvor kritiske systemer er koblet opp mot Internett, få alvorlige konsekvenser.

4 En sårbarhet som blir utnyttet, eksempelvis av hackergrupperinger, før den blir rapportert inn til sikkerhetsmiljøet.

sabotører, dess større sikkerhetsmessig verdi har objektet eller informasjonen. Det er avgjørende for samfunnssikkerheten at virksomheter er i stand til å foreta en vurdering av hva som har sikkerhetsmessig verdi slik at objekter og informasjon som virkelig har *samfunnsmessig betydning,* blir beskyttet. Det er ikke mulig å beskytte absolutt alt, derfor må en gjøre et utvalg. Nasjonal sikkerhetsmyndighet vil kunne bistå i en verdivurdering. Det er imidlertid virksomhetene selv som må foreta den innledende verdivurderingen. Nærhet til og erfaring fra oppgaveløsningen innenfor egen sektor eller egen virksomhet, gir et godt grunnlag for å kunne foreta en verdivurdering.

Bak de tilsiktede, ondsinnede handlingene står en **trusselaktør**. Trusselaktører kan være alt fra misfornøyde ansatte i en bedrift til pressgrupper, organiserte kriminelle, terroristorganisasjoner eller andre stater. Muligheten for at spionasje, sabotasje eller en terrorhandling faktisk vil finne sted har blant annet sammenheng med egenskaper hos trusselaktøren. Sentrale vurderingstema i denne forbindelse vil være aktørens *intensjon* og *kapasitet*.

Intensjonen, altså ønsket om og viljen til for eksempel å utføre en terroraksjon, er i første rekke styrt av motivasjonen. Motivasjonen vil også påvirke forhold som besluttsomhet, grad av voldsanvendelse og vilje til å overse risiko ved gjennomføring av aksjoner.

Eksempel på motiverende faktorer hos forskjellige trusselaktører kan være:
- politiske
- ideologiske
- kriminelle
- religiøse
- hevn
- økonomiske
- etterretning

Ulike katalysatorer kan påvirke valg av både mål og tidspunkt for et angrep. Katalysatorer kan være av forskjellig karakter:

Hendelser: Kan være relatert direkte eller indirekte til angriperen, for eksempel en personlig opplevelse eller tilgang til et nyhetsinnslag som fører til at en forhåndsplanlagt aksjon settes i verk. Det kan også være endringer i politiske forhold mellom land eller andre konflikter, som får stor oppmerksomhet.

Teknologiendringer: Viktige teknologiendringer skjer stadig. Nye anvendelsesområder synliggjøres, og det kan også gi nye sårbarheter som kan utnyttes. Dette kan i seg selv være en katalysator for å utløse angrep.

Personlige forhold: Endringer av personlig karakter hos en (potensiell) trusselaktør kan utløse og gi motivasjon for å utføre en ondsinnet handling. Ikke minst i forhold til innsidetrusselen, er dette en type katalysator som det må tas hensyn til.

Kapasitetsbegrepet beskriver ulike sider ved en trusselaktør, som vil ha betydning for å vurdere hvilken evne denne har til å gjennomføre et anslag av forskjellig styrke og karakter. Teknologisk kunnskap, økonomisk støtte, tilgang på våpen/annet utstyr og nivå på organiseringen er eksempler på elementer som inngår i kapasitetsbegrepet. I vurderinger av kapasitet vil det måtte legges forskjellig vekt på de ulike aspektene, etter hvilken type trusselaktør det er snakk om.

En trusselaktør vil kunne benytte seg av alle tilgjengelige nivåer i sine angrep, inkludert enkle metoder dersom dette kan gi den ønskede effekt. Men det kan også være aktuelt med høynivå/høykapasitets metoder over en lengre periode, for å få en tilsiktet effekt.

Det er grunn til å understreke at ønsket om å skade ser ut til å ligge på et permanent, høyt nivå hos enkelte trusselaktører i dag. Kapasiteten synes imidlertid å være utilstrekkelig på enkelte områder.[5] Tilgang til informasjon om et samfunns sårbare punkter kan være med på å øke kapasiteten hos ondsinnede aktører i forhold til å gjennomføre anslag. I spesielle tilfeller kan en heller ikke se bort fra at ervervelse av sårbarhetsinformasjon faktisk kan bli en utløsende faktor slik at anslag gjennomføres som, uten tilgang på sårbarhetsinformasjon, ellers ikke ville ha blitt gjennomført.

4 Risikobildet

Faktorene *verdi (hva må beskyttes), sikkerhetstrussel og sårbarhet* utgjør til sammen risikobildet. Kjennskap til alle faktorene i risikobildet er en forutsetning for å være i stand til å innrette defensive, forebyggende sikkerhetstiltak på en hensiktsmessig måte.

4.1 Hva må beskyttes?

Tidligere har *territoriell integritet* vært hovedinnholdet i begrepet *rikets sikkerhet.* Dette er endret nå, blant annet med bakgrunn i det endrede trusselbildet. Fra en situasjon hvor rikets sikkerhet i

[5] Fremstilling og spredning av biologiske våpen synes for eksempel å være såpass komplisert at terrorgrupperinger så langt ikke har lyktes med dette i særlig grad, selv om intensjonene synes å være til stede.

første rekke var truet av muligheten for en invasjon fra en annen stat, er vårt (og andre) lands sikkerhet i dag utsatt for det som beskrives som en asymmetrisk trussel. Dette innebærer at trusselen kan komme fra ikke-statlige aktører, og den vil kunne medføre bruk av ikke-konvensjonelle midler (inkludert masseødeleggelsesmidler). Fremfor alt vil trusselen også kunne komme gjennom elektroniske nettverk (Internett), og den kan utløses fra hvor som helst i verden. «Spilleregler» ved staters krigføring mot hverandre, som Genevekonvensjonen, overses av de asymmetriske aktørene. Dette gir disse aktørene en mulighet til å øve innflytelse på politisk nivå i stater, blant annet ved å ramme helt vilkårlige personer.[6]

Vitale nasjonale sikkerhetsinteresser omfatter kritisk infrastruktur innenfor vitale samfunnsfunksjoner som energi- og matforsyning, samferdsel, telekommunikasjon, helseberedskap samt bank- og pengevesen. Opplistingen er ikke uttømmende.

Et sentralt spørsmål når det gjelder å vurdere om egen informasjon er skjermingsverdig i henhold til sikkerhetsloven, må være om informasjonen i *vesentlig* grad kan misbrukes slik at virksomheten selv eller andre virksomheter rammes. Et annet spørsmål vil være om *sammenstillingen* av ugradert informasjon kan utgjøre en så verdifull kunnskapsbase for mulige ondsinnede aktører, at den helhetlige informasjonen vil kunne være skjermingsverdig i henhold til sikkerhetsloven.

Det utgjør en stor utfordring for virksomheter å kunne foreta en vurdering av hvilken samfunnsmessig verdi eksempelvis et informasjonssystem vil kunne få når en ser på den totale informasjonsstrømmen som systemet skal håndtere. En konsekvensanalyse må stå sentralt i en slik vurdering. Hva skjer dersom systemet ikke fungerer? Kan dette ha betydning for rikets sikkerhet eller andre vitale nasjonale sikkerhetsinteresser?

Ulike forhold kan påvirke verdivurderingen. Globalisering og økt avhengighet mellom land og regioner fører til at landegrenser ikke spiller den samme rollen i dag som tidligere i form av sikkerhetsbarrierer. Geografisk avstand har fått redusert betydning blant annet som en konsekvens av grenseoverskridende teknologi. Et eksempel på dette er den ustrakte avhengigheten av Internett, hvor landegrenser ikke eksisterer. Et annet eksempel er samfunnets økende avhengighet av navigasjonssystemer som Global Positioning System (GPS).

Norge er et lite land og må derfor bygge og vedlikeholde allianser for å bevare egen sikkerhet. Alliansebygging kan innebære utfordrende avveininger mellom informasjonsdeling eller skjerming av informasjon overfor motparten.

Prinsippet om skjerming av informasjon for å gjøre spionasje og terror så vanskelig som mulig kan bryte med et annet viktig prinsipp for å bekjempe spesielt terrorhandlinger, nemlig informasjonsdeling fra offentlige myndigheter og ut til befolkningen. Det er antagelig slik at «mannen i gata» gjennom sin årvåkenhet og evne til rapportering av mistenkelige personer/gjenstander/hendelser og lignende, stadig vil bli viktigere for å bekjempe terrorhandlinger i fremtiden. Dette innebærer at offentligheten har et informasjonsbehov. Det kan være grunn til å spørre om ikke «det informerte samfunn» også vil være «det mest motstandsdyktige samfunn» i forhold til terrorhandlinger. Men balansegangen kan være hårfin. Det kan tenkes at visse typer informasjon som, dersom den blir kjent for offentligheten, vil kunne skape unødig redsel. Det kan også være tilfeller hvor informasjon må sikkerhetsgraderes høyt av hensyn til samarbeidende tjenester, slik at en ikke opplever «informasjonstørke» dersom disse tjenestene mener at opplysningene ikke beskyttes tilstrekkelig fra norsk side.

4.2 Sikkerhetstrusselen

Spionasjetrusselen[7] eksisterer fremdeles i form av tradisjonell, statsinitiert spionasje.[8] Spionasjen retter seg både mot økonomiske og teknologiske mål, så vel som mot mer tradisjonelle mål som beredskapsplaner, krisehåndteringsevne, forsvarshemmeligheter og sikkerhetspolitiske standpunkter. Skadevirkninger av spionasje som rettes mot økonomiske og teknologiske **mål** vil blant annet være svekket konkurranseevne og mulig tap av arbeidsplasser. Skadevirkninger av spionasje rettet mot for eksempel sikkerhetspolitiske standpunkter og forsvarshemmeligheter, kan være en svekkelse av norsk strategisk evne til å møte endringer i risikobildet. Samfunnssikkerheten i Norge kan også trues dersom detaljert informasjon om beredskapsplaner kommer på avveie.

Sikkerhetsgradert informasjon vil alltid være av spesiell interesse for fremmed etterretning,

[6] Et kjent eksempel kan være Filippinenes tilbaketrekning av sine styrker i Irak etter en kidnapping av filippinske statsborgere, som ikke hadde noe med styrkene å gjøre.

[7] Sikkerhetsloven § 3 nr. 3: «Spionasje; innsamling av informasjon ved hjelp av fordekte midler i etterretningsmessig hensikt.»

[8] Politiets sikkerhetstjeneste peker på at flere stater utfører etterretningsvirksomhet med fordekte midler i og mot Norge. (PSTs ugraderte trusselvurdering 2005).

fordi informasjonen skal være vurdert som spesielt verdifull, av informasjonsutstederen. Åpent tilgjengelig informasjon, for eksempel i form av stortingsmeldinger og artikler i media, utgjør likevel en svært viktig del av etterretningsbildet. En sammenstilling av ugradert informasjon vil, som tidligere nevnt, på et tidspunkt kunne få så stor verdi som kunnskapsbase for fremmed etterretning, at den totale informasjonsmengden bør sikkerhetsgraderes.

Terrorgrupperinger er også nødt til å samle inn informasjon om mulige mål i forkant av aksjoner. Detaljert informasjon om eksempelvis bygningers tåleevne, vaktrutiner og kontrollsentralers plassering, vil lette gjennomføringen av en aksjon og øke skadepotensialet.

Eksempler viser at fremmed etterretning ofte arbeider gammeldags, med verving som en mye brukt **metode**.[9] Følgende eksempel viser at spionasjetrusselen fremdeles er reell: Norge utviste i januar 2004 en ambassadesekretær ved den russiske ambassade, som var mistenkt for å utføre aktiviteter som ikke var forenlig med vedkommendes diplomatiske status.[10]

På generell basis kan det sies at det finnes et mangfold av metoder for å utføre spionasje. Ny teknologi gir blant annet nye muligheter for spionasje. Samtidig gir også teknologi nye muligheter for forebygging.

Informasjon om planlagte og utførte *terrorhandlinger*[11] i Europa kan si noe om utviklingstrekk i forhold til mål og metode.

Spania ble rammet av en terroraksjon 11. mars 2004. Det har også blitt avverget flere planlagte terroraksjoner i Europa siden år 2000. Det er gjennomgående radikale, islamistiske grupperinger som står bak planene. **Målutvelgelsen** er variert og omfatter symbolske, militære, statlige og private mål. Når det gjelder **metoder**, så dominerer fremdeles eksplosiver, blant annet i form av sprengstoffet C4. Sprengstoff i form av ammoniumnitrat, altså kunstgjødsel, som er blandet med for eksempel diesel, synes også å være en aktuell metode. Metoden har blitt benyttet tidligere. Den såkalte Oklahomabomben var laget av gjødsel og drivstoff.

Enkelte av aksjonsplanene tyder på en sterk interesse hos terrorgrupperinger for å utvikle giftstoffer. Beslaglagt datautstyr tyder også på en interesse for å bedre evnen til å utføre angrep mot elektroniske informasjonssystemer. I dag ligger det verktøy for å utføre angrep lett tilgjengelig på Internett. Det kreves ikke spesielle datakunnskaper for å nyttiggjøre seg denne typen verktøy.

4.2.1 Nærmere om al-Qaida[12]

Begrepet al-Qaida begynte å florere i mediene etter bombingene av USAs ambassader i Kenya og Tanzania i 1998. Begrepet ble brukt som en betegnelse på nettverket til Usama bin Ladin, som erklærte jihad mot USA for første gang i 1996.

Internasjonale forskningsmiljøer har ikke noe fullgodt svar på hva *al-Qaida* er. Studier av ulike dimensjoner ved al-Qaida kan bidra til å klargjøre bildet noe.

En viktig dimensjon er diskusjonen om al-Qaida er en *organisasjon* eller en *bevegelse*. Kilder indikerer at det, tidlig på 90-tallet, fantes ambisjoner om å lage en strukturert organisasjon. Etter 2001 har al-Qaida imidlertid beveget seg mer i retning av å være en bevegelse eller en ide som utøver handlinger gjennom lokale islamistgrupper med ulik grad av tilknytning til «den harde kjernen» av al-Qaida (Usama bin Ladin og hans nære medarbeidere). Sikkerhetmessige konsekvenser av denne utviklingen er blant annet at det som i dag best kan betegnes som et nettverk vil være vanskeligere å bekjempe, fordi limet i nettverket er en felles ideologi som i mindre grad enn før er personavhengig. Det er derfor grunn til å anta at ideologien kan komme til å leve videre, til tross for at enkeltpersoner blir nøytralisert.

En annen viktig dimensjon i studiet av al-Qaida handler om å se på utviklingen hos de lokale islamistgruppene som tidligere har vært mest opptatt av lokale konflikter. Nå kan det i økende grad se ut til at disse grupperingene bifaller ideologien om global jihad.

En tredje dimensjon ved studiet av al-Qaida er den sosiale profilen til medlemmer av al-Qaida og sympatisører. Yngre, muslimske menn med felles bakgrunn fra kamper mot sovjetiske styrker i Afghanistan, grunnla al-Qaida. Lederskapet henvender seg i dag til et yngre, hovedsakelig mannlig publikum. Også her skjer det imidlertid en utvikling, blant annet ved at al-Qaida i løpet av 2003 hen-

---

[9] Politiets sikkerhetstjeneste forventer at utenlandske etterretningstjenester også i 2005 vil forsøke å verve nordmenn med tilgang til sensitiv og skjermingsverdig informasjon. (PSTs ugraderte trusselvurdering 2005).

[10] Aftenposten, 21.8.04.

[11] Sikkerhetsloven § 3 nr. 5: «Terrorhandlinger; ulovlig bruk av, eller trussel om bruk av, makt eller vold mot personer eller eiendom, i et forsøk på å legge press på landets myndigheter eller befolkning eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål.»

[12] Blant annet basert på et notat fra FFI: «Transnasjonale terrororganisasjoners bruk av medier og massekommunikasjon: Case al-Qaida», notat på oppdrag fra Nasjonal sikkerhetsmyndighet (NSM) september 2004.

vendte seg direkte til kvinner. Kanskje kan en mer pragmatisk holdning til ideologi ligge bak en slik utvikling, selv om henvendelsene i første rekke handler om at kvinner skal støtte sine ektemenn i jihadarbeidet, ikke utføre selvstendige aksjoner.[13]

4.2.2 Al-Qaida og Internett

Internett blir benyttet på flere måter. Spredning av informasjon er viktig og dette kan skje enkelt og effektivt på Internett. Samtidig er det også naturlig å samle inn informasjon fra Internett. Oppdatert kunnskap om våpen, ny teknologi og fiendens svakheter og styrker vil alltid ha stor nytteverdi i forbindelse med aksjoner.

På en internettside drevet av «al-Qaida på den arabiske halvøy», ble leserne bedt om å fremskaffe informasjon om «økonomiske og militære mål tilhørende de amerikanske vantro korsfarerne (i Saudi Arabia)». Følgende mål ble nevnt som attraktive:

- Kontorer og rørledninger tilhørende amerikanske oljeselskaper
- Amerikanske ammunisjonslager
- Boligområder og rekreasjonssenter for amerikansk personell
- Luftkorridorer
- Oppstillingsplasser for tanking av amerikanske fly
- Havner brukt av amerikanske militære og kommersielle skip.

Avsenderen foreslo å legge ved bilder og kart for å gjøre det enklere for de som følte seg kallet til å gjennomføre et angrep. Leserne ble også bedt om å legge ut navn og adresser på høyerestående militært personell og etterretningstjenestemenn.

Det antas at al-Qaida har intensjoner om å gjennomføre angrep mot samfunnskritiske objekter via Internett. Fremdeles vet man imidlertid lite om hvor alvorlig cybertrusselen fra al-Qaida og allierte grupperinger egentlig er. Amerikanske myndigheter mener å ha sterke indikasjoner på at al-Qaida nettverket har gjort forberedelser for fremtidige cyberangrep, fortrinnsvis rettet mot elektrisitetsforsyningen, telefonnettet, damanlegg og atomkraftverk samt kontrollsystemer for lufttrafikken. Også britiske myndigheter mener at de ødeleggende konsekvensene av vellykkede cyberangrep er vel kjent i hackermiljøene.[14]

Det er imidlertid uklart hvilken kapasitet al-Qaida har i dag, til å gjennomføre angrep. Spørsmålet er kanskje heller om sympatisører av al-Qaida, som bifaller ideologien til nettverket, utgjør den største trusselen foreløpig. Flere islamistiske websider spesialiserer seg på «elektronisk jihad». Under den palestinske al-Aqsa-intifadaen har det vært en rekke kampanjer med cyberangrep, både av pro-israelske og pro-palestinske hackere, rettet mot motpartens websider. Pro-palestinske hackere har lyktes med å lukke eller skade nettsidene til en rekke israelske statsinstitusjoner, som det israelske parlamentet, hæren og utenriksdepartementet.

En rekke meget destruktive og ødeleggende virusprogrammer er også spredt gjennom Internett de siste årene. Noen av disse er trolig produsert av hackere med tydelige al-Qaida sympatier.[15]

4.3 Sårbarhet

Den siste komponenten i risikobildet er sårbarhet. Sårbarhet er svakheter som reduserer eller begrenser evnen i et system eller i samfunnet til å motstå uønskede, negative hendelser. Under sikkerhetsloven manifesterer hendelsene seg i første rekke som spionasje, sabotasje eller terror.[16]

4.3.1 Internett

Internett er tidligere nevnt som et område av stor verdi for samfunnet. Stadig flere tjenester i samfunnet, både offentlige og private, baserer seg på bruk av Internett. Internett er et system som i utgangspunktet var designet nettopp for å være robust og redundant, slik at mulighetene for å utføre sabotasje mot Internett skulle være små. Enkeltpunkter i Internettsystemet kan imidlertid være sårbare, både overfor logiske angrep i form av for eksempel tjenestenekt, og overfor konvensjonelle angrep i form av eksplosiver. Det er ikke utenkelig at kapasiteten på Internett vil bli betydelig dårligere dersom nøkkelpunkt skulle falle ut for eksempel som

[13] Tsjetsjenske kvinner, de såkalte «sorte enkene», har gjennomført flere aksjoner mot russiske interesser. Årsakene til disse kvinnenes handlinger er sammensatt, men det ser ikke ut til at al-Qaida foreløpig har hatt spesiell innflytelse på handlingsmønsteret. Andre forhold, som kvinnenes tap av ektemenn/slektninger i russiske krigshandlinger i Tsjetsjenia, kan være en motivasjonsfaktor. Radikale islamister skal også ha forsøkt å rekruttere særlig kvinner i Tsjetsjenia for å gjennomføre terrorhandlinger, idet islamistene mener at kvinner kanskje ikke avsløres så lett.

[14] Stephen Cummings, direktør for National Infrastructure Security Coordination Centre.

[15] Dan Verton i Computerworld 20 november 2002.

[16] Teknisk og menneskelig svikt samt naturskade kan også lede til sikkerhetsbrudd og kompromitteringer. Dette viser blant annet at sammenhengen mellom tilsiktede og utilsiktede hendelser kan være sterk i forhold til forebyggende sikkerhetstjeneste, fordi konsekvenser av hendelsene kan være de samme.

en følge av sabotasje, eller av andre, kanskje mer naturlige årsaker, som utstyrsfeil.

Det synes i dag som om forskningsmiljøene mangler kunnskap i forhold til konsekvenser ved bortfall av nøkkelpunkt i Internett. Det synes imidlertid klart at dersom sårbare punkter rammes så hyppig at angrepstakten overstiger systemets reparasjonstid, kan skaden gjøres mer eller mindre permanent.[17] En konsekvens av hyppige tjenestenektsangrep kan være sterkt redusert kapasitet i Internett, som igjen blant annet kan føre til at tjenester som nettbank ikke lenger vil være tilgjengelig.

Varslingssystem for digital infrastruktur (VDI) registrerer stadig kartleggingsforsøk via Internett, rettet mot de deler av kritisk infrastruktur som er tilknyttet VDI. Kartleggingsforsøk kan etterfølges av mer målrettede angrep. VDI vil, i tilfelle forsøk på koordinerte angrep skulle bli oppdaget, *varsle* berørte virksomheter raskt slik at disse kan treffe tiltak. Norge behøver imidlertid også en enhet som kan koordinere *respons* på alvorlige IT-sikkerhetsangrep på nasjonalt nivå, når angrepet er rettet mot kritisk infrastruktur.

4.3.2 Mulig effekt av nettverksterrorisme

Det har hittil ikke vært påvist noe koordinert eller vidtrekkende nettverksangrep som har ødelagt kritisk infrastruktur noe sted. Likevel kan det ikke avvises at det økende antall av tilsynelatende tilfeldige nettverksangrep i noen tilfeller er initiert av terrorgrupper. Det finnes undersøkelser[18] som viser at i siste halvdel av 2002 var virksomheter innen kritisk infrastruktur på topp av listen over mål for nettverksangrep. En annen rapport, utarbeidet av British Columbia Institute of Technology og PA Consulting Group tok utgangspunkt i data helt fra 1981. Rapporten påviser en ti-dobling i økningen av nettverksangrep mot infrastruktur og SCADA-systemer[19] etter år 2000. USAs forsvarsdepartement har også påvist en sterk økning i forsøk på inntrening i militære IKT-systemer.

Det er ulike synspunkter på i hvilken effekt nettverksangrep vil ha på kritisk infrastruktur. Noen mener at koordinerte nettverksangrep kan bli benyttet for å forsterke effekten av konvensjonelle angrep. Andre er mer usikre på hvor ødeleggende effekten vil kunne bli av direkte angrep på kritisk infrastruktur. Mens enkelte mener at virkningene kan slå alvorlig ut i økonomien, mener andre at de forskjellige systemene allerede er svært robuste og at gjenoppretting etter et angrep vil kunne gå relativt raskt slik at katastrofale effekter unngås.

I juli 2002 ble det gjennomført et krigsspill i regi av US Naval War College under tittelen «Digital Pearl Harbour». Scenariet var et koordinert nettverksangrep gjennomført av terrorister mot kritisk infrastruktur. Resultatet av det simulerte angrepet viste at den mest sårbare infrastrukturen var Internett selv, i tillegg til IKT-systemer innen den finansielle infrastrukturen. Spillet viste også at forsøkene på å ødelegge telekommunikasjonsnettet i USA ble mislykket på grunn av stor redundans i nettet. Hovedkonklusjonen den gang (i 2002) var at et «digitalt Pearl Harbour» for USA var mindre sannsynlig.

Som nevnt utpekte selve Internett seg som det mest sårbare i denne sammenheng. Det ble oppdaget en alvorlig svakhet i SNMP-protokollen[20] som kunne ha gitt angripere mulighet til å ramme Internett katastrofalt over hele verden. Informasjonen om denne svakheten ble holdt tilbake så lenge at alle leverandører kunne rette programvarefeilen og korrigere maskiner over hele verden.

Eksempelet viser at uoppdagede sårbarheter til en hver tid utgjør en trussel, avhengig av hvem som oppdager sårbarheten og dermed muligheten til å utnytte den. Man kan tenke seg en meget alvorlig situasjon dersom noen finner en tilsvarende sårbarhet og i tillegg gjør en grundig planlegging av hvordan den skal utnyttes før den oppdages og korrigeres. Dette kalles «Zero-Day Attack» (se også kap. 2).

4.3.3 Navigasjonssystemer

Samfunnets avhengighet av *navigasjonssystemer* som GPS, øker. Eksempler på bruksområder er innen alle deler av transportsektoren, energisektoren, telekommunikasjon, finanssektoren, fiskerisektoren, miljøsektoren, nødetatene og militærsektoren. GPS har ulike svakheter eller sårbare områder. Andre radiotjenester, for eksempel innenfor VHF-båndet, kan gi forstyrrelser som kan medføre interferens og påfølgende unøyaktighet eller manglende evne til å ta imot signaler fra satellitter. Det finnes også muligheter for å forstyrre GPS-systemet bevisst ved bruk av jammeutstyr. Jammeutstyr er kommersielt tilgjengelig. Utstyr som sender ut villedende signaler er også en sikkerhetsmessig utfordring. Galileo er et europeisk

[17] FFI/rapport-2004/01666: «CYBERSPACE SOM SLAGMARK: Refleksjoner omkring Internett som arena for terrorangrep» av Iver Johansen.
[18] Symantec Internet Security Report, Feb. 2003, p.48
[19] SCADA: Supervisory Control and Data Acquisition System
[20] SNMP: Simple Network Management Protocol

alternativ til GPS som er under utvikling nå. Navigasjonssystemene vil være interoperable. To uavhengige navigasjonssystemer kan gi betydelig redundans og minske sårbarheten.

4.3.4 Elektroniske informasjonssystemer

Sårbarheten knyttet til *elektroniske informasjonssystemer* blir stadig større, samtidig som stadig større deler av samfunnet blir mer avhengig av disse. En årsak til økt sårbarhet er at det stilles store krav til mobilitet. Begrepet mobilitet kan dekke områder som trådløs teknologi, mobiltelefoner, personal digital assistants (PDA), bærbare PCer og så videre.

4.3.4.1 Trådløse nettverk

Bruk av trådløst nettverk har blitt svært populært både blant hjemmebrukere og bedrifter. Gjennom media har det blitt satt søkelys på institusjoner som benytter trådløse nettverk uten noen form for kryptering. Dette gjør at nettverket ligger helt åpent for uvedkommende. De to krypteringsprotokollene WEP[21] og WPA[22] som omfattes av dagens standard for kryptering (802.11), har også mangler i forhold til sikkerhet, men vil i alle fall gi en bedre beskyttelse enn om nettet ligger åpent.

4.3.4.2 Mobiltelefoner

Mobiltelefoner kan manipuleres uten at eieren av telefonen er klar over dette. En slik manipulering kan føre til at det er mulig for utenforstående å benytte mobiltelefonen som et medium for avlytting av sensitiv informasjon. Mobiltelefoner får stadig ny funksjonalitet. Evne til å ta opp lyd og bilde med stadig bedre kvalitet, representerer en sikkerhetsmessig ufordring.

4.3.4.3 Minnepinner og PDA

PDAer og minnepinner (memory sticks) har etter hvert fått stor lagringskapasitet. Lagringskapasiteten øker stadig. Relativt store mengder informasjon kan dermed tas med ut av det kontrollerbare området til virksomhetene. Fysisk sikring i forbindelse med små, flyttbare enheter innebærer en stor utfordring. En PDA kan inneholde informasjon som gir tilgang til virksomhetens nettverk.

4.3.4.4 Kompleksitet og avhengighet

Informasjonssystemene består generelt av stadig flere komponenter som fører til en kompleks konfigurasjon og administrasjon. Integrering av systemer og produkter fordi det oppstår nye ønsker om hva systemet faktisk skal kunne gjøre, kan medføre økt sårbarhet. Det blir stadig vanskeligere å ha en fullstendig oversikt over blant annet sikkerhetsløsningene i systemet, og om disse er konfigurert slik at de virker hensiktsmessig. Personellet som skal operere systemene blir også stilt overfor stadig større utfordringer som krever at kompetanse vedlikeholdes og utvikles. Det er heller ikke heldig dersom enkeltpersoner blir alt for sentrale i utvikling og drift av et komplisert informasjonssystem. Virksomheter kan bli for avhengige av enkeltpersoner i sin oppgaveløsning.

4.3.4.5 Særlig viktige datasystemer

Datasystemer med kritiske oppgaver, som for eksempel styringssystemer i forbindelse med fjernregulering av petroleumsproduksjon, adgangskontrollsystemer, bagasjescanningssystemer på flyplasser, betalingssystemer og andre systemer av betydning for samfunnssikkerheten, leveres av private aktører. Dersom leverandørene ikke har behov for sikkerhetsgradert informasjon i forbindelse med sin leveranse, vil leverandørene normalt ikke omfattes av sikkerhetsloven. Dette innebærer igjen at det ikke finnes noen hjemmel for å etterspørre eksempelvis sikkerhetsklareringer eller dokumentasjon på implementerte sikringstiltak hos leverandøren, som kan redusere risiko for at ondsinnede aktører får mulighet til å gjennomføre anslag. En kan ikke utelukke at dette forholdet gir større mulighet for ondsinnede aktører til å plante feil i et kritisk datasystem, eller på annen måte sette et informasjonssystem ut av funksjon.

4.3.5 Problemet med avhengigheter på tvers av infrastrukturer

En viktig del av trusselbildet utgjøres av den til dels uforutsigbare avhengigheten på tvers av ulike infrastrukturer. Vi vet en del om disse avhengighetene (se for eksempel rapporter fra tidligere BAS-prosjekter), men nøyaktig hvordan disse avhengighetene påvirker utfallet av et større angrep eller utfall i en sektor er fortsatt vanskelig å forutsi.

En eller annen form for kaskadevirkning vil kunne bli resultatet av et angrep. Ett eksempel er resultatet av «Blaster-ormen» i august 2003, som slo ut en lang rekke datamaskiner i flere dager. Det er antatt at virkningen av dette også forplantet seg og forverret situasjonen ved det store strømutfallet 14 august i USA, ved at kapasiteten i kommunikasjonen fra styringssystemer ble sterkt redusert.

[21] Wired Equivalent Privacy.
[22] Wi-Fi Protected Access.

Varsling og styring kom dermed ikke frem i tide til underliggende systemer.

SCADA-systemer kan vise seg å utgjøre stadig større sårbarhet for samfunnet. I store deler av kritisk infrastruktur utgjør disse systemene en helt sentral del. Det er automatiserte systemer med liten bemanning, og de er som regel avhengige av forbindelser til punkter som ligger spredt omkring og ofte på vanskelig tilgjengelige steder.

Noen eksperter mener at disse systemene er særlig sårbare, og at den vitale rollen de har gjør dem særlig interessante for nettverksterrorisme. Tidligere var disse systemene isolert fra andre systemer i tillegg til å bestå av proprietær programvare. I dag er det mer og mer vanlig at det benyttes hyllevare-programmer (COTS[23]), og dessuten er de i stadig større grad knyttet sammen med andre nettverk, for ikke å si Internett. Enkelte mener at mange SCADA-systemer har utilstrekkelig beskyttelse mot nettverksangrep og vil forbli sårbare fordi de virksomhetene som benytter seg av systemene i for liten grad fokuserer på sikkerheten. Fordi slike systemer har så høy grad av krav til tilgjengelighet (driftes som regel på 7/24/365-basis), blir kanskje ikke korreksjoner i programvare lagt inn så raskt som de burde.

Imidlertid gis også uttrykk for at SCADA-systemene og den kritiske infrastrukturen er mer robust og motstandsdyktig enn antatt, og at normalisering av driften som regel ikke vil ta særlig lang tid. I den forbindelse vises det til at det faktisk skjer ganske mange tilfeldige hendelser og feil i disse systemene fra tid til annen; hendelser som i noen grad forårsaker virkninger som kan likne på dem fra et nettverksangrep. Som regel får disse hendelsene ikke så omfattende effekter. Dersom et nettverksangrep skal kunne få en terrorliknende effekt, vil angrepet måtte rette seg mot mange mål samtidig og over lengre tid.

4.3.5.1 Innsideproblematikk

Teknologien skaper store endringer i forhold til måten mennesker organiserer sin virksomhet på. Organisasjoner veves i stadig større grad sammen ved hjelp av IT-systemer. Interaksjonen mellom menneske, teknologi og organisasjon kan skape økt sårbarhet. Holdninger og atferd på individuelt plan som i sin helhet utgjør organisasjonskulturen i en virksomhet, kan føre til økt sårbarhet ved at informasjonssikkerhet ikke tas på alvor.

Computer Security Institute (CSI) og Federal Bureau of Investigation (FBI) sin store undersøkelse om datakriminalitet i USA, viser at innsidemisbruk av nettverk er den nest største sikkerhetstrusselen. Bare virusangrep er større.[24]

CERT/CC[25] i USA rapporterer at mens 43% av alle som svarte i en undersøkelse viste til økende trussel mot nettverksangrep de siste årene (2004). Av disse svarte over 30% at de ikke visste om trusselen skyldtes innside eller utside! Av de som mente de hadde kunnskap om dette, ble 71% av angrepene initiert fra utsiden, mens 29% kom fra innsiden[26].

Årsakene til innsideproblematikk kan deles inn i ni underkategorier[27] ut fra hendelsens natur og motivasjon: Ønske om økonomisk gevinst, ulykkelighet, dekke over feil, lage og løse kriser, støtte eksterne grupperinger, misbruk av informasjon, tyveri av maskinvare eller programvare, bruk av utstyr til privat sammenheng og feil som skyldes interaksjon mellom brukere og datamaskiner.

4.3.6 Kraftsektoren

Kraftsektoren er spesielt interessant i forbindelse med samfunnssikkerhet. Fellesnevneren for Internett og elektroniske informasjonssystemer er nettopp kraftsektoren. Uten elektrisk strøm vil verken Internett eller elektroniske informasjonssystemer kunne fungere. Selv om det i mange tilfeller er etablert redundans blant annet i form av reservestrømløsninger, er det sannsynlig at det vil kunne oppstå problemer over tid dersom strømmen er borte. Kraftsektoren har imidlertid innført en del tiltak som skal redusere risiko for ondsinnede, tilsiktede handlinger. Et eksempel på tiltak er «Forskrift om beredskap i kraftforsyningen» som trådte i kraft 1.1.2003. Det kan også bemerkes at kraftforsyningen i Norge er mindre sårbar enn i andre land, blant annet på grunn av at avhengigheten av det enkelte produksjonsanlegg er mindre.[28]

4.3.7 Transportsektoren

Transportsektoren utpeker seg som et attraktivt mål for terrorhandlinger ved at transportmidler kan

[23] COTS: Commercial-Off-The-Shelf

[24] Power, Richard (2002): Computer Crime and Security Survey, Computer Security Institute & Federal Bureau of Investigation.

[25] CERT/CC: Computer Emergency Response Team Coordination Center

[26] «E-crime Watch Survey Shows Significant Increase in Electronic Crimes», CSOonline.com, 25.mai 2004

[27] Albrechtsen, E. (2002): A review of the insider threat to organisations' information security level. Department of Industrial Economics and Technology Management, NTNU, Trondheim.

[28] Stortingsmelding nr. 39 2003-2004 «Samfunnssikkerhet og sivilt-militært samarbeid», s. 9.

benyttes både som leveringsmiddel for eksplosiver og som våpen i seg selv. I tilknytning til transport er det ofte store folkeansamlinger, noe som i seg selv også er et attraktivt mål.

Ødeleggelsespotensialet ved for eksempel å kapre en tankbil fylt med bensin for deretter å kjøre den inn i en bygning/installasjon, er dramatisk. Kjøretøy benyttes også svært ofte som plattform for eksplosiver, eksempelvis i selvmordsangrep. Denne type angrep, som kommer svært hurtig og gjerne helt uventet, har økt terroristenes sjanser til å ramme såkalte «harde» mål, det vil for eksempel si militære mål, dramatisk. Det er særdeles vanskelig å forebygge selvmordsaksjoner av denne typen. Fysiske barrierer må ha en kraftig dimensjonering for å kunne stanse store kjøretøy effektivt. I et bymiljø vil det uansett være svært problematisk å oppnå avstand til detonasjonen, selv om en har fysiske barrierer.

Det bør være et mål for sikkerhetsarbeidet at det ikke skal være enkelt å få tilgang til store kjøretøy som transporterer farlig gods. Tilgang til farlig gods på generell basis, herunder eksplosiver, bør gjøres så vanskelig som mulig for ondsinnede aktører.[29]

Folkerike områder vil alltid være attraktive mål for terrorhandlinger. Jernbanestasjoner og lufthavner kan nevnes i denne sammenheng.

Det har vært få angrep mot maritime mål i den vestlige verden, sammenlignet med angrep mot andre typer mål. Skip som transporterer eksplosiv eller giftig last kan være et mål i seg selv. Men skipet kan også utnyttes for å ramme andre mål, slik at skipet blir et våpen. Et skip i fart vil være spesielt sårbart overfor angrep for eksempel fra selvmordsaksjonister i småbåter fylt med sprengstoff. Skip som ligger i havn vil kunne beskyttes bedre mot terrorhandlinger enn skip som er i fart. International Maritime Organization (IMO) har vedtatt internasjonale sikkerhetsbestemmelser for skip og havner. Bestemmelsene trådte i kraft 1.7.2004.

4.3.8 Petroleumssektoren

Petroleumssektoren er viktig for den norske stat. Den daglige verdien av norsk gasseksport i 2004 var på ca. 260 millioner kroner. Petroleumssektoren er også viktig i en større sammenheng ved at Norge er en viktig leverandør av særlig gass, til blant annet Europa. Manglende sikringsnivå i Norge sammenlignet med andre land, kan gjøre det mer attraktivt for ondsinnede aktører å gjennomføre handlinger her. En bevissthet om dette hos utenlandske kjøpere av norske petroleumsprodukter, kan i verste fall føre til at andre leverandører, med et høyere sikringsnivå, blir valgt.

Produksjon og eksport av olje og gass må kunne skje uhindret av for eksempel terrorhandlinger. Rørledningssystemet i seg selv, samt installasjoner til havs, kan være et mål for sabotasje og terrorhandlinger. Men ulike forhold gjør at transportsystemet er robust.

En historisk gjennomgang[30] av terroranslag mot olje- og gassinstallasjoner viser at anlegg på land er langt mer utsatt for anslag enn de som er til havs. Viktige anlegg på land i Norge kan være attraktive mål for ondsinnede aktører. Petroleumssektoren har tradisjon for å være dyktige i forhold til «safety». Tiltak i forhold til «security», som innebærer økte kostnader uten at det synes som om en reell trussel foreligger, synes ikke å være like høyt prioritert i Norge, til tross for sektorens betydning for samfunnet i sin helhet. Sektoren faller i dag utenfor sikkerhetslovens virkeområde.[31]

4.3.9 Menneskelige sårbarhetsfaktorer

Tekniske sikkerhetstiltak har ikke særlig verdi dersom organisasjonskulturen gir rom for å bryte regler/tekniske barrierer fordi det kan være både praktisk og tidsbesparende.

Mennesket er en barriere mot sikkerhetstruende virksomhet ved at mennesket følger de regler og rutiner som er gitt. Årvåkenhet er en stor styrke og den viktigste deteksjonsmekanismen for sikkerhetstruende virksomhet.

Samtidig har mennesket fri vilje og egne følelser, noe som innebærer spesielle utfordringer i forhold til forebyggende sikkerhetstjeneste. Press utenfra, som kan ha sin årsak i for eksempel dårlig økonomi, kan gjøre en person ustabil. Lojalitet til den virksomheten som en arbeider i, kan bli satt på prøve i en omstillingsfase. Oppsigelser kan medføre misnøye, som igjen kan gå ut over lojalitetsfølelsen. Ansatte kan, i visse tilfeller, dermed bli en sikkerhetsrisiko.

4.4 Hvor reell er trusselen om nettverksterrorisme?

I utgangspunktet er det viktig å skille mellom «nettverksangrep» og «nettverksterrorisme». Det

[29] Direktoratet for samfunnssikkerhet og beredskap har varslet at det vil bli innført strengere krav til sikring av eksplosivlagre mot innbrudd (www.dsb.no 3.3.05).

[30] FFI/rapport-2004/01682.

[31] Det kan nevnes at petroleumstilsynet ble etablert 1.1.2004 og har som prioritert oppgave satt i gang en oppfølging av sikkerhet og beredskap ved landanleggene.

første begrepet omhandler alle logiske angrep, så vel store som små, som kan rette seg mot enkeltmaskiner hos privatpersoner eller bedrifters informasjonssystemer. Nettverksterrorisme må defineres som omfattende logiske angrep som fører til store ødeleggelser og betydelige tap av liv. Selv om hackeres aktiviteter på nettet kan føre til omfattende skadevirkninger, ville det ikke være riktig å sette alle hackere i samme kategori som terrorister.

Det er vanskelig å forestille seg at nasjonal infrastruktur som vannforsyning, strømforsyning, kraftforsyning etc. kan rammes katastrofalt på grunn av terror i form av logisk angrep fra utsiden alene, uten at det også er etablert noen form for støttespillere på innsiden. På grunn av den sikkerheten som tross alt finnes i disse systemene er et fullstendig fjernstyrt terrorangrep med slike virkninger mindre sannsynlig. Ikke desto mindre skal man være oppmerksomme på de stadig sterkere koblingene som skjer mellom prosess-systemer og Internett.

Det er mulig å hacke seg inn i IT-systemer som styrer for eksempel vannforsyning. Men det er ikke uten videre enkelt å skulle overta styringen uten at dette oppdages av det ordinære driftspersonellet. Å hacke seg inn i slike nettverk for å gjøre skadeverk er fortsatt vanskeligere enn å plassere en bombe på et strategisk sted. Selv om terrorister kan ha aldri så onde hensikter, vil de fortsatt være opptatt av hvilke midler som er mest effektive ut fra en «kost/nytte-betraktning». Det er jo heller ikke slik at det finnes én logisk bryter noe sted verken i kraftforsyningen, telesystemene eller andre steder som har en «steng alt»-funksjon!

Den største trusselen fra så vel rene hackere som terrorister er et angrep som kombinerer bruk av fysiske midler og logisk inntregning. Logisk angrep som forhindrer planlagt respons og andre nødtiltak, saboterer transport eller telekommunikasjon ved hjelp av innsidere kan mangedoble effekten av et vel planlagt angrep.

Den angrepsformen som fortsatt er mest sannsynlig er den vi har sett til nå, med spredning av ondsinnet programvare via e-post og på andre måter i nettverket., identitetstyveri og phishing, DDoS angrep og endring av data via åpne og skjulte angrep. Slike kriminelle angrep kan utløses meget enkelt og av svært mange mennesker. Vi har imidlertid sett svært få (om noen) eksempler hittil på forsøk på å slå ut for eksempel strømforsyningsnettverk på denne måten.

Uansett vil slike angrep, dersom de skal komme på en terrorists agenda, høyst sannsynlig måtte betinge hjelp fra innsiden. Trusselen må følgelig også sees i sammenheng med innsidetrusselen.

Den raske utviklingen i nettverksangrep fra så vel organiserte kriminelle som andre grupper, gjør at myndigheter må ta på alvor behovet for å beskytte kritisk infrastruktur kontinuerlig på 24/7-basis. Selv uten terrorangrep med katastrofale tap er virkningene av alle de pågående angrepene i seg selv en grunn til å beskytte seg.

Kanskje er særlig små og mellomstore bedrifter (i tillegg til privatpersoner) særlig utsatt ved at de ikke har tilstrekkelig kompetanse og økonomiske midler til å skaffe seg tilfredsstillende beskyttelse. Selv om de ikke er utpekte mål for spesielle angrep, vil mange av dem før eller senere bli offer for ett av de utallige angrepene som settes ut i livet uten noen bestemt adresse.

Som nevnt vil et målrettet og effektiv logisk angrep mot et mål kreve bistand fra noen på innsiden. En enkelt ansatt vil kanskje ikke alene kunne sette opp et slikt angrep. En misfornøyd ansatt som arbeider på et særlig viktig sted kan bestikkes eller trues, eller kanskje frivillig stille seg til rådighet for noen på utsiden som har kapasitet til å planlegge et større angrep. Akkurat dette har vært demonstrert mange ganger i for eksempel svindelsaker eller når særlig alvorlige hackerangrep har vært gjennomført.

En mer inngående vurdering av trusselen fra terrorgrupper må innbefatte konkret vurdering av intensjon og kapasitet hos bestemte, identifiserte grupperinger. Dette ville forusette etterretningsinformasjon som nødvendigvis er sikkerhetsgradert. Likevel kan det gjøres noen generelle betraktninger om dette.

Terroristgrupper har i det store og hele ikke vist seg å være innovatører. (Ett viktig unntak er i så fall planleggingen, forberedelsene og gjennomføringen av terrorangrepet 11.9.2001.) I lang tid har terroren hatt som middel å forårsake mest mulig fysisk ødeleggelse og tap av menneskeliv. Konvensjonelle våpen er blitt brukt, gjerne improviserte eksplosiver og andre våpen. Et eksempel på mindre vanlig middel var bruken av sarin fra sekten Aum Shinrikyo i Tokyos undergrunnsbane i 1995. Men også her var formålet å skade størst mulig antall personer, for på den måten å skape frykt i samfunnet. I den grad kritisk infrastruktur har vært gjenstand for angrep fra terrorgrupper, har det også vært benyttet konvensjonelle midler.

Det finnes enkelte momenter som kan virke i retning av å avstå fra å benytte logisk nettverksangrep som terrormiddel:

Usikkerhet om virkningen

Et logisk angrep mot for eksempel et SCADA-system som styrer funksjoner i kritisk infrastruktur, kan ha potensial til å være ødeleggende og forårsake mye skade og kanskje også tap av menneskeliv. Dette er et hovedmotiv for en slik terroraksjon. Med mindre angriperen virkelig har detaljert kjennskap og nærmest kan forutsi virkningen, kan han risikere at virkningen uteblir eller også forblir ukjent. Dersom driftspersonell faktisk er i stand til å håndtere situasjonen som oppstår som følge av angrepet, vil formålet med angrepet jo heller ikke bli oppfylt. På den annen side ville virkningen av et konvensjonelt angrep vise seg øyeblikkelig, og krever dessuten i mye mindre grad deltaljkunnskaper om systemet.

Gjenoppretting etter logisk angrep enklere

Et logisk angrep mot et SCADA-system forutsetter at angriperen er i stand til å manipulere systemet mer eller mindre på dets premisser. Dersom angrepet oppdages raskt, vil det som regel være mulig å korrigere skaden samt forebygge ytterligere ødeleggelse. Slik gjenoppretting vil gå raskere enn etter et konvensjonelt angrep, gjennom reinstallering av operativsystem og nødvendige applikasjoner, innhenting av sikkerhetskopier etc. Til sammenlikning vil gjenoppretting etter konvensjonelt angrep kunne medføre atskillig mer omfattende arbeid. Fra en terrorists synspunkt vil muligheten for rask gjenoppretting bety et langt mindre effektivt angrep.

Mulighet for benekting av hendelsen

I alminnelighet vil dette kunne være aktuelt for en utøver av et ordinært logisk angrep, nemlig å skjule kilden for angrepet og eventuelt hvem som har utført det. Men benekting kan også tenkes fra «offerets» side. Dersom viktige samfunnskritiske mål er angrepet, men rask respons har gjort det mulig å avgrense skaden, vil det kanskje være mulig å skjule hva som faktisk har skjedd. Selv om angrepet ble vellykket i større eller mindre grad, vil det fortsatt være vanskelig å påvise hvem som utførte det og hvordan det faktisk skjedde. Resultatene etter et konvensjonelt angrep vil være langt vanskeligere å benekte, for ikke å si umulig. Dersom det viser seg å være vanskelig å påvise at resultatet etter et logisk angrep faktisk skyldtes et terrorangrep, vil effekten av det som sådant bli redusert.

4.4.1 Trusler om logiske angrep med andre motiver

Helt siden «world wide web» så dagens lys tidlig på 90-tallet har politisk motiverte logiske angrep forekommet, også kalt «hacktivism». Til å begynne med var dette ikke en veldig utbredt aksjonsform, men i de senere år har vi sett stadig flere eksempler. Politisk motiverte nettverksangrep ble iverksatt under Balkan-konflikten, under globaliseringskonferansen og i forbindelse med politisk massemobilisering i Nederland i mai 2004.

Slike politiske nettverksangrep involverer vanligvis «defacing»[32] (med politisk budskap) eller en eller annen form for tjenestenektangrep (DoS) fra grupper av hackere eller enkeltpersoner. Denne typen nettverksaksjoner vil sjelden kunne føre til katastrofal skade eller true liv og helse.

Enhver virksomhet eller organisasjon som er knyttet til Internett står overfor en trussel om et nettverksangrep. Hyppigheten av søk med ondsinnede motiver på nettet, økningen av stadig mer informasjon om sårbarheter i maskiner og på nett og stadig flere rapporter om alvorlige nettverksangrep illustrerer at muligheten for et angrep er svært høy og antallet mulige angripere likeså.

Motivene for slike angrep varierer fra rene økonomiske, ønske om å utnytte andres ressurser, skaffe seg konkurransefortrinn til ønske om ren ødeleggelse. Dessuten er dette som oftest «blind vold» ved at de som utfører angrepene er mindre interessert i hvem de rammer enn det å utføre et angrep i seg selv.

Trusselen om et nettverksangrep må altså sies å være høy. Dette vil hovedsakelig ikke dreie seg om en terrortrussel, økt internasjonal spenning eller konflikter stater imellom.

Misbruk av uttrykket «nettverksterrorisme» og å løfte dette opp som den største trussel i dag vil imidlertid kunne avlede oppmerksomhet mot andre former for nettverksangrep som har kapasitet i seg til å gjøre stor skade på virksomheter, og også på kritisk infrastruktur. Slike angrep forekommer ofte og vil fortsette å gjøre det. Fokuset bør derfor være på trusselen om alvorlige og skadelige nettverksangrep uavhengig av hvem som utfører dem og hva motivene kan være. Gjennom å ta disse truslene på alvor vil man ha et godt utgangspunkt for å beskytte seg mot alle former for nettverksangrep.

5 Kort om organisatoriske og juridiske sikkerhetsmessige utfordringer

De senere år har flere statlige virksomheter blitt skilt ut som egne selskaper. Endringer i eierskapsforhold innen kritisk infrastruktur gir sikkerhets-

[32] Uønsket endring av web-side

messige utfordringer. Sikkerhetsloven vil stort sett ikke være gjeldende for samfunnsviktige institusjoner etter at denne type endringer har funnet sted.

En årsak til dette er at virksomhetene helt og fullt privatiseres og dermed faller utenfor sikkerhetslovens virkeområde.

En annen årsak er at virksomhetene organiseres på en annen måte enn tidligere, for eksempel som statlige aksjeselskap hvor staten eier størstedelen av selskapet. Sikkerhetsloven gjelder ikke for aksjeselskap.

Det er derfor av sikkerhetsmessig betydning at sektordepartementene fortløpende vurderer om et selskap eller en institusjon bør omfattes av sikkerhetsloven, og eventuelt fremmer forslag om dette til Forsvarsdepartementet, slik sikkerhetsloven gir adgang til.[33]

Det er naturlig nok ikke slik at en virksomhet automatisk vil få redusert risiko for å bli rammet av spionasje, sabotasje og terrorhandlinger, dersom virksomheten blir omfattet av sikkerhetsloven. Mange samfunnsviktige aktører har også flere tiltak på plass allerede i dagens situasjon, selv om de ikke omfattes av sikkerhetsloven.[34]

Sikkerhetsloven beskriver likevel et rammeverk av tiltak som, dersom reglene implementeres, vil gi en helhetlig grunnsikring. Et viktig fortrinn med sikringsregimet som beskrives av sikkerhetsloven, er de klare krav som settes blant annet til verdivurdering av informasjon, sikkerhetsgradering og håndtering av denne. Innledningsvis ble det poengtert at *tilgang til* sårbarhetsinformasjon, eksempelvis beredskapsplaner og planer for fysisk sikring av en samfunnsviktig institusjon, faktisk kan være med på å *utløse anslag*. En måte å redusere risiko for anslag på, er derfor å beskytte virksomhetens sårbarhetsinformasjon. Sikkerhetsloven angir også at selve objektet skal skjermes gjennom ulike tiltak, for eksempel fysiske sikringstiltak. Nærmere regler om dette forventes å komme.

6 Hva vet vi om sikkerhetsnivået i virksomheter i dag?[35]

Det er, på generelt grunnlag, vanskelig for virksomheter å vurdere om informasjon skal gis beskyttelse i form av en sikkerhetsgradering. Endringer i risikobildet ser ikke ut til å bli oppfanget i form av endringer i virksomheters praksis i forhold til sikkerhetsgraderinger. Dette innebærer at informasjon som burde ha blitt beskyttet ikke blir beskyttet, eller at virksomheter bruker unødige ressurser på å beskytte informasjon som ikke er spesielt verdifull.

Det ser ikke ut som om virksomheter evaluerer egne sikkerhetstiltak i særlig grad. Dette innebærer at virksomheter egentlig ikke vet om sikkerhetstiltakene gir den sikkerhet de er ment å skulle gi. Flere virksomheter gjennomfører ikke en autorisasjonsprosess. Autorisasjon er et sikkerhetstiltak som skal sikre at den sikkerhetsklarerte har tilstrekkelig kunnskap om håndtering av skjermingsverdig informasjon. Politiets sikkerhetstjeneste har i april 2005 uttalt at spionasjevirksomheten mot Norge og norske forhold har økt de siste årene. Det er derfor bekymringsfullt at autorisasjonsprosessen ikke ser ut til å bli prioritert som et viktig, forebyggende sikkerhetstiltak rettet særlig mot å redusere risiko for spionasje.

Organiseringen av sikkerhet ser ut til å bli nedprioritert når virksomheter er i en omstillingsfase. Dette er spesielt uheldig fordi virksomheter ofte er mest sårbare nettopp i en omstillingsfase, hvor det skjer endringer både innenfor personell og materiell.

---

[33] Departementene ble bedt om å foreta en slik vurdering i skriv fra Forsvarsdepartementet, datert 10.9.2003 (2003/00851-25-/FD I 4 jur/JHO/353. Senere er virkeområdet utvidet til å omfatte bl.a. Telenor ASA og Avinor AS. Enkelte andre virksomheter vurderes nærmere.

[34] Konkurransemessige hensyn kan være årsaken til at sikringstiltak er på plass. Muligheten for tap av fortjeneste og omdømme dersom virksomheten for eksempel rammes av kriminalitet, kan være med på å begrunne implementering av sikringstiltak.

[35] Nasjonal sikkerhetsmyndighet innhenter informasjon om sikkerhetstilstanden gjennom tilsyn, resultater fra spørreundersøkelser, innrapporterte hendelser, innhenting av informasjon fra samarbeidende tjenester og ulike fagmiljøer, samt medieovervåkning.

Vedlegg 7

Oppfølgingen av sårbarhetsutvalgets forslag

Delrappport til Utvalg for sikring av landets kritiske infrastruktur

Kjetil Sørli, Direktoratet for samfunnssikkerhet og beredskap
Enhet for analyse og utredning
Endelig versjon 5. juli 2005

1 Innledning

3. september 1999 utnevnte regjeringen ved kongelig resolusjon et offentlig utvalg for å utrede samfunnets sårbarhet og beredskap. Utvalget ble kjent under navnet Sårbarhetsutvalget, og ble ledet av Kåre Willoch. 4. juli 2000 leverte utvalget sin sluttrapport. Denne teksten er en delrapport til ISU med en redegjørelse av oppfølgingen av sårbarhetsutvalgets rapport

Sårbarhetsutvalget utredet samfunnets sårbarhet med sikte på å styrke samfunnets sikkerhet og beredskap. Mandatet var å gi en helhetlig beskrivelse av risikoen for ekstraordinære påkjenninger mot det sivile samfunnet i fred, sikkerhetspolitiske kriser og krig. Et felles risikobilde skulle danne grunnlag for prioriteringer og anbefalinger om tiltak.[1]

Sårbarhetsutvalget rapport fikk stor oppmerksomhet i det politiske miljø og media, og fremstår i ettertid som et referansedokument om samfunnets sårbarhet. Det blir i ulike sammenhenger fremdeles referert til sluttrapporten i dag.

Det kan hevdes at det viktigste resultatet av utvalgets arbeid var å gjøre oppmerksom på og øke bevisstheten om samfunnets sårbarhet hos allmennheten generelt, og hos beslutningstakere og embetsverk spesielt. Trusselen om den totale krig hadde vært fraværende i om lag ti år, og med rapporten ble den sikkerhetspolitiske oppmerksomhet mer rettet mot det moderne samfunnets sårbarhet for avbrudd i viktige forsyninger av varer og tjenester som følge av menneskelige feil, tekniske sammenbrudd, naturkatastrofer, terror, sabotasje og krigshandlinger. Det første BAS-prosjektet om samfunnets sårbarhet og organiseringen av beredskap ved Forsvarets forskningsinstitutt (FFI), leverte riktignok sin sluttrapport i 1997, men det var først med sårbarhetsutvalget at utfordringene ble løftet opp til et nivå hvor det fikk nasjonal oppmerksomhet. Det er også av interesse i denne sammenheng at utvalget pekte på hvor sårbart det moderne samfunn er mot terrorisme over ett år før hendelsene i USA 11. september 2001.

2 Utvalgets forslag

Retrospektivt er det vanskelig å vise til at konkrete forslag ble fulgt opp eller ikke som et direkte resultat av utvalgets anbefalinger. Parallelle prosesser og andre kilder har bidratt til å påvirke utformingen av tiltak i ettertid. Det empiriske grunnlaget for å hevde det ene eller det andre er ikke tilstrekkelig. Vi vil derfor i de fleste tilfeller være forsiktig med å fastslå direkte koblinger, og heller eventuelt antyde disse. Samtidig kan vi i ettertid fastslå at svært mange av forslagene er gjennomført. Vi ser også at utvalgets rapport ga vektige innspill og påvirket viktige dokumenter som St.meld. nr. 17 (2001-2002) Samfunnssikkerhet – Veien til et mindre sårbart samfunn og Stortingets oppfølging av den, St.meld. nr. 17 (2002-2003) Om statlige tilsyn og Stortingets oppfølging av den og St.meld. nr. 39 (2003-2004) Samfunnssikkerhet og sivilt-militært samarbeid og Stortingets oppfølging av den. Hendelsene i USA 11. september 2001 bidro også til at enkelte tiltak som utvalget hadde foreslått i forskjellig grad ble forsert.

Det vil i det følgende ikke bli redegjort for oppfølgingen av alle forslagene. Redegjørelsen tar utgangspunkt i de utfordringer, anbefalinger og forslag som er samlet i delkapittel 1.3. i utvalgets rapport. De fanger opp bredden av utvalgets forslag, og er i seg selv omfattende.

De viktigste forslagene er delt opp i følgende: Sektorvise forslag, organisatoriske forslag, juridiske forslag og forslag knyttet til forsknings og

[1] Se vedlegg 1 for mandatet.

utdanning. Utvalgets forslag er presentert i kursiv, mens oppfølgingen blir gjengitt i kulepunktet under forslaget.

3 Sektorvise forslag:

Terror og sabotasje – kapittel 5

- *Å styrke samarbeidet mellom politi og forsvar mot mulig omfattende terror og sabotasje. eksisterende regelverk og beslutningsprosedyrer for bistand fra Forsvaret til politiet i fred bør gjennomgås med sikte på at man overfor væpnede motstandere i kritiske situasjoner så raskt og effektivt som mulig vil kunne sette inn militære ressurser som støtte til politiets krisehåndtering.*
  - Ansvars- og kommandolinjene mellom Forsvaret og Politiet er gjennomgått og fastsatt, jf. kgl. res. 28. februar 2003 (bistandsinstruksen). Ansvarsforholdet mellom Politiet og Forsvaret er for øvrig grundig redegjort for i St.meld. nr. 39 (2003-2004), kap. 5. Det er også gjennomført øvelser med scenarioer hvor forsvaret gir bistand til politiet.

Informasjons- og kommunikasjonsteknologi (IKT) og kraftforsyning – kapittel 6

- *Å fastsette klare sikkerhetskrav til etablering og drift av kritiske IKT-systemer.*
  - Post- og teletilsynet arbeider med skjerpede sikkerhetskrav til leverandørene. I dag er det slik at Ekomlovens bestemmelser om krav til sikkerhet i utgangspunktet omfatter alle leverandører av telefoni- og kommunikasjonstjenester. Til og med 2005 er det i tillegg inngått særlige avtaler med Telenor om spesielle sikkerhetstiltak. Fra og med 2006 vil alle leverandører med IKT infrastruktur av betydning og andre leverandører med leveranser til brukere med samfunnskritisk funksjon bli omfattet av slike avtaler. Sikkerhetskravene omfatter blant annet tiltak innen fysisk og logisk sikring av kommunikasjonssystemer, krav om beredskapsplanlegging og prioritering av ressurser.
- *Å etablere et Senter for informasjonssikring som får i oppgave å koordinere oppgaver innen hendelsesrapportering, varsling, analyse og erfaringsutveksling i forhold til trusler mot IKT-systemer.*
  - Nærings- og handelsdepartementet (NHD) besluttet å etablere Senter for informasjonssikring (SIS) som et prøveprosjekt med virkning fra. 01.04.2002 og ut 2004. Formålet med prosjektet er å etablere et senter som på sikt kan få ansvar for nasjonal koordinering av oppgaver innen hendelsesrapportering, varsling, analyse og erfaringsutveksling i forhold til trusler mot informasjons- og kommunikasjonsteknologiske systemer (IKT). Prøvedriften er utvidet, og slik det ligger an per mai 2005, ser det ut til at prøvedriften vil vare ut 2005. Det arbeides også med å få etablere en NorCERT (Computer Emergency Responce Team) for å håndtere angrep mot kritiske IKT-systemer. Per mai 2005 er det ikke avgjort hvilken institusjonell tilknytning NorCERT vil få. Kandidater er SIS, Post- og teletilsynet, Nasjonal sikkerhetsmyndighet og et konsortium med tilknytning til Høgskolen på Gjøvik.
- *Å bygge opp kapasitet og kompetanse til å føre effektivt tilsyn med IKT-sikkerheten innenfor all samfunnskritisk virksomhet.*
  - Ingen helhetlig løsning er på plass. Nasjonal sikkerhetsmyndighet har et overordnet myndighetsansvar innenfor sikkerhetsloven. Sikkerhetsloven gjelder kun offentlige virksomheter.
- *Å oppdatere retningslinjene for sikring av kraftforsyningen.*
  - NVE har utarbeidet strategier for beredskap innenfor sitt forvaltningsområde, basert på sårbarhetsutredningen og anbefalinger fra FFIs BAS 3. Strategiene gjelder for perioden 2002-2010. Hva gjelder retningslinjene for sikring av kraftforsyningsanlegg og håndbok for beredskap innen kraftforsyningen, er disse erstattet av forskrift om beredskap i kraftforsyningen. Forskriften ivaretar de hensyn som er omtalt i BAS 3, og gir en lovhjemmel der det før kun var retningslinjer. Revidert energilov, med et kapittel 6 om beredskap, gir NVE hjemmel til å utferdige forskrifter for bl.a. leveringskvalitet, systemansvar, energiplanlegging, kraftrasjonering og beredskap.
- *Å videreføre arbeidet med kartlegging av risiko for flom og dambrudd i lys av nye risikoforhold.*
  - I vannressursloven av 2001 er hjemmelsgrunnlaget forbedret i forhold til den gamle vassdragsloven, og tilpasset de fremtidige utfordringene innen vassdragsforvaltningen. Forskrift om sikkerhet og tilsyn med vassdragsanlegg er gitt med hjemmel i vannressursloven. Forskriften krever at dameier utfører dambruddsbølgeberegnin-

ger. I tillegg utfører NVE omfattende flomsonekartlegging for kommunal planlegging.

Transportsikkerhet – kapittel 7

- *Å etablere et organisasjonsmønster som sikrer et klart skille mellom viktige tilsynsfunksjoner og sektorinteresser.*
  - Dette kan ikke sies å være fulgt opp. Det er stor variasjon i hvordan man skiller mellom tilsynsfunksjoner og sektorinteresser.
- *Å få til et tettere samarbeid eller vurdere sammenslåing av tilsyn for transport med fly, båt og jernbane. Det må også sørges for uavhengig tilsyn med sikkerheten på veger og i tunneler.*
  - Det foreligger ikke planer om å slå sammen tilsyn på transportområdet, men tilsynsmyndighetene for transportsikkerhet er under endring, blant annet ut fra et ønske om at ansvaret for sikkerheten blir mer presist definert. Selv om sektorene har sine særtrekk, er det under vurdering å etablere organer for gjensidig erfarings- og kunnskapsutveksling mellom transporttilsynene. For detaljer om tilsyn for transport med fly, båt og jernbane, se St.meld. nr. 17 (2002-2003) Om statlige tilsyn og Stortingets behandling av denne, og St.meld. nr. 24 2003–2004 Nasjonal transportplan 2006–2015 og Stortingets behandling av denne.
- *Å foreta en ny kartlegging av risiko ved transport av farlig gods. Denne bør utgjøre et grunnlag for blant annet å vurdere den samlede beredskap på området, også når det gjelder helseberedskapen.*
  - I 2002 og 2003 kartla Direktoratet for samfunnssikkerhet og beredskap transport av farlig gods på vei og jernbane. Den endelige rapporten ble utgitt mars 2004. Forrige kartlegging ble foretatt i 1993 av det daværende Direktoratet for brann- og eksplosjonsvern. Kartleggingen kom som resultat av et behov både i DSB og i fagmiljøet ellers for å få foretatt en ny kartlegging av farlig godstransport. Dette ble ytterligere aktualisert etter propanulykken på Lillestrøm i år 2000 (NOU 2001:9) og gjennom Willoch-utvalgets utredning om utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet; NOU 2000:24 – Et sårbart samfunn. Både NOU 2000:24 og NOU 2001:9 anbefaler at det foretas en kartlegging av farlig godstransport i Norge. NOU 2000:24 nevner at farlig godskartleggingen bør utgjøre et grunnlag for å vurdere den samlede beredskap på området, inkludert helseberedskapen. Etter kontakt og drøfting mellom DSB og Sosial- og helsedirektoratet, ble imidlertid helseberedskapsaspektet utelatt i kartleggingen.

Forsyningsberedskapen – kapittel 8

- *Å gjøre forsyningssikkerheten innen kritiske samfunnsområder eller i særlig utsatte geografiske områder mer robust, blant annet ved å bygge inn krav til forsyningssikkerhet i avtaleverk med leverandører.*
  - Forsyningsberedskap omfatter tiltak for å styrke robustheten i leveransene av alle varer og tjenester. Nærings- og handelsdepartementet har innenfor sine ansvarsområder gjennomført en rekke risiko- og sårbarhetsanalyser og identifisert behov for særskilte forberedelser eller tiltak innenfor næringene skipsfart, forsikring, bygg- og anlegg og matvaredistribusjon. Det er blant annet gjennomført en særskilt risiko- og sårbarhetsanalyse av dagligvaretilgangen til Nord-Norge. Denne analysen er representert i en rapport, som også omfatter en oppfølgingsplan med en rekke tiltak. Mange av disse tiltakene er allerede gjennomført. Blant annet er beredskapslagrene redusert til 10 dagers kaloriforbruk for befolkningen nord for Ofoten. Lagrenes sammensetning er dessuten endret fra råvarer til produkter som krever lite ressurser i form av tilberedelse. Det er dessuten kjøpt inn nødstrømsaggregater ved de store distribusjonsanleggene i landsdelen og det arbeides med å legge til rette for planlagt oppbygging av ytterligere 20 dagers beredskapslagre dersom man skulle vurdere dem som påkrevet utfra endringer i varetilgangen. Et annet oppfølgingstiltak etter risiko- og sårbarhetsanalysen for landsdelen har vært gjennomføring av fylkesvise risiko- og sårbarhetsanalyser. Disse har avdekket at bare et fåtall kommune anser seg selv eller blir vurdert av fylkesmennene som forsyningsmessig utsatte. På sentralt nivå har man siden midten av 1990-tallet arbeidet med en omlegging av beredskapssystemene fra detaljstyring og omfattende omlegginger av næringslivet til markedsbaserte tiltak basert på tett samarbeid med næringene. Omfattende reguleringstiltak som leveranseplanlegging, industriberedskapsorganisasjonen og rasjoneringssyste-

mer er fjernet. Der analyser har avdekket behov for det, er de erstattet av bransjebaserte beredskapsorganer som i samarbeid med myndighetene kan håndtere utfordringer utfra den aktuelle situasjonen. Disse organisasjonene er dels hjemlet i forskrifter og dels opprettet i henhold til frivillige rettslig bindende avtaler mellom departementet og store kommersielle aktører.

- *Å etablere tettere samarbeid mellom sivile og militære myndigheter med sikte på å forvalte sivile og militære ressurser i sammenheng.*
  - Det er flere samarbeidsfora knyttet til sikkerhet og beredskap. I de fleste fora deltar både sivile og militære myndigheter. Det sivil-militære samarbeidet er for øvrig vurdert i St.meld. nr. 39 (2003-2004) Samfunnssikkerhet og sivilt-militært samarbeid. Hva gjelder forvaltningen av ressurser knyttet til det sivil-militære samarbeidet, er det etablert en ordning med at Justisdepartementet og Forsvarsdepartementet legger frem sine respektive langtidsdokumenter parallelt for Stortinget. På denne måten kan innrettingen og prioriteringene innenfor henholdsvis Forsvaret og det sivile sikkerhets- og beredskapsarbeidet ses i sammenheng. Stortinget har forøvrig etablert som praksis at det er forsvarskomiteen som behandler budsjettkapittel 451/3451 Samfunnssikkerhet og beredskap.

Olje- og gassvirksomheten – kapittel 9

- *Å utrede behovet for å tilpasse og utvikle beredskapsorganisering, beredskapsplaner og mobiliseringstiltak i forhold til nye risiko- og sårbarhetsvurderinger.*
  - Mht. fare- og ulykkessituasjoner, herunder terror- og sabotasje handlinger, så er disse forhold ivaretatt gjennom gjeldende regelverk for petroleumsvirksomheten på sokkelen. For de åtte petroleumsanleggene på land, som Petroleumstilsynet har tilsynsansvar for, så vil disse forhold ivaretas gjennom pågående regelverksarbeid som har som siktemål et felles HMS regelverk for petroleumsvirksomhet på sokkelen og til lands. Regelverksarbeidet ledes av Petroleumstilsynet og gjennomføres i dialog og samarbeid med andre berørte etater. Nytt regelverk planlegges å trå ikraft fra 1.1.2007.
- *Søke å forhindre for stort press på sikkerhetsmarginene hos oljeselskaper og/eller Staten ved at de rådende prinsipper for risikobasert styring og kontroll suppleres med grunnleggende sikkerhetskrav om barrierer og redundans ut fra et «føre var»-prinsipp.*
  - De prinsippene det her vises til er grunnleggende prinsipper for det gjeldende HMS-regelverket for petroleumsvirksomheten på sokkelen. Følges løpende opp av Petroleumstilsynet som har fokus på disse forhold gjennom i det løpende tilsynsarbeidet. Gjennom det pågående regelverksarbeidet vil disse grunnleggende prinsippene få økt fokus også for landanleggene.
- *I tillegg til arbeidet for styrket beredskap mot terror, sabotasje og militære angrep som nevnt under kapittel 5, å styrke samordningen mellom dette og det arbeidet som nedlegges i forbindelse med storulykkesrisiko.*
  - DSB er en av fem myndigheter som forvalter Storulykkesforskriften. DSB er utpekt som koordinerende myndighet for samarbeidet om oppfølgingen av denne forskriften. Den er utledet fra EUs Seveso II direktiv og omfatter om lag 100 norske virksomheter som er regulert av storulykkeforskriften. Dette er i stor grad prosessindustri hvor det arbeides med giftige eller på andre måter farlige kjemikalier, og hvor det kan skje uhell som kan medføre alvorlige konsekvenser for mennesker, miljø og materielle verdier. Med hensyn til samordningen opp mot terror, sabotasje og militære angrep, er dette ikke gjort. Storulykkesforskriften har kun et safetyperspektiv. Endringer i dette må forankres i EU, og det pågår diskusjoner i EU som å integrere securityperspektiver i Sevesodirektivet. Justisdepartementet har utarbeidet en kongelig resolusjon som skal sette rammene for DSBs arbeid med koordineringsoppgaver som gjøres for å understøtte Justis- og politidepartementet i dets koordineringsrolle innenfor arbeidet med samfunnssikkerhet og beredskap, direktoratets generelle koordineringsansvar for oppfølging av og tilsyn med aktiviteter, objekter og virksomheter med potensial for store ulykker, samt direktoratets ansvar i forbindelse med koordinering av tilsyn med og oppfølging av virksomheters etterlevelse av storulykkeforskriften. Denne resolusjonen er nå på en siste høringsrunde i departementene.

Mat og vann – kapittel 11 og 12

- *Å etablere et felles uavhengig tilsyn for matvarekontroll som dekker alle næringsmidler. All matvarekontroll bør legges inn under en sentral ledelse. Dette inkluderer lokal matvarekontroll, som nå er et kommunalt ansvar.*
  - 1.1. 2004 ble dette overført til statlig kontroll og tilsyn med opprettelsen av Mattilsynet.
- *Å påse at det settes større kraft bak arbeidet for at kravene i drikkevannsforskriften blir oppfylt ved alle landets vannverk.*
  - Ønsket om å samle en helhetlig kontroll til statlig myndighet over vannverk og vannkvalitet, førte til at ansvaret ble tillagt én myndighet, nemlig Mattilsynet. DSB har som oppfølging til rapporten Sårbarhet i vannforsyningen (2003) tatt initiativ til prosjekter vedrørende implementering av drikkevannsforskriften ved landets vannverk (Prosjekt: Veiledningsmateriell for sikkerhet og beredskap i vannsektoren).
- *Å vurdere om Statens næringsmiddeltilsyn, fylkeslegen eller fylkesmannen kan føre tilsyn med vannverkene. Kommunenes dobbeltrolle i dag som vannverkseier på den ene siden og godkjennings- og tilsynsmyndighet på den andre siden er prinsipielt betenkelig.*
  - Etter ansvarsomlegging i 2004, ved at Mattilsynet har overtatt myndighetsområdet til næringsmiddelstilsynet, ble strukturen endret. Dette innebærer at de tidligere laboratoriene underlagt næringsmiddeltilsynet i dag er fristilt/privatisert. I praksis er de fleste nedlagt. Fylkeslegens ansvar på området begrenser seg til vannbårne sykdommer, og i noen tilfeller vannforurensing.
    Bakgrunnen for alle tre punktene finnes i rapporten Sårbarhet i vannforsyningen (2003). Sektorspesifikke lover og forskrifter for vann og avløp er fremdeles meget fragmentert.

Radioaktivitet – kapittel 13

- *Å utdype og videreutvikle samarbeidet mellom norske myndigheter og over landegrensene slik at risikoen for illegal handel og smugling av radioaktive eller spaltbare materialer til eller fra Norge reduseres. Grensekontrollen må styrkes.*
  - Toll- og avgiftsdirektoratet har anskaffet mobile skannemaskiner for kontroll av containere. Maskinene er mobile og flyttes rundt med lastebil. Den ene vil brukes først og fremst ved Svinesund, og den andre vil bli flyttet rundt om i landet.
  - Det er anskaffet tre stasjonære nukleære detektorer ved Storskog grensestasjon ved den russiske grensen. Toll- og avgiftsdirektoratet drifter detektorene og Strålevernet bistår faglig.
  - I mars 2004 ble Norge fullverdig partner i det såkalte Initiativet for spredningssikkerhet, forkortet PSI. En rekke land deltar i arbeidet, herunder USA, Russland, Frankrike og Storbritannia. Siktemålet er å hindre at bl.a. skip og fly benyttes for å spre masseødeleggelsesvåpen.
- *Å sikre beredskapsorganisasjonen mot atomulykker tilstrekkelige ressurser til å ivareta og videreutvikle atomulykkesberedskapen også hos aktører hvor det er uklart sektoransvar og ikke direkte departemental styring.*
  - Det foreligger en langsiktig plan for oppgradering av den nasjonale atomulykkeberedskapen. Dette i regi av Kriseutvalget. Planen er fulgt opp gjennom St.prp. 54 (2001-2002), og gjennom sektorbevilgninger, spesielt fra HOD. Også andre sektorer arbeider med dette, men en god del arbeid gjenstår.
- *Å sikre kompetanse i organisasjonen og videreutvikle varslings- og vaktordningene for den nasjonale beredskapen på området.*
  - Atomberedskapsorganisasjonen i Norge består av kriseutvalget, fylkesmennene med Atomberedskapsutvalgene og kommunene. Strålevernet har sammen med DSB i den senere tid utgitt et plangrunnlag for den kommunale atomberedskapen og direktiver for gjennomføringen av denne. Alle landets fylkesmenn har aktivt bidratt til den kommunale gjennomføringen. Det er i tillegg blitt øvet i en rekke fylker og kommuner de siste årene. Det som ennå mangler er vaktordning hos fylkesmennene som gir en bedret tilgjengelighet ifm. viderevarsling etc. utover normal arbeidstid. Kriseutvalgets medlemmer har 2-timers beredskap.
- *Å gi nødvendig opplæring til det personell som vil ha oppgaver i akuttfasen av en atom- eller strålingsulykke. Grundig øvelsesvirksomhet er helt nødvendig for en effektiv beredskapsorganisasjon.*
  - Sivilforsvarets radiacmåletjeneste og renseenheter er operative. Radiacmålepatruljene og renseenhetene øves årlig og har en utrykningsberedskap lik Sivilforsvarets fredsinnsatsgrupper. Radiacmålepatruljene foretar rutinemessig måleoppdrag på om lag 500 målepunkter over hele landet, og rutiner for dette samt rapportering av data er gjennomgått og forbedret. Også politimann-

skaper, akuttmedisinsk personell og brannmannskaper er i noen grad gitt kompetanse innen ABC-vern. Det gjenstår en del arbeide, og det arbeides spesielt overfor helse.
- Kriseutvalget, de faglige rådgiverne og regionalt nivå øves. Spesielt var det mye øvingsaktivitet i atomberedskapsorganisasjonen i 2004.

Smittevern og kjemiske og biologiske stridsmidler – kapittel 10 og 14

- *Å styrke kommunenes smittevernberedskap, blant annet ved å legge til rette for mer interkommunalt samarbeid, spesielt hva angår leger med ansvar for kommunens smittevern.*
  - Utenom Oslo er det etablert 25 enheter omfattende 152 kommuner og vel 1.6 mill. innbyggere hvor interkommunalt samarbeid om kommunehelsetjenester er etablert eller oppe til vurdering. I Oslo er smittevernarbeidet dels lagt ut til bydel, men under koordinering av den sentrale Helse- og velferdsetaten hvor det er ansatt egen smittevernoverlege. Andre steder har to kommuner ansatt en og samme lege som medisinsk faglig rådgiver (MFRL) og smittevernlege på deltid. I indre Østfold har man ansatt felles interkommunal smittevernlege for til sammen 10 kommuner.
    Sosial- og helsedirektoratet har gjennomført en nasjonal ROS-analyse for helse. Rapporten er per dags dato ikke ferdigstilt. Iverksetting av tiltak for å styrke kommunal smittevernberedskap avventer denne analysen.
- *Å integrere kunnskap omkring kjemiske og biologiske stridsmidler i de aktuelle utrykningsetaters programmer for opplæring og videreutdanning.*
  - For å stimulere til opplærings- og kompetansetiltak, herunder øvelser for å styrke helsesektorens kompetanse i håndtering av hendelser med atom-, biologiske og kjemiske stridsmidler, skal det gjennomføres øvelser lokalt, regionalt og nasjonalt. ABC-vern kurs for leger gjennomføres ved Forsvarets ABC-skole (FABCS). Kurs, øvelser og kompetanseheving for førstelinjepersonell er gjennomført på ad-hoc basis i regi av både FABCS og Sivilforsvarets skole Starum. Utdanningen er generelt ikke en integrert og planmessig del av utdanningsprogrammene, men gjennomføres ved behov og anmodning. Kurs for leger og politi gjennomføres på FABCS.
- *Å vurdere vaksinering av førstelinjepersonell mot aktuelle biologiske stridsmidler.*
  - Spørsmålet har vært vurdert og diskutert og det er konkludert med at det ikke er relevante vaksiner ut over det som førstelinjepersonell vanligvis tar (hovedsaklig hepatitt-B). Utrykningsteamet sammensatt av personell fra Folkehelseinstituttet og Ullevål Universitetssykehus, som skal i aksjon ved utbrudd av koppesmitte, er vaksinert mot kopper.
- *Å sørge for at sykehusene inkluderer scenarier for angrep med kjemiske og biologiske stridsmidler i sine kriseplaner.*
  - Sosial- og helsedirektoratet har gjennom ulike tiltak som møter, seminarer og øvelser minnet helseforetakene om at scenarier for angrep med B og C-stridsmidler skal inkluderes i kriseplanene.

Informasjonsberedskap før og under en krise – kapittel 16

- *Å innføre lovpålegg om informasjonsberedskap i kommunene med basis i en standard for god beredskap og som en integrert del av en mer omfattende plikt til beredskapsplanlegging.*
  - Det legges til grunn at forslaget om plikt til informasjonsberedskap i kommunene ses i sammenheng med arbeidet knyttet til en generell beredskapsplikt i kommunene.

4 Organisatoriske forslag

For å styrke arbeidet for sikkerheten og beredskapen i samfunnet forslår utvalget:

- *Samling av arbeid for samfunnssikkerhet og beredskap i ett departement som får dette som hovedoppgave.*
  - 1. september 2003 ble Direktoratet for samfunnssikkerhet og beredskap (DSB) opprettet. DSB består av tidligere av Direktoratet for brann- og elsikkerhet og Direktoratet for sivilt beredskap.
  - 1. januar 2003 ble Nasjonal sikkerhetsmyndighet (NSM) opprettet. NSM er gitt en faglig ansvarslinje til Justisdepartementet i sivil sektor.
  - Det er etablert et permanent sekretariat for Koordinerings- og rådningsutvalget for etterretnings- og sikkerhetstjenestene (KRU). I tillegg er Politiets sikkerhetstjeneste (PST) styrket.

- Regjeringen gikk inn for å følge opp sårbarhetsutvalgets anbefalinger med nødvendige tiltak og forankre totalansvaret for samfunnets sivile sikkerhet i Justisdepartementet (Sem-erklæringen). De fleste av de oppgavene som sårbarhetsutvalget mente burde samles i ett departement ligger nå til Justisdepartementet. Justisdepartementet har ansvar for Politidirektoratet, Politiets sikkerhetstjeneste, Direktoratet for samfunnssikkerhet og beredskap (det tidligere Direktoratet for sivilt beredskap og det tidligere Direktoratet for brann- og elsikkerhet), Nasjonal sikkerhetsmyndighet (sivil sektor), Hovedredningssentralene samt ansvaret for Fylkesmennenes beredskapsarbeid.

- *Opprettelse av et koordineringsorgan for EOS-tjenestene.*
  - Koordinerings- og rådgivningsutvalget for etterretnings- og sikkerhetstjenestene (KRU) er etablert som et samarbeidsorgan for spørsmål som gjelder etterretnings- og sikkerhetstjenestene, og et rådgivningsutvalg for de berørte statsråder. Utvalgets oppgaver er å ivareta overordnet koordinering av Politiets sikkerhetstjenestes, Nasjonal sikkerhetstjenestes og Etterretningstjenestens arbeidsoppgaver, prioriteringer og mål, samt analysere og utrede felles problemstillinger knyttet til trusselbildet, jf. Instruks for Koordinerings- og rådgivningsutvalget for etterretnings- og sikkerhetstjenestene, fastsatt ved forskrift 20.12.2002 nr. 1699. Utvalget består av 6 faste medlemmer fra hhv. Forsvarsdepartementet, Justisdepartementet, Utenriksdepartementet, sjefen for Etterretningstjenesten, direktøren for Nasjonal sikkerhetsmyndighet og sjefen for Politiets sikkerhetstjeneste. Ledelsen av utvalget alternerer mellom representantene fra Justisdepartementet, Forsvarsdepartementet og Utenriksdepartementet. Det er etablert et fast sekretariat for utvalget med representanter for de tre departementer som skal tilrettelegge for og følge opp saker som behandles i utvalget. Sekretariatsledelsen ivaretas av det departement som til en hver tid innehar ledelsen av utvalget. KRUs ansvar og oppgaver ivaretar samfunnets evne til å fange opp endringer i trussel- og risikobildet og evne til å iverksette tiltak for å møte nye utfordringer, særlig innenfor samfunnskritiske funksjoner.

- *Samlet strategi og vurdering av å slå sammen organer for tilsyn med sikkerhet på ulike områder.*
  - I st.meld 17 (2002-2003) Om statlige tilsyn ble det gjort en vurdering om tilsynsmyndighetene har de rammevilkår og den selvstendighet som er nødvendig for å fylle oppgavene. Det ble også gjort en vurdering om vi har de rette tilsynsmyndighetene, og om avgrensningen dem i mellom er hensiktsmessig. Videre om oppgavefordelingen mellom tilsynsenheter på den ene siden, og departementer og direktorater på den andre var i samsvar med de respektive rollene ulike deler av forvaltningsapparatet skal ha. Av konkrete fremlegg var blant annet opprettelsen av et eget petroleumstilsyn med utgangspunkt i miljøer fra Oljedirektoratet, Direktoratet for brann- og elsikkerhet og Arbeidstilsynet, og opprettelsen av Direktoratet for samfunnssikkerhet og beredskap. Av interesse i denne sammenheng er også opprettelsen av Mattilsynet 1. 1. 2004

- *Gjennomgang av landets operative rednings- og beredskapsressurser*
  - Redningsberedskapsutvalget ble etablert ved kgl.res. 10.11.2000, og avga sin innstilling til justisministeren 1. november 2001, jf. NOU 2001:31 Når ulykken er ute. Utvalget gjennomgikk landets operative redningsog beredskapsressurser og behandlet spørsmålet om man skulle ha en felles forsterkningsressurs for aktuelle brukere, eller om de enkelte fagmyndigheter og nødetater skal ha ansvaret for egne forsterkningsressurser. Utvalget fant at sistnevnte ikke ville være hensiktsmessig, og falt ned på et slags *One for all, and all for one*- prinsipp. Utvalget delte seg imidlertid på spørsmålet om hvordan den statlige forsterkningsressursen skulle organisere.

- *Felles granskningskommisjon for store ulykker og kriser.*
  - En gruppe i Arbeids- og sosialdepartementet vurderer etableringen av en fast undersøkelseskommisjon for petroleumssektoren. I denne forbindelse vil forholdet til Havarikommisjonen for sivil luftfart og jernbane vurderes. Det kan for øvrig opplyses at det foreligger en veiledning om oppnevning av ad-hoc granskingskommisjoner og om de saksbehandlingsregler som må eller bør følges av kommisjonene, jf. rundskriv G-48/75 fra Justisdepartementet. Rundskrivet retter seg til det departement som i det enkelte tilfelle forbereder spørs-

mål om å nedsette en slik kommisjon og til granskningsommisjonene selv. Rundskrivet er ikke avgrenset til gransking av ulykker og kriser.

- *Departementet bør etablere en egen enhet for å tilrettelegge for og forberede en god håndtering av ulike krisesituasjoner. Denne enheten bør plasseres i et fast lokale med oppdatert teknisk utstyr. Enheten bør ha en fast kjerne med spesialister på krisehåndtering og koordinering. Ved behov forsterkes enheten med utpekte representanter fra relevante departementer.*
  - I st.meld. 37 (2004-2005), Flodbølgekatastrofen i Sør-Asia og sentral krisehåndtering, er dette fulgt opp i følgende form:

    Regjeringen har vurdert tiltak for å styrke krisehåndteringen på strategisk nivå og vil basere fremtidig strategisk krisehåndtering på tre hovedelementer:
    - Forsterket krisekoordinering gjennom opprettelsen av Regjeringens kriseråd.
    - Presisering og klargjøring av ansvaret for krisestyring i lederdepartementet (det departementet som er mest berørt av krisen).
    - Etablering av ny krisestøtteenhet som skal bidra med støttefunksjoner til lederdepartementet og Regjeringens kriseråd i deres krisehåndtering.

Det pågår for tiden en konkretisering av tiltakene.

5 Juridiske forslag

Utvalget fremmer enkelte forslag om tilpasning av lovgivning for å fremme samfunnets sikkerhet og beredskap.

- *Pålegge kommunene arbeid med kriseplanlegging (kapittel 24). En slik lovfestet planleggingsplikt vil i liten grad bli merket i kommuner som allerede har en tilfredsstillende beredskap. På grunn av ulike forhold må kommunene i betydelig grad selv bestemme hva en kriseplan bør inneholde. Men Staten må stille visse minimumskrav, blant annet til plan for etablering av kriseledelse og for informasjon til befolkningen og massemediene under en krisesituasjon.*
  - I Inst. S. nr. 9 (2002-2003), jf. St.meld. nr. 17 (2001-2002) Samfunnssikkerhet, støtter komiteene Regjeringens konklusjon om innføring av en generell beredskapsplikt i kommunene. Dette arbeidet blir sett i sammenheng med ny lov om Sivilforsvaret.
- *Ansvarsområdet til Politiets overvåkingstjeneste bør lovfestes (kapittel 22).*
  - De gjøremål som utføres av Politiets sikkerhetstjenestes reguleres av lov 4. august 1995 nr. 53 om politiet (politiloven) § 17 a-c. PSTs ansvar for å utarbeide trusselvurderinger fremgår av § 17 c, nr. 1.
- *Utvalget er kjent med at dette er under utredning i Justisdepartementet. Som en del av denne prosessen bør det foretas en nødvendig samordning og avklaring i forhold til lovgivningen til etterretnings- og sikkerhetstjenestene. Det bør gis lovbestemmelser som gir Politiets overvåkingstjeneste muligheter til offensiv forebyggende virksomhet, herunder kommunikasjonskontroll i forebyggende øyemed.*
  - Ulike utredningsarbeider som berører PST er avgitt. Det vises i denne sammenheng til NOU 2003:18 Rikets sikkerhet (Straffelovkommisjonens delutredning VIII), som ble avgitt i juni 2003, og utvalget som har vurdert metodespørsmål ift. forebygging, ledet av førstelagmann Odd Jarl Pedersen, jf. NOU 2004:6 Mellom effektivitet og personvern – politimetoder i forebyggende øyemed.
- *Det nåværende regelverket og beslutningsprosedyrene for bistand fra Forsvaret til politiet (og andre sivile myndigheter) i fred bør gjennomgås med sikte på at det i kritiske situasjoner overfor væpnede motstandere vil være mulig raskt å sette inn militære ressurser som støtte til politiets krisehåndtering (kapittel 5). I denne gjennomgangen vil det kunne være aktuelt med en ny drøfting av beredskapslovgivningen.*
  - Spørsmålet om Forsvarets bistand til Politiet er fulgt opp i forbindelse med drøftelsene i St.meld. nr. 39, kap. 5. Siste setningen av utvalgets forslag kan imidlertid forstås som et forslag om å gjennomgå beredskapslovgivningen totalt sett. Dette er ikke fulgt opp enda. Tilpasningen av beredskapslovene til det nye trusselbildet skjer stykkevis.
- *De mange lovene på næringsmiddelområdet bør samles i én lov (kapittel 11).*
  - Lov om matproduksjon og mattrygghet mv. (Matloven) trådte i kraft 1. januar 2004, Jfr. tidligere lover som fiskekvalitetsloven, floghavreloven, husdyrloven, plantevernmiddelloven, moltekartloven, såvareloven, gjødselvareloven, fôrvareloven, samordningsloven, kjøttproduksjonsloven, fiskesjukdomsloven og plantehelseloven. (Ikke fått enn endelig avklaring på om de gamle lovene faktisk er opphevet. Hvis de ikke er

opphevet kan det skyldes at enkelte mindre forhold fremdeles er hjemlet i de gamle lovene.)

- *Regelverket for transport av farlig gods bør evalueres (kapittel 7).*
  - Regelverket for transport av farlig gods i Norge er i samsvar med de internasjonale regelverk for slik transport, slik kravene fremstår i EØS-direktiver og internasjonale konvensjoner som Norge har tiltrådt. Utformingen av regelverkene skjer i FNs ekspertkomité for transport av farlig gods, samt i de internasjonale organisasjoner som ivaretar regelverkene (UN-ECE/IMO/ICAO). I 2001 ble det gjennomført en restrukturering av alle regelverkene i samsvar med FNs anbefalinger, og alle regelverkene er nå utformet over samme lest. Kriteriene for klassifisering, emballering og merking av farlige stoffer er de samme for land-, luft- og sjøtransport. Regelverkene er under kontinuerlig evaluering og revisjon, med en periodisitet på 2 år. Norge spiller en aktiv rolle i dette arbeidet. Siste utgave av landtransportregelverkene (ADR/RID) og luftfartsregelverket (ICAO-TI) er fra 1. januar 2005. IMDG-koden er fra 2004, men trådte i kraft 1. januar 2005.
    Det er iverksatt et forskningsarbeide nasjonalt under RISIT-prosjektet, som blant annet skal videreføre arbeidet med kartleggingen av farlig gods transporter i Norge. Dette arbeidet tar for seg det farlige godset som ble utelatt i DSBs undersøkelse, samt analyse av risikoen rundt transport av farlig gods med ferger.
- *Det bør foretas en nærmere vurdering av behovet for endringer i lover og regler, og behovet for insentiver, for å redusere samfunnets IKT-sårbarhet og styrke robusthetsnivået i kritisk infrastruktur (kapittel 6). Det er også behov for å revurdere den øvre strafferammen for datainnbrudd.*
  - Lover og forskrifter på informasjonssikkerhet er fragmentert. Til sammen er det gitt minst 26 forskrifter som inneholder helhetlige reguleringer av informasjonssikkerhet. I tillegg er det en rekke enkeltstående «datasikkerhetsbestemmelser» spredt rundt i lov- og forskriftverk.[2] De viktigste lovene i denne sammenheng er:
    - Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), 1998.
    - Lov om Schengen informasjonssystem (SIS-loven), 1999.
    - Lov om folketrygd (folketrygdloven), 1997, med ny bestemmelse om informasjonssikkerhet i § 25-16, vedtatt i 2000.
    - Lov om behandling av personopplysninger (personopplysningsloven), 2000.
    - Lov om helseregistre og behandling av helseopplysninger (helseregisterloven), 2001.
    - Forvaltningsloven § 15a (vedtatt i 2001). Gir Kongen hjemmel til å gi nærmere forskriftsbestemmelser om konkrete typer sikkerhetstiltak. Fvl § 15a inneholder ikke materielle sikkerhetsbestemmelser.
    - Lov om elektroniske signaturer (vedtatt i 2001). Har som formål å legge til rette for sikker og effektiv bruk av elektroniske signaturer.
    - Lov om elektronisk kommunikasjon §§ 2-7 og 2-10 (vedtatt 2003).
  - Juni 2003 kom Nasjonal strategi for IT-sikkerhet, med fokus på utfordringer, prioriteringer og tiltak. I strategien er det formulert forslag til en rekke tiltak på følgende områder:
    - Kritisk IT-infrastruktur
    - Regelverk for IT-sikkerhet
    - Nasjonal koordinering av IT-sikkerhet
    - Risiko og sårbarhetsanalyser
    - Klassifisering av informasjon og informasjonssystemer
    - Bevisstgjøring av alle aktører
    - Varsling og rådgivning
    - Tiltak hos leverandører av IT-produkter og –tjenester
    - Sertifisering og standarder
    - Forskning, kompetanse og utdanning
    - Elektronisk signatur/PKI
    - Internasjonalt samarbeid
  - Når det gjelder å styrke robustnivået i kritisk infrastruktur generelt så ble luftsikkerheten styrket etter innføringen av ny forskrift i mai 2004.[3] Skip og havner fikk styrket sikkerhet med innføring av EUs og FNs regler for havnesikkerhet.[4] De inneholder en rekke myndighetskrav og krav til kon-

[2] I følge professor Dag Wiese Schartum, Avdeling for forvaltningsinformatikk, UiO. Se også Nasjonal strategi for informasjonssikkerhet, juni 2003. Forsvarsdepartementet, Nærings- og handelsdepartementet og Justis- og politidepartementet.

[3] Forskrift om forebyggelse av anslag mot sikkerheten i luftfarten.

[4] The international convention for the Safety Of Life At Sea (SOLAS-konvensjonen) og International Ship and Port Facility Security Code (ISPS-koden)

krete sikkerhetstiltak som skal iverksettes om bord på skip i internasjonal fart og i havneanlegg som betjener slike skip. En kgl res om store ulykker er til høring i departementene. Disse er i første rekke av fysisk karakter. I telesektoren arbeider Post- og teletilsynet med skjerpede sikkerhetskrav til leverandørene. Dette er omtalt tidligere i dokumentet. I Forsvarsdepartementet utarbeides det nye retningslinjer for objektsikkerhet (objektsikkerhetsforskriften).

– Datakrimutvalget avga sin utredning NOU 2003:27 Lovtiltak mot datakriminalitet til Justisdepartementet 04.11.2003. Utredningen har vært på høring, og departementet tar sikte på å fremme en odelstingsproposisjon for Stortinget i løpet av 2005. Dette vil gjøre det mulig for Norge å ratifisere Europarådets konvensjon om bekjempelse av datakriminalitet. Det vil bli organisert et nytt utvalgsarbeid som får i oppgave å foreta en fullstendig gjennomgang av straffeloven og straffeprosessloven for å vurdere om det er behov for ytterligere lovendringer.

6 Forskning og utdanning

Det trengs en ny giv for norsk sikkerhetsforskning for å holde tritt med teknologi- og samfunnsutviklingen (kapittel 25).

- *Ett departement må ta et hovedansvar for at sikkerhetsforskning igangsettes, vedlikeholdes og videreutvikles. Det bør søkes løsninger som gjør at sektordepartementer med stort ansvar for sikkerhet og beredskap går sammen med næringslivet i et forpliktende «partnerskap» for et sektorovergripende forskningsprogram.*
  – Ansvar for sikkerhetsforskning i de forskjellige sektorene ivaretas ut fra ansvarsprinsippet. Justis- og politidepartementets samordnings- og tilsynsansvar for samfunnets sivile sikkerhet gir departementet et særlig ansvar for å se tverrsektorielle utfordringer. Dette har gitt seg utslag i at departementet har og har hatt en fremtredende rolle i FFIs forskning om Beskyttelse av samfunnet (BAS) siden 1994.
- *Norges Forskningsråd må innta en initierende og koordinerende rolle for å fremme sikkerhetsforskning.*
  – En utredningsgruppe nedsatt av Norges forskningsråd har utarbeidet et forslag til forskningsprogrammet SAMRISK. Programmet legger opp til å være både flerfaglig og sektorovergripende og skal bidra til å bygge kunnskap om samfunnssikkerhet på nasjonalt nivå og kvalifisere norske forskere til EU-forskning. Gruppens forslag skal innarbeides i budsjettforslaget for 2006.
- *Sikkerhet bør i større grad integreres i IKT-utdanningen på alle nivåer fra videregående skoler til universiteter. I tillegg er det behov for spesialkompetanse og at IKT-sikkerheten etableres som eget fag ved enkelte av våre universiteter og høyskoler.*
  – I nasjonal strategi for IT-sikkerhet fra juni 2003 er det foreslått tiltak. Blant annet skal det innledes et samarbeid med UFD med tanke på utarbeidelse av en undervisningspakke rettet mot grunn- og videregående skoler med fokus på informasjonssikkerhet. Status er at man avventer reformen i grunnopplæringen. Videre så har Høgskolen i Gjøvik (HiG) fått godkjenning for et Masterstudium innen informasjonssikkerhet. HiG har også etablert et tilbud på bachelor-nivå innen informasjonssikkerhet.
    Det henvises til rapport fra DSB til ISU datert 17. januar 2005 (Sårbarhet i kritisk infrastruktur – utfordringer) for oversikt over relevant forskning, herunder forskning på informasjonssikkerhet.

Vedlegg 8

Statlige styringsvirkemidler-Sikkerhet og beredskap

Statskonsult, 9. mai 2005

1 Innledning

Siden begynnelsen av 1990-tallet er en rekke statlige virksomheter skilt ut som egne selskaper. En del av disse er senere blitt privatisert. Organisering av statlig virksomhet som selvstendige selskaper legger rammer for statens styringsmuligheter og virkemiddelbruk. Når virksomhet skilles ut fra staten og organiseres som selvstendige rettssubjekter, må instruksjon og etatsstyring erstattes med andre typer styringsvirkemidler.

Dette notatet gir en oversikt over statens virkemiddelbruk på områder der det har skjedd selskapsdannelser. Notatet er utarbeidet av Statskonsult på oppdrag fra Utvalg for sikring av landets kritiske infrastruktur. Notatet bygger på tidligere arbeider i Statskonsult. I forbindelse med utarbeidelsen av notatet har vi sett nærmere på hvilke virkemidler som brukes for å ivareta sikkerhets- og beredskapshensyn. Vi har i denne sammenheng sett på virkemiddelbruken innenfor følgende sektorer: kraft, legemiddel, tele og luftfart. Notatet gir en beskrivelse av virkemiddelbruken så langt det har latt seg gjøre med den tiden som har stått til disposisjon, og vi har ikke innhentet synspunkter på eller gjort noen egen vurdering av begrunnelser for valg av virkemidler eller for virkemidlenes kvalitet og funksjonalitet.

2 Statlige styringsvirkemidler

De statlige virkemidlene kan grupperes på følgende måte:

- Juridiske, for eksempel lover, forskrifter, konsesjoner, lisenser, prisreguleringer
- Økonomiske, for eksempel tilskudd, kjøp av varer og tjenester, skatter og avgifter
- Organisatoriske, for eksempel utskilling av kommersielle enheter, selskapsdannelser og etablering av tilsynsorganer
- Pedagogiske, for eksempel informasjon, øvelser og opplæring.

I tillegg til disse generelle virkemidlene, kommer mulighetene for eierstyring der det er heleide statlige selskaper. I praksis er det ikke alltid like lett å klassifisere de ulike virkemidlene i tråd med en slik inndeling. Det er også slik at virkemidler fra forskjellige kategorier påvirker hverandre direkte. For eksempel vil bruken av økonomiske eller organisatoriske virkemidler være regulert av et lov- eller regelverk. Vi finner det likevel hensiktsmessig å operere med et analytisk skille mellom ulike typer virkemidler for å skape en mer oversiktlig framstilling.

3 Juridiske virkemidler

Lov og regelverk er sentralt i reguleringen av ulike samfunnsområder og for å nå viktige samfunnsmål. Regelverket normerer og angir andre virkemidler som kan eller skal nyttes på en sektor, og det angir hvordan virkemidlene skal innrettes. Juridiske eller rettslige virkemidler er sentrale for å ivareta samfunnspolitiske målsettinger, på sektorer der det har skjedd en selskapsdannelse.

Staten benytter ulike rettslige virkemidler for å nå politiske målsettinger. Viktige i denne sammenhengen er blant annet:

- Lover og forskrifter
- Konsesjoner
- Reguleringer: for eksempel prisreguleringer og regulering av markedsadgang og eierskap
- Vedtekter (omtalt i forbindelse med eierstyring i avsnitt 7)

3.1 Lovgivning

Alle offentlige og private bedrifter reguleres av en rekke forskjellige og *generelle lover*. Det kan være lover som regulerer arbeidsrettslige forhold, arbeidsmiljøet, forholdet til det eksterne miljøet og lignende. Det er i tillegg en rekke lover som regulerer enkeltområder eller sektorer av samfunnet. Det er ikke noe klart og stringent skille mellom det vi kan kalle *generell lovgivning* og *sektorlovgivning*.

Sektorlovgivningen regulerer et bestemt område av samfunnet eller produksjonen av en bestemt tjeneste, og vil derfor i hovedsak ha betydning for aktørene innenfor det aktuelle området. Eksempler kan være energi-, kringkastings-, jernbane- og luftsfartslovene og lov om elektronisk kommunikasjon. Lovgivningen på de nevnte sektorene er alle blitt endret i løpet av de siste 10 til 15 årene i forbindelse med selskapsdannelser og liberalisering av sektorene og erfaringene med dette. Lovgivningen kan fastsette formål, men regulerer i stor grad gjennom myndighet til å gi konsesjoner og tillatelser til å utøve virksomhet og ved bestemmelser om kontroll og tilsyn. Både generell lovgivning og sektorlovgivning er viktige styringsformer.

Sikkerhet og beredskapshensyn

Lovregulering er et viktig virkemiddel for å ivareta sikkerhets- og beredskapshensyn og en rekke forhold på området reguleres gjennom lov eller forskrift. Gjennom lovverket gis hjemmel for bruk av andre virkemidler på området, både organisatoriske (som etablering av tilsyn og komiteer) og økonomiske (avgifter og gebyrer.)

Telesektoren

§ 2-10 i lov om elektronisk kommunikasjon omhandler sikkerhet og beredskap. Loven omhandler tilbyders ansvar for å tilby nett med nødvendig sikkerhet for brukerer i «fred, krise og krig». Loven gir myndighetene hjemmel til å pålegge tilbyder spesielle tiltak, bl.a.:

- utarbeide beredskapsplaner og bidra i beredskapsøvelser
- innføring av spesielle funksjoner i systemene
- fysisk sikring av installasjoner

Loven omtaler også hvordan utgifter til sikkerhets- og beredskapstiltak skal dekkes inn. Tilbyder skal i utgangspunktet dekke kostnader ved sikkerhets- og beredskapstiltak etter denne paragrafen. Tilbyderes reelle merkostnader forbundet med levering av sikkerhets- og beredskapstiltak, skal kompenseres av staten.

Loven åpner for å nekte tilbyder tilgang til markedet dersom dette er nødvendig av hensyn til offentlig sikkerhet, helse eller andre særlige forhold.

Energisektoren

Kap. 6 i energiloven omhandler beredskap. I loven vises det til at kraftforsyningen under beredskap og i krig skal underlegges Kraftforsyningens beredskapsorganisasjon. Organisasjonen består av de enheter som står for kraftforsyningen i fred. Olje- og energidepartementet skal samordne beredskapsplanleggingen og lede kraftforsyningen under beredskap og i krig. Organisasjonen kan også pålegges oppgaver i fred.

Loven gir hjemmel for å pålegge sikringstiltak ved anlegg over en viss størrelse (av betydning for landets kraftforsyning). Aktørene kan pålegges for egen regning å sette i verk de sikringstiltak som departementet i hvert enkelt tilfelle finner påkrevd, ved vesentlige utgifter kan det gis kompensasjon. Utgiftene kan i visse tilfeller pålegges helt eller delvis bruker. Det er meldeplikt i forbindelse med utbygging eller ombygging for å få fastsatt de sikringstiltak som skal gjøres ved anlegget.

Luftfartssektoren

Sikkerheten i luftfarten har vært et viktig tema i alle år og er ikke blitt mindre viktig de siste årene. Luftfartsloven regulerer en rekke forhold som har betydning for sikkerhet og beredskap i luftfarten. Det internasjonale regelverket er omfattende og Norge må i stor grad tilpasse seg dette regelverket. Et eksempel er forskrift om sikkerheten ved norske lufthavner som ble vedtatt i 2004. Den nye forskriften er i tråd med EUs regelverk og inngår i EØS-avtalen. Dette regelverket betyr at det blir innført krav som gjelder blant annet følgende:

- Samme sikkerhetsnivå for alle lufthavner i EU, slik at det ikke skilles mellom innenlands- og utenlandstrafikk når det gjelder. sikkerhetskontroll av passasjerer, håndbagasje og innsjekket bagasje. Det skilles heller ikke mellom offentligeide og privateide lufthavner.
- Felles europeiske regler for frakt av gods, medregnet post.
- Sikkerhetskontroll av alle personpasseringer, medregnet flybesetning og av varetransport inn til «flyside eller avsperret område».
- Mer omfattende fysisk sikring av lufthavnene, for eksempel ved inngjerding og vakthold.
- Systematisk opplæring og godkjenning av personell som arbeider med sikkerhet.

Legemidler

Forsyningen av legemidler og helsemateriell er ifølge St.prp. nr. 1 (2004-2005) fra Helse- og omsorgsdepartementet sårbart overfor leveransesvikt eller ved behov for uventet økt forbruk. Ifølge Sosial- og helsedirektoratet har grossistene og apotekene i gjennomsnitt en beholdning på om lag tre

ukers forbruk. Helse- og omsorgsdepartementet har nettopp lagt fram en Stortingsmelding om legemidler.

Legemiddelberedskap ivaretas først og fremst gjennom helse- og sosialberedskapsloven med tilhørende forskrifter. Generelt vil imidlertid lovgivning for å sikre tilgjengelighet også være en form for beredskap – dette gjelder både på grossist- og på detaljistleddet.

Statens legemiddelverk kan pålegge den enkelte grossist å holde et beredskapslager av nødvendige legemidler og medisinsk forbruksmateriell, jf. §5 i *Forskrift om grossistvirksomhet med legemidler*.

HOD kan gi forskrift om hvilke varer et apotek alltid skal ha på lager og stille minstekrav til leveringsgrad for legemidler, jf. apotekloven § 5-4 fjerde ledd. Denne hjemmelen er ikke benyttet pr. idag. Departementet kan også gi forskrift om at apotek, grossister og tilvirkere av legemidler skal ha plikt til å utarbeide beredskapsplan for virksomheten, eventuelt at virksomhetene skal inngå i beredskapsplanene til kommuner, regionale helseforetak og helseforetak. Heller ikke disse hjemlene er benyttet ennå.

3.2 Konsesjoner

En konsesjon er en tillatelse eller løyve fra offentlige myndigheter. Å få tildelt konsesjon medfører nærmere fastsatte rettigheter og/eller plikter som både kan være positivt og negativt formulert. Konsesjoner kan ha svært ulik utforming fra sektor til sektor. Konsesjonens innhold vil ofte innebære koblinger til andre virkemidler. Muligheten til å gjøre bruk av konsesjoner må være hjemlet i lov. Regelverket på en gitt sektor gir ofte rammer for innhold og vilkår som settes i konsesjonene.

Konsesjoner er viktige virkemidler i styringen av sektorer som har vært igjennom en markedseksponering og fristilling av statlig virksomhet. Konsesjoner benyttes innenfor mange områder, men det er betydelige forskjeller med hensyn til hvordan de er innrettet og på hvilke krav som kan stilles til konsesjonsinnehaver. Konsesjonsbetingelsene kan variere fra enerett og plikt til å utføre samfunnspålagte oppgaver, til å regulere hvem som skal få rett til innpass på et marked (kvalitetssikring) og enkelte forpliktelser knyttet til dette.

Sikkerhet og beredskap

Konsesjoner er et virkemiddel som benyttes på de sektorene som vi har sett på. Det virker ikke som konsesjon benyttes som virkemiddel for å pålegge virksomheter spesielle sikkerhets- og beredskapsoppgaver. Konsesjonen kan imidlertid innebære en kvalitetssikring av aktørene som kan være viktig i en sikkerhetssammenheng.

Ytelser til totalforsvaret omtales ofte som «spesielle samfunnspålagte oppgaver». Slike plikter kan pålegges en operatør gjennom konsesjon. Spesielle samfunnspålagte oppgaver inngikk tidligere i Telenors konsesjon på fasttelefoni og Telenors merkostnader ble dekket av staten gjennom kjøp av tjenester.

3.3 Enerett- og monopolordninger

Formelle enerettsområder eller monopoler er regulert gjennom lovgivning. Monopoler vil vanligvis være begrunnet ut fra hensynet til å nå samfunnsmessige mål ved utnyttelse av stordriftsfordeler. På de områdene vi har sett på er det monopol på deler av oppgavene/nettet. Monopol eller enerett blir i liten grad trukket fram som et virkemiddel som er spesielt viktig i forhold til sikkerhet.

4 Organisatoriske virkemidler - tilsynsorganer

Det er i dag nærmere 40 statlige organer som fører tilsyn med at private og offentlige aktører i Norge holder seg innenfor regler fastsatt i lover og forskrifter. Områdene det føres tilsyn med, spenner fra produktkvalitet og arbeidsmiljø til transportsikkerhet, mediemangfold og konkurranse. I en forvaltningspolitisk utvikling der virksomheter flyttes ut av staten og der det legges vekt på delegering, ser vi at styring med vekt på forhåndskontroll, blir erstattet av styring gjennom etterkontroll, rapportering og evaluering. I en slik utvikling får tilsynene en viktig rolle i å kontrollere at tjenester blir utført i henhold til fastlagte krav.

I forbindelse med at statlige forvaltningsorganer eller forvaltningsbedrifter er blitt omdannet til selvstendige selskaper eller foretak, er det blitt etablert egne tilsynsorganer som har et ansvar for tilsyn og kontroll innenfor sektoren. Tidligere var tilsynsvirksomheten ofte en integrert del av forvaltningsorganet eller forvaltningsbedriften. Det legges stor vekt på at tilsynene skal ha faglig og organisatorisk selvstendighet. I flere tilfeller er skillet mellom statens ulike funksjoner blitt forsterket ved at tilsynsorganet er underlagt fagdepartementet, mens eieransvaret for selskapet er overført til Nærings- og handelsdepartementet. Dette gjelder blant annet for Statkraft og Telenor. I stortingsmeldingen om tilsyn er det lagt stor vekt på hensynet til uavhengighet og rolleklarhet og på

hensynet til faglig kvalitet i tilsynene. Det legges opp til at det på flere områder skal foretas en lovmessig avskjæring av statsrådenes instruksjonsrett og at klager på tilsynenes vedtak skal behandles i uavhengige klagenemnder.

I noen tilfeller ligger eieransvar, faglig ansvar og tilsynsansvar fortsatt i samme departement. Dette er hovedsakelig på områder der virksomhetene i betydelig grad er faglig og/eller formålsmessig definert. Det gjelder blant annet for NRK, Statnett og Posten Norge.

Tilsynenes arbeidsoppgaver omfatter blant annet utarbeidelse av forskrifter, behandling av konsesjons- og dispensasjonssøknader, direkte inngrep, kontroller og aktivt forbedringsarbeid overfor dem man fører tilsyn med.

Sikkerhet og beredskap

Tilsynene har en sentral rolle i myndighetenes arbeid for å ivareta sikkerhet og beredskap på sektorer der det har skjedd selskapsdannelser.

Telesektoren

Post- og teletilsynet har et myndighetsansvar for telesikkerhet og -beredskap innenfor telesektoren. Ansvaret omfatter blant annet følgende områder:

- Sette krav til telesikkerhet og teleberedskap.
- Forestå ulike former for forebyggende og skadebøtende tiltak for å gjøre telenettene mer robuste
- Føre tilsyn med at pålagte tiltak blir iverksatt.
- Bevisstgjøring, kompetanseheving og veiledning overfor operatører, brukere og andre aktører.

Post- og teletilsynet er tildelt ansvaret for forvaltning av statlige tilskudd på området.

TRISTI - totalforsvarets råd for sikring av tele- og informasjonssystemer er rådgivende organ for Samferdselsdepartementet. Post- og teletilsynet er sekretariat for rådet.

Kraftsektoren

Norges vassdrags- og energidirektorat (NVE) har ansvaret for å samordne beredskapsplanleggingen, og skal lede landets kraftforsyning under beredskap og i krig. For dette formål er det etablert en landsomfattende organisasjon - Kraftforsyningens beredskapsorganisasjon (KBO) - bestående av NVE og de virksomheter som står for kraftforsyningen. Dette omfatter alle enheter som eier eller driver kraftproduksjon med tilhørende vassdragsregulering, overføring og distribusjon av elektrisk kraft og fjernvarme.

Når KBO ved krigsberedskap overtar ansvaret for landets kraftforsyning, plikter alle kraftforsyningsenheter å rette seg etter direktiver fra overordnet myndighet i KBO. Dette medfører ingen endring i selskapenes eierforhold.

KBO skal kunne løse oppgaver i fred ved skade på kraftanlegg som følge av naturgitte forhold, teknisk svikt, terror- eller sabotasjeaksjoner, samt i forbindelse med rasjonering etter energiloven.

Luftfartssektoren

Luftfartstilsynet ble opprettet 1. januar 2000. Luftfartstilsynets oppgaver ble tidligere utført av Luftfartsinspeksjonen, som var en del av Luftfartsverket. EUs regelverk setter ikke spesifikke krav til organisering av tilsynsfunksjoner innen luftfart.

Luftfartstilsynets oppgaver er primært knyttet til sikkerhet i luftfarten. Tilsynet har det overordnede ansvar blant annet for å fastsette forskrifter, drive kvalitetskontroll av materiell og utstede sertifikater til flyselskaper, verksteder, piloter og kabinpersonell, samt godkjenne Avinors virksomhet. I tillegg skal etaten føre tilsyn med at lover og forskrifter etterleves.

Legemidler

Etter omorganiseringen av den sentrale helseorganiseringen fom. 01.01.02, har Helsetilsynet i fylkene og Statens helsetilsyn (fortsatt) ansvar for tilsyn med tilsynsoppgavene knyttet til legemidler. Beredskap er ikke eksplisitt omtalt i loven.

5 Økonomiske virkemidler

Økonomiske virkemidler kan være fastsettelse av *avgifter og gebyrer, statlig kjøp av tjenester, tilskudd, lån og garantier.* Avgifter eller gebyrer kan brukes for å sikre at sektorpolitiske hensyn blir ivaretatt. På sektorer med markedsorganisering, kan staten kjøpe tjenester fra private og/eller offentlige tjenesteleverandører på mer avgrensede felt der det kan oppstå markedssvikt. Tilskudd/kjøp av tjenester kan også benyttes for å etablere eller opprettholde et tjenestetilbud når dette ikke er bedriftsøkonomisk lønnsomt.

5.1 Avgifter og gebyrer

Avgifter er et mye brukt statlig virkemiddel. Bruken av avgifter på de områdene som er aktuelle her, kan ha ulike begrunnelser eller formål:

– En del avgifter er begrunnet ut fra statsfinansielle hensyn og vil i hovedsak ha som formål å skaffe inntekter til statskassen.
– Noen avgifter er begrunnet med at de skal fungere som betaling for ytelser på området. Nivået er satt for å dekke utgiftene og for å regulere prisnivået, slik at alle kan betale.
– Andre avgifter kan ha en spesifikk sektorpolitisk betydning. Et typisk eksempel er særavgiften på omsetning av alkohol, som primært er et virkemiddel for å begrense alkoholforbruket i befolkningen. Et annet eksempel er miljøavgifter, blant annet avgiften på utslipp av karbondioksyd.

Et viktig poeng med avgifter som styringsvirkemiddel, er nettopp at det i stor grad er brukere av tjenestene eller markedsaktørene som betaler. På enkelte områder vil dette være formålstjenlig og et forsøk på direkte styring av for eksempel omfang eller tilgjengelighet. Dette ser vi blant annet ved at avgifter på flytrafikk delvis er knyttet til miljøhensyn.

Begrepene gebyrer og avgifter går noe over i hverandre. Men mens avgifter har en mer generell karakter, vil gebyrer ofte være koblet direkte til bruk og finansiering av en konkret tjeneste.

Sikkerhet og beredskap

Tilsynsvirksomhet finansieres helt eller delvis gjennom gebyrer eller avgifter fra brukerne. Dette gjelder også tilsynenes virksomhet innenfor sikkerhet og beredskap. Dette gjelder blant annet Luftfartstilsynet som tar gebyrer for godkjenning og tilsyn med luftfartøy, flyselskaper, verksteder og lufthavner. Post- og teletilsynet er finansiert ved gebyrer og tilsynets ordinære oppgaver innenfor sikkerhet og beredskap vil dekkes av dette.

På kraftområdet kan departementet i henhold til energiloven bestemme at det skal utlignes gebyr til dekning av utgiftene ved beredskapsmyndighetens arbeid med kraftforsyningsberedskap. Utgiftene utlignes på eiere og brukere av de aktuelle anleggene.

5.2 Kjøp av tjenester - tilskudd

Staten kan kjøpe tjenester fra, eller gi tilskudd til, virksomheter for å opprettholde et tilbud av tjenester som ikke kan drives bedriftsøkonomisk lønnsomt, og som det er av samfunnsmessig interesse å opprettholde. Slike tjenestekjøp kan skje gjennom en anbudsrunde eller ved direkte kjøp. Anbud innebærer at det avholdes konkurranse om retten til å levere en vare eller tjeneste. På sektorer som er liberalisert vil det vanligvis brukes anbudskonkurranser. Dersom det bare er en aktuell leverandør eller det er andre tungtveiende hensyn kan staten benytte direkte kjøp.

Staten kjøper tjenester direkte fra blant andre Posten Norge, Avinor og NSB for å opprettholde tjenester i distriktene eller av miljømessige grunner. Statskog betales for utføringen av sin myndighetsutøvende virksomhet. I forbindelse med slike kjøp, spesifiseres det hva som skal leveres og til hvilken pris.

Sikkerhet og beredskap

Tilskudd eller kjøp av tjenester benyttes i noen grad for å ivareta sikkerhets- og beredskapshensyn. Samferdselsdepartementet kjøpte i flere år tjenester knyttet til sikkerhet og beredskap direkte fra Telenor. Forvaltningen av dette tilskuddet er nå overført til Post- og teletilsynet. Også på legemiddelområdet er det skjedd en delegering av dette ansvaret fra departementet til underliggende organ.

Bruk av anbudskonkurranser for å ivareta sikkerhets- og beredskapsoppgaver har vært vurdert både på legemiddelområdet og på telesektoren. I St.meld. nr 47 (2000-2001) skrev Samferdselsdepartementet følgende om dette:

«Prinsipielt er det intet til hinder for at andre aktører kan konkurrere også om å levere de tjenestene som omfattes av USO-forpliktelsen, eller utføre spesielle samfunnspålagte oppgaver. I et etablert og velfungerende marked kan det være hensiktsmessig og effektivitetsfremmende å la flere aktører konkurrere om samfunnsoppgavene. En forutsetning for å innføre konkurranse om disse oppgavene vil imidlertid være at flere aktører har opparbeidet betryggende evne til å ivareta oppgavene på en tilfredsstillende og kontinuerlig måte i hele eller deler av landet.»

Legemidler

Sosial- og helsedirektoratet inngikk i januar 2003 en avtale med NMD grossisthandel AS (tidligere Norsk Medisinaldepot[1]) om et beredskapslager av medisiner. Avtalen skal sikre forsyningsberedskapen og omfatter lagring, rullering og utskiftning av et definert antall legemidler. Avtalen gjelder for to år

[1] Norsk medisinaldepot hadde fram til begynnelsen av 1990-tallet monopol på grossistleddet i legemiddelomsetning. Monopolet ble avskaffet som en konsekvens av EØS-avtalen. NMD ble fra 1997 gradvis privatisert og staten har solgt ut alle sine aksjer.

med en opsjon på ytterligere en to års forlengelse. Ifølge HOD utgjør lageret en begrenset beredskapsressurs. Departementet har nylig lagt fram en stortingsmelding om legemiddelpolitikken.

(Daværende) SHD inngikk i 2001 treårige avtaler med Norsk Medisinaldepot (nåværende NMD grossisthandel AS) og Apokjeden AS om sikring av apotekdrift i kommuner som kun hadde ett apotek. Disse avtalene ble forlenget fram til 01.07.05 i påvente av stortingsmeldingen.

6 Pedagogiske virkemidler

Pedagogiske virkemidler omfatter et forholdsvis vidt spekter av virkemidler som kan ha til hensikt å informere, lære opp eller bevisstgjøre befolkningen eller bestemte målgrupper. De pedagogiske virkemidlene har ikke vært spesielt fremtredende på sektorer der det har skjedd selskapsdannelser eller avvikling av statlige monopoler. Dette betyr imidlertid ikke at de ikke blir benyttet. Blant annet er informasjon om leverandører og priser et virkemiddel som blir brukt for å få markedene til å fungere bedre. Et eksempel på dette er Konkurransetilsynets offentliggjøring av strømpriser. Post- og teletilsynet er blir bedt av departementet om å gjøre tilsynets årlige telestatistikk lett tilgjengelig for forbrukerne, slik at de enklere skal kunne orientere seg i markedet.

Sikkerhet og beredskap

Virkemidler som hører inn under kategorien pedagogiske virkemidler ser ut til å være forholdsvis viktige på sikkerhets- og beredskapsområdet. Virkemidler som beredskapsplaner og beredskapsøvelser er viktige og i flere tilfeller er det nedfelt i lovverket at det kan pålegges aktørene å utarbeide beredskapsplaner og å gjennomføre beredskapsøvelser. Opplæring av personell er sentralt når det gjelder sikkerhet og beredskap, ref forskrift til luftfartsloven. Post- og teletilsynet har blant sine oppgaver å bidra til bevisstgjøring, kompetanseheving og veiledning overfor operatører, brukere og andre aktører og å arrangere felles øvelser mellom operatørene. Informasjon til befolkningen er også et virkemiddel som benyttes for å ivareta sikkerhet og beredskap.

7 Eierstyring

Regjeringen og departementet har en generell myndighet til å instruere alle virksomheter som er organisert innenfor staten (forvaltningsorganer). Dette betegnes gjerne som etatsstyring. Når en virksomhet er organisert som selvstendig rettssubjekt, kan ikke departementet benytte instruksjon, og må i stedet styre gjennom andre virkemidler eller gjennom eierstyring. Instruksjonsmyndigheten kan i prinsippet benyttes på en omfattende og lite regulert måte. At staten i stedet for må benytte eierposisjonen, legger mer begrensninger på styringens form og innhold. I heleide statlige selskaper omfatter eierstyringen følgende:

- fastsetting av vedtekter og formålsparagraf
- oppnevning av styret i virksomheten
- at statsråden i eierdepartementet er generalforsamling/foretaksmøte
- at generalforsamling/foretaksmøte kan fatte vedtak som instruerer styret
- fastsetting av avkastingskrav/utbytte

Styrene for heleide statlige aksjeselskaper og for statsforetakene oppnevnes av generalforsamlingen eller foretaksmøtet, som for disse selskapene vil si statsråden. Bortsett fra kravet til ansattes representasjon, er det få formelle krav til styresammensetning.

Det er den sittende statsråden i det departementet som forvalter eierskapet som er generalforsamlingen/foretaksmøtet i selskapet. Statsråden utøver dermed den øverste myndigheten i selskapet. I statsforetaksloven er det presisert at departementets myndighet i selskapet ikke kan utøves utenom foretaksmøtet. Det samme følger av aksjeloven for statsaksjeselskapene.

Aksjeloven tillegger styret et selvstendig ansvar for utbyttepolitikken i og med at det «ikke kan besluttes utdelt høyere utbytte enn styret foreslår». For statsaksjeselskap og statsforetakene ligger imidlertid utbyttemyndigheten hos generalforsamlingen eller foretaksmøtet.

Bruk av eierstyring for å ivareta sektorpolitiske mål kan komme i konflikt med ønsket om at virksomheten skal baseres på forretningsmessige prinsipper. Flere arbeider i regi av Statskonsult viser at eierstyring i liten grad brukes for å nå sektorpolitiske mål. De viser også at staten gjennomgående er forsiktig med å instruere sine selskaper og at staten følger de formelle spillereglene.

Ved å bruke myndigheten til å fastsette vedtekter for virksomhetene kan staten som eier bidra til å tilpasse organisasjonsformene til de særlige behov som virksomhetene måtte ha. Et statsaksjeselskap kan for eksempel ha en bestemmelse i vedtektene om en mer omfattende kontakt mellom selskap og eier enn aksjeloven krever. Flere norske statsaksjeselskaper har en slik § 10 i vedtektene.

Paragrafen sier at «alle saker som antas å være av vesentlig, prinsipiell, politisk eller samfunnsmessig betydning» skal forelegges generalforsamlingen. Styrene i selskaper med denne bestemmelsen skal hvert år legge frem en plan for virksomheten for generalforsamlingen der forhold som kommer inn under § 10 skal omtales. I tillegg skal departementene rapportere om selskapenes virksomhet til Stortinget i egen melding annet hvert år. Det er få eksempler på at slike rapporteringer har ført til instruksjon av styret.

Statsforetakslovens paragraf § 23 andre ledd, er en parallell til § 10 i vedtektene for statsaksjeselskapene, men innebærer en noe mer omfattende rapporteringsplikt. Bestemmelsen gir styret i statsforetaket en plikt til å legge frem saker av vesentlig betydning eller saker som vil endre virksomhetens karakter for eier. Dersom eier ønsker å gripe inn i en slik sak, må det skje gjennom foretaksmøtet. Etter statsforetakslovens § 24 tredje ledd, skal styreprotokollene i statsforetakene sendes eier innen to uker etter styremøtet.

Sikkerhet og beredskap

Hensynet til sikkerhet og beredskap kan være ett (av flere) argument for statlig eierskap, for valg av selskapsform og for at statens eierinteresser skal forvaltes av sektordepartementet og ikke av Nærings- og handelsdepartementet. I en normalsituasjon vil dette ikke nødvendigvis virke inn på eierstyringen, men eierstyring gir andre styringsmuligheter enn dem som følger av de generelle regulatoriske virkemidlene. Behovet for en slik styringsmulighet kan endres over tid, og kan også anses som en sikkerhetsforanstaltning for mulige situasjonsbestemte styringsbehov.

Energisektoren

En av begrunnelsene for valg av statsforetaksformen for Statnett var hensynet til sikkerhet og beredskap. Systemansvaret for kraftnettet er viktig blant annet for å ivareta interesser knyttet til forsyningssikkerhet. I tillegg til det årlige foretaksmøtet avholdes det eiermøter eller kontaktmøter med Statnett to ganger i året. Disse møtene benyttes ikke til instruksjon eller eierstyring, men er i følge partene viktige for informasjonsutveksling.

Luftfartssektoren

Omdanningen av Luftfartsverket til selskap var begrunnet ut fra hensynet til økonomi og fleksibilitet og virksomhetens samfunnsmessige rolle og forpliktelser ble ikke endret. I forbindelse med etableringen av Avinor AS, skrev Samferdselsdepartementet i St. prp. nr.1 at «myndighetenes eierstyring av Luftfartsverket AS vil være et viktig virkemiddel for å sikre de overordnede luftfartspolitiske målsettingene.» Departementet mente videre at Avinors samferdselspolitiske rolle tilsa at det nye aksjeselskapet ble lagt under Samferdselsdepartementet. Avinor har den såkalte § 10 i vedtektene som tilsier at selskapets styre hvert år skal legge fram en plan for virksomheten for samferdselsministeren i egenskap av selskapets generalforsamling. Styrets planer vil danne grunnlag for regelmessige meldinger til Stortinget om virksomheten. Saker av vesentlig samfunnsmessig eller prinsipiell betydning skal legges fram for samferdselsministeren.

8 Riksrevisjonens kontroll

I sum vil en kombinasjon av bruk av mange styringsvirkemidler overfor et selskap gi en omfattende myndighetsstyring. Når det gjelder selskapskontrollen, er Riksrevisjonens oppgave å kontrollere at statsrådene forvalter statens interesser på en lovlig og økonomisk forsvarlig måte, og i samsvar med de vedtakene og forutsetningene som Stortinget har angitt. Den løpende regnskapsrevisjonen er derimot ikke Riksrevisjonens oppgave. Hovedprinsippene for selskapskontrollen er nylig vurdert og foreslått videreført i utkastet til ny lov og instruks.

Stortinget behandlet den 25. februar 2003 Dokument nr. 3:2 (2002–2003) Riksrevisjonens kontroll med statsrådens (departementets) forvaltning av statens interesser i selskaper, banker med videre for 2001, jf. Innst. S. nr. 123. (2002–2003). Stortinget besluttet da å utvide Riksrevisjonens kontroll til også å gjelde oppgaver av ikke-økonomisk art, for eksempel oppgaver knyttet til bredere samfunnsinteresser, sektorpolitikk eller andre oppgaver som er pålagt av Stortinget som ledd i selskapskontrollen.

Litteraturliste

Stortingsdokumenter:

St.meld. nr. 17 (2002–2003) *Om statlige tilsyn*.
St.prp. nr. 1 (2004-2005) *Helse- og omsorgsdepartementet*
St.meld. nr. 18 (2004-2005) *Rett kurs mot riktigere legemidler – legemiddelpolitikken*
St.meld. nr. 47(2000-2001) *Om telesikkerhet og beredskap*

Ot.prp.nr. 40 (2003-2004) *Om lov om endringer i lov 11. juni 1993 nr. 101 om luftfart (luftfartsloven)*
St.prp.nr. 1 (2002 –2003) *Samferdselsdepartementet - Tillegg 2*

Annet:

NOU 2003:34 *Mellom stat og marked – selvstendige organisasjonsformer i staten*

Dokument nr. 3:2 (2002–2003) Riksrevisjonens kontroll med statsrådens (departementets) forvaltnings av statens interesser i selskaper, banker med videre for 2001, jf. Innst. S. nr. 123 (2002–2003).

Lover:

Lov om statlig tilsyn med helsetjenester (LOV 1984-03-30 nr. 15)

Lov om helsemessig og sosial beredskap (LOV 2000-06-23 nr. 56)

Forskrift om grossistvirksomhet med legemidler (FOR 1993-12-21 nr. 1219)

Forskrift om krav til beredskapsplanlegging og beredskapsarbeid mv. (FOR-2001-07-23-881)

Lov om luftfart (luftfartsloven) LOV-2004-06-11-35

Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven) LOV-2003-12-19-131

Lov om elektronisk kommunikasjon (ekomloven) LOV-2004-03-05-12

Nettsteder:

www.odin.no
Post- og teletilsynet www.npt.no
Luftfartstilsynet www.luftfartstilsynet.no
Norges vassdrags- og energidirektorat
www.nve.no

Statskonsultrapporter:

Rapport 1998:21 *I godt selskap*

Rapport 1999:16 *Statlig eierskap og sektorstyring.*

Rapport 2001:19 *Virkemiddelbruk og sektorstyring*

Vedlegg 9

Rammeverk for gjennomføring av risiko og sårbarhetsanalyser av samfunnskritisk infrastruktur

Terje Aven, Hermann Steen Wiencke. SEROS Senter for risikostyring og samfunnssikkerhet

1 Innledning

I mandatet til Utvalg for sikring av kritisk infrastruktur står det at utvalget skal vurdere hvordan hensynet til rikets sikkerhet og vitale nasjonale interesser på best mulig måte kan ivaretaes ovenfor virksomheter som ikke er offentlige. Eksempler på områder som utvalget skal vurdere er, kraftsektoren, telesektoren, vannforsyning m.m. Utvalgets arbeid skal omfatte alle typer installasjoner og systemer som er nødvendig for at samfunnet skal fungere tilnærmet normalt.

Dette innebærer bla. at utvalget skal kartlegge de virkemidler som brukes for å sikre rikets sikkerhet og vitale nasjonale interesser når offentlige virksomheter privatiseres, og utvalget skal kartlegge virksomheter som antas å ha betydning for rikets sikkerhet og vitale nasjonale interesser.

Privatisering av samfunnskritisk infrastruktur, globalisering av økonomien, raske teknologiske endringer og nye organisasjonsformer gjør samfunnet generelt mer sårbart i forhold til trusler som kan påvirke stabilitet og opprettholdelse av viktige samfunnsfunksjoner. Dermed vil endringer i trusselbildet, for eksempel i forhold til terrorisme, organisert kriminalitet, naturskapte hendelser osv. skape stor usikkerhet omkring samfunnets evne til å fungere i ulike situasjoner.

Hvordan kan vi styre en slik utvikling, hvordan kan vi styre samfunnssikkerheten og den risiko viktige funksjoner i samfunnet utsettes for?

Lover, regler og internasjonale standarder er virkemidler som myndigheter og det internasjonale samfunn bruker i dette arbeidet. SEVESO direktivet, BASEL II, og Petroleumstilsynets nye regelverk er eksempler på regelverk som er tiltenkt å virke mot en del av det trusselbildet samfunnet står ovenfor.

I forhold til truslene mot samfunnskritisk infrastruktur er det per i dag ikke et helhetlig lovverk som ivaretar samfunnets interesser. Med helhetlig lovverk mener vi her et lovverk som både omfatter offentlige og private virksomheter og som omhandler helheten i det trusselbildet samfunnet står ovenfor, dvs både villede hendelser, ulykker og naturskapte hendelser. I dag har vi bla sikkerhetsloven men den gjelder bare offentlige virksomheter og er bare fokusert mot deler av det trusselbildet som et slikt lovverk bør ivareta.

Et nytt helhetlig lovverk ønskes etablert, der det stilles krav til at alle virksomheter som har ansvaret for samfunnskritisk infrastruktur, har kontroll på sin virksomhet, de sårbarheten den har og den risiko dette utgjør for samfunnet. Et slikt lovverk vil omfatte enkeltvirksomheter, men vil også stille krav til at det gjøres mer overordnede vurderinger på tvers av enkeltvirksomheter og sektorer. Slike vurderinger vil spesielt se på avhengigheter imellom ulike systemer, og omfatte risiko i forhold til alle typer trusler, dvs villede handlinger, ulykker og naturskapte hendelser.

I utredningen av et slikt lovverk må også et hensiktsmessig tilsynsapparat etableres. Sentralt her står spørsmålet om styrket samordning av tilsynsvirksomheten.

Et slikt lovverk må bygge på en del grunnleggende prinsipper. Det er ikke opplagt hvordan man skal »styre» samfunnssikkerheten og den risiko viktige funksjoner i samfunnet utsettes for. I dette notatet gis et innspill i arbeidet med å etablere slike prinsipper. Vi gjør dette ved å foreslå et rammeverk og et teoretisk fundament for hvordan den enkelte virksomhet (bedrift, kommune, fylkeskommune, sektor, nasjon) skal kunne kartlegge og overvåke det gjeldende trussel- og risikobildet, og dermed få et styrket underlag for å kunne håndtere sårbarhetene og risikoforholdene i virksomheten. Innspillet er i stor grad basert på det arbeidet som SEROS har utført i BAS 5 prosjektet.

2 Bruk av Risiko- og Sårbarhets-analyser i samfunnet

Utgangspunktet for bruken av rammeverket vil være ulike situasjoner og behov. Vi har i dette notatet gjort en inndeling av ulike nivåer der ROS-analyser bør gjennomføres. Hensikten med en slik gruppering er å synliggjøre ulike situasjoner og behov. Følgende inndeling er foreslått:

- Enkeltvirksomheter
- Fylke/kommune
- Nasjon

Enkeltvirksomheter:

En virksomhet, for eksempel et vannverk, vil ønske å kartlegge hendelser/forhold som kan gjøre at leveranser av vann til samfunnet forsvinner. Virksomheten må da gjøre en analyse av sine aktiviteter der den kartlegger avhengigheten av ulike underliggende årsaksfaktorer. Slike faktorer kan være strøm, IKT-systemer, kompetanse, prosessanlegget, vannkvalitet i reservoar, nedbørsmengde etc. Deretter må en identifisere hva som kan gi bortfall av disse faktorene, for eksempel villede handlinger, naturskapte hendelser eller ulykker.

Risiko- og sårbarhetsanalysene må inngå i en kontinuerlig risikostyringsprosess. For virksomheter vil beslutninger, for eksempel knyttet til bruk av ny teknologi, bytte av underleverandør eller omorganisering av virksomheten, kunne påvirke sårbarheten av systemene i forhold til ulike hendelser, og det er derfor viktig for virksomheten at analysene inngår som en integrert del av styringsprosessene.

Et vannverk er åpenbart viktig for samfunnet og kommer inn i den kategorien selskaper som må gjøre slike analyser. For andre virksomheter eller offentlige etater kan det være vanskeligere å se sin egen betydning for samfunnet, for eksempel en underleverandør til vannverket. Retningslinjer knyttet til hvem som er viktige for å ivareta samfunnskritiske funksjoner må utformes slik at det blir tydelig hvem som kommer inn under lovverket. Det må også være en del av den enkelte samfunnskritiske virksomhets ansvar å stille krav til sine underleverandører som sikrer egne leveranser.

Fylkeskommune/kommune (naturlig geografisk område)

Hver enkelt virksomhet vurderer sin egen situasjon og hva de kan gjøre for å sikre sine leveranser til samfunnet, men virksomhetene klarer ikke uten videre å se helheten i samfunnet. Det må derfor være et offentlig ansvar å gjøre ROS-analyser for samfunnet som helhet. Hva som er det mest hensiktsmessige analysenivået her, om det skal være kommuner og/eller fylkeskommuner, eller større områder, kan diskuteres. Stormer, naturfenomen, forurensning etc, følger ikke kommune eller fylkesgrenser. Analysene må derfor organiseres slik at de ser helheten på tvers av de til enhver tid rådende organisatoriske strukturer. Analysene må samordnes og organiseres i forhold til det trusselbildet som til enhver tid gjelder. Samtidig må resultatene fra analysene tolkes og omsettes i praktiske resultater innenfor de eksisterende organisatoriske rammene.

Resultatene fra analysene skal kunne brukes på et høyt nivå til å prioritere ressurser i en planlegging- og budsjetteringsfase, men også til å gi innspill til konkrete tekniske eller organisatoriske løsninger.

Norge som nasjon

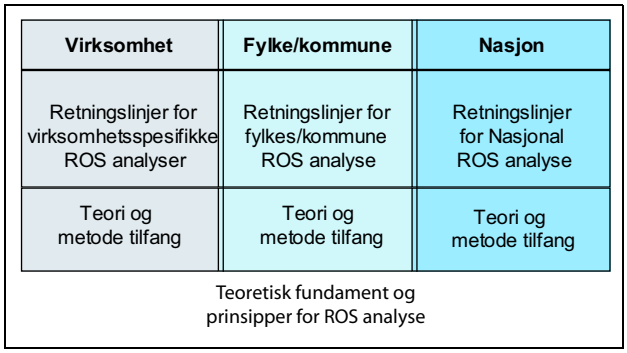
I utgangspunktet så vil kartlegging og håndtering av de fleste situasjoner skje lokalt i regionene.

Det er imidlertid en del trusler som er rettet mot nasjonen som helhet. Dette vil bla være epidemier, forurensning, store naturkatastrofer, krig, terrorisme med mer. Dette må håndteres i en ROS-analyse på nasjonalt nivå. I tillegg til å vurdere trusler mot nasjonen vil det på nasjonalt nivå ligge prioriteringsoppgaver og fordeling av midler når det gjelder forebyggende arbeid. Det er også en rekke oppgaver i forhold til å stille med kompetanse og ressurser til støtte for regionene, som skjer på nasjonalt nivå. På mange områder der regionene har felles utfordringer, vil løsningen i form av beredskap og kompetanse legges på nasjonalt nivå.

3 Rammeverk for Risiko og Sårbarhets-analyser - Samfunnskritisk infra-struktur

Rammeverket presentert i dette notatet omfatter alle de tre nivåene presentert ovenfor, dvs nasjon, region og virksomhet. Utfordringene er forskjellige på disse nivåene, og dette må reflekteres i rammeverket.

På nasjonalt og regionalt nivå, er utfordringen knyttet til å se helheten i et risikobildet, sikre at alle viktige elementer er med og avdekke sårbarhetene knyttet til avhengigheter mellom ulike virksomhe-



Figur 9.1 Rammeverk for risiko og sårbarhetsanalyser

ter og aktiviteter. Vi ser for oss en felles metodikk som kan anvendes på alle regioner (kommuner/fylkeskommuner).

På virksomhetsnivå er utfordringen annerledes. Det finnes virksomheter som er veldig kritiske for samfunnet og som har betydning for hele nasjonen, og det finnes regionale virksomheter som ikke er samfunnskritiske. Med en så stor variasjon mellom ulike virksomheter, er det ikke hensiktsmessig å utarbeide en metodikk som alle virksomheter skal bruke. Spennvidden er for stor.

Rammeverket tar høyde for dette og består av følgende delelementer:

– Retningslinjer for gjennomføring av nasjonale ROS-analyser og etableringen av et nasjonalt risikobilde (dette er en FoU-oppgave, inspirasjon kan hentes fra blant annet Risikonivå norsk sokkel prosjektet, Vinnem m.fl. (2006))
– Retningslinjer for gjennomføring av ROS-analyser for fylker og kommuner (her gjenstår en del arbeid selv om det er gjort en del arbeid på dette området)
– Retningslinjer for valg av ROS-metodikk for virksomheter. Med virksomhet menes her alle organisasjoner som leverer samfunnskritiske tjenester. Dette innbefatter private bedrifter, offentlige etater og kommuner i forhold de tjenestene disse leverer til samfunnet.

Fokuset i dette notatet vil være på virksomheter, men strukturen kan overføres også til de to andre nivåene. Rammeverket bygger på et felles teoretisk fundament og prinsipper. For de ulike nivåene er det et tilfang av ulike teorier og metoder, for eksempel knyttet til hvordan analysere risiko og ta beslutninger under usikkerhet.

Virksomhet: Retningslinjer for valg av ROS-metodikk

Utgangspunktet er virksomheter som er ansvarlig for samfunnskritisk infrastruktur eller virksomheter som er kritiske for at infrastrukturen skal fungere. Fokus i ROS-analysen vil være situasjoner karakterisert av høy risiko, dvs. det er et potensiale for store konsekvenser, betydelige usikkerheter hvorvidt slike konsekvensene vil inntreffe og/eller høye sannsynligheter for at slike hendelser vil inntreffe. Konsekvensene er knyttet til tap av viktige samfunnsfunksjoner. Vi omtaler slike situasjoner som *kritiske.*

Risiko- og sårbarhetsanalyser brukes i denne forbindelse for å gi underlag for beslutninger ved å

– identifisere kritiske infrastrukturer
– uttrykke grad av kritikalitet
– beskrive effekt av tiltak

Beslutningssituasjonene kan være veldig forskjellige når det gjelder risiko og beslutningsnivå, og vil innebære ulike behov for beslutningsstøtte og beslutningsprosesser. Det foreslåtte rammeverket tar høyde for dette og presenterer et klassifiseringssystem som strukturer de forskjellige beslutningssituasjoner, slik at man velger hensiktsmessig risiko- og sårbarhetstilnærming og metoder.

Utgangspunktet for en slikt rammeverk er erkjennelsen av at det vil være vanskelig å etablere *en* metodikk for risiko- og sårbarhetsanalyse, som er hensiktsmessig i alle beslutningssituasjoner. Det er per i dag utviklet en rekke ulike metoder tilpasset spesifikke formål og spesifikke fagområder. Noen av dem er gode til et begrenset formål, andre er mindre gode og har klare mangler. Et rammeverk som skissert i dette notatet har til hensikt i bidra i en utvelgelsesprosess, slik at metoden som brukes er hensiktsmessig i forhold til problemstillingen.

4 Klassifiseringssystem for beslutningsproblem

Klassifiseringen er basert på følgende grunnleggende prinsipp:

Fastsettelse av grad av kritikalitet (dvs. risiko i betydningen gitt ovenfor) gjennomføres ved

1. å klarlegge
   i. Forventede konsekvenser i forhold til aktuelle attributter, for eksempel sikkerhet for mennesker, helse, miljø, nasjonens sikkerhet, økonomi, etc.
   ii. Usikkerhetsfaktorer som kan bidra til store forskjeller mellom de faktiske konsekvenser og de forventede verdier, for eksempel sårbarheter, kompleksitet i teknologi, kompleksitet i organisasjonen, tidshorisont, etc.
2. å sammenholde i) og ii).

	Ranking			Argument	Comment
	1	2	3		
Expected consequenses					
Effect on safety for personnel	Low	Medium	High		
Healh effect	Low	Medium	High		
Effect on enviroment	Low	Medium	High		
Effect on national security	Low	Medium	High		
Effect on elfare	Low	Medium	High		
Effect for protection of privacy	Low	Medium	High		
Effect on ..... (other critical societal function).....	Low	Medium	High		
Effect on business economy	Low	Medium	High		
Effect on business deliverables	Low	Medium	High		
Effect on ..... (other critical business issues).....	Low	Medium	High		
Total	Low	Medium	High		
Uncertainties/probabilities	Low	Medium	High		
Probability of intended attack (Evaluated to be a high risk system)	Low	Medium	High		
Expected vulneralbility to human error (Competence, User interface, Design philosophy, redundancy,....)	Low	Medium	High		
Expected vulneralbility to extreme weather (Geographical distribution, technology, age, ...)	Low	Medium	High		
Complexity of technology (Unproven technology, interface with other systems, geographical distribution.....)	Low	Medium	High		
Complexity of organisation (Complex user organisation, many interface, ongoing change processes etc.....)	Low	Medium	High		
Availibility of information (Quality of documentation in project phases: design, construction, operation)	Low	Medium	High		
Time frame for evaluation	Short	Medium	High		
Total					

Figur 9.2 Eksempel på system for klassifisering av kritikalitet

Rasjonale for dette prinsippet er at forventningsverdien er en god styringsstørrelse for virksomheter med mange aktiviteter, i og med at forventningsverdien vil kunne gi gode prediksjoner for gjennomsnittsverdier. Det er imidlertid en rekke faktorer som gjør at vi kan få store avvik mellom forventningsverdiene og de faktiske konsekvenser. Disse faktorene er i stor grad knyttet til grad av usikkerhet i de underliggende fenomener som studeres.

Vektingen i forhold til ulike attributter og sammenholdningen av i) og ii) kan skje på ulike måter, kvalitativt eller ved hjelp av ulike former for scoringssystemer. Høyt utslag på både i) og ii) gir åpenbart høyest grad av kritikalitet: Vi forventer alvorlige konsekvenser og ekstreme konsekvenser kan oppstå under visse forutsetninger. Et eksempel på faktorer som kan inngå i et slikt scoring system er vist i figur 9.2.

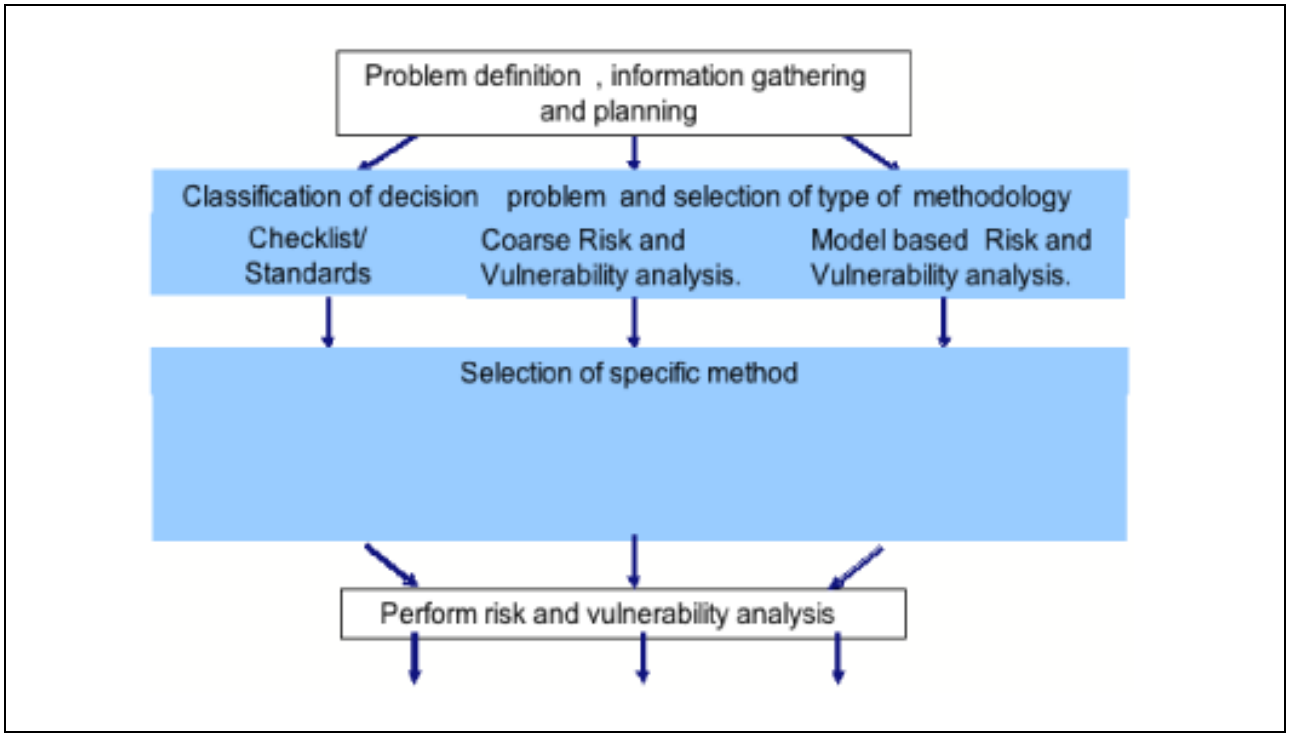
Ved å se på ulike eksempler vil man fort oppdage at konsekvensene vil variere sterkt for de forskjellige attributter og usikkerheten som ligger i de underliggende faktorer.

I eksempelet presentert i figur 9.2 er konsekvens og usikkerhetselementene presentert på et overordnet nivå. Utdypende evaluering kan gjøres innenfor hvert av disse hovedelementene. Dette kan være naturlig å gjøre der forventet konsekvens og/eller usikkerheten er høy.

Klassifiseringen vil gi innspill til valg av ROS metode, men er i seg selv også en overordnet risiko- og sårbarhetsanalyse, som gir grunnlag for beslutninger i forhold prioriteringer, innsatsområder etc..

Figur 9.3 illustrerer tankegangen bak framgangsmåten for å velge egnet ROS-metodikk.

Normalt vil høy grad av kritikalitet, kreve dybde og presisjon i analysen, mens ved lav kritika-



Figur 9.3 Framgangsmåten for å velge egnet ROS-metodikk

litet kan man i større grad bruke koder, standarder, sjekklister etc.

Men andre forhold spiller også inn, og viktigst her er formålet med analysen. I en del sammenhenger vil grove analyser måtte gjøres for svært kritiske systemer, på grunn av begrensninger i tid. Hensikten er å gi beslutningsstøtte, og det har ingen mening å utføre analyser som gir sine konklusjoner etter at beslutningene er tatt.

Dessuten må en trekke inn i hvilke grad det aktuelle analyseobjektet er et standard system, hvor en kan trekke på etablerte sjekklister og standarder som er utarbeidet og basert på lang erfaring fra tilsvarende systemer nasjonalt/internasjonalt. For unike systemer vil en i større grad måtte kreve detaljerte ROS-analyser.

Fremgangsmåten illustrert i figur 9.3 er en del av det arbeidet som gjøres i BAS 5 prosjektet. I arbeidet inngår retningslinjer for klassifisering av system/beslutningsproblem samt er evaluering av etablerte teknikker og metoder for risiko og sårbarhetsanalyser. Fokus er her sårbarheten i IKT systemer.

5 Diskusjon

Hensikten med å etablere et rammeverket for ROS-analyser er å sikre en helhetlig og konsistent tenkning i det arbeidet som bør gjøres for å sikre samfunnskritisk infrastruktur. Rammeverket må favne vidt og ha en innebygd fleksibilitet som sikrer at det vil være et effektivt rammeverk i tider med store endringer.

Rammeverket inkluderer derfor alle nivåer i samfunnet, fra nasjonale utfordringer til de lokale. Det gjenstår betydelig arbeid i forhold til utviklingen av elementene i rammeverket:

- Retningslinjer for gjennomføring nasjonale ROS-analyser og etableringen av et nasjonalt risikobilde.
- Retningslinjer for gjennomføring av ROS-analyser for fylke/kommune.
- Retningslinjer for valg av ROS-metodikk for virksomheter.

Når det gjelder det teoretiske fundamentet og prinsippene for ROS-analyse, vises det til den betydelige forskningen og utviklingen som er blitt gjennomført de senere årene, blant annet i forbindelse med flere forskningsprosjekter i regi av Norges forskningsråd (Risiko og Usikkerhet 2000-02, HMS petroleum - beslutningsstøtte 2002-06). Aktuelle temaområder er her håndtering av usikkerhet, bruk av statistiske forventningsverdier i risikostyringen, bruk av forsiktighets-prinsippet og føre-var, bruk av risikoakseptkriterier, m.m. Det vises til Aven (2003) og Aven og Vinnem (2006).

Rammeverket presentert i dette notatet må sees i større kontekst, der også lovverket og tilsynsordningene inngår. Implementeringen av et nytt regime vil være krevende, ikke minst i forhold til å utvikle kompetanse i den enkelte virksomhet. Også i forhold til forskning og utvikling vil det være behov for betydelig innsats.

Det er viktig å understreke at rammeverket bygger på en tenkning til risiko som gir rom for ulike perspektiver. Det er lagt til grunn en del felles prinsipper, men disse prinsippene understøtter en bred tilnærming, som åpner opp for vurderinger utover ekspertenes risikoanalyser. Analysene gir kun beslutningsstøtte, og det vil alltid være behov for å se analysene i en større sammenheng og trekke inn de begrensninger og svakheter som ligger i analysene. Ulike aktører kan ha ulike perspektiver og syn på de sentrale premisser for de analyser som gjøres. Det er derfor viktig å etablere et mest mulig helhetlig og bredt bilde av risiko og sårbarhet, som avspeiler mangfoldet i kunnskap og oppfatninger der dette er viktig for de beslutninger som skal tas. Prosessene for å etablere risiko- og sårbarhetsbildet og oppfølgingen av dette må være forankret i en tenkning som tar innover seg at risiko primært er en vurdering og ikke fakta. Vi viser til Vinnem m.fl. (2005) for et eksempel på en slik prosess i forbindelse med Risikonivå norsk sokkel (RNNS)-prosjektet.

Referanser

Aven, T. (2003) *Foundations of Risk Analysis. Wiley, N. Y.*

Aven, T. and Vinnem, J.E. (2006) *Risk Management, with Applications from the Offshore Oil and Gas Industry.* Springer Verlag, forthcoming.

Vinnem, J.E., Aven, T. Husebø, T., Seljelid, J., Tveit, O.J. (2006) *Major hazard risk indicators for monitoring of trends in the Norwegian offshore petroleum sector. To appear in Rel. Eng. System Safety.*

Wiencke, H.S., Aven T. E. (2006) *A framework for selection of methodology for risk and vulnerability assessments of infrastructures depending on ICT.* Paper to be presented at ESREL 2006.

Vedlegg 10

Ivaretakelse av sikkerhet og beredskap i fristillingsprosesser

Statskonsult, 7. juni 2005

1 Innledning og bakgrunn

Bakgrunn

Siden begynnelsen av 1990-tallet er en rekke statlige virksomheter blitt skilt ut som egne selskaper. En del av disse er senere blitt helt eller delvis privatisert. Organisering av statlig virksomhet som selvstendige selskaper legger rammer for statens styringsmuligheter og virkemiddelbruk. Målsettingen med dette notatet er å belyse på hvilken måte sikkerhets- og beredskapshensyn ble vektlagt og ivaretatt i forbindelse med selskapsdannelse, liberalisering og eventuell privatisering. I samarbeid med oppdragsgiver er telesektoren og kraftsektoren valgt ut for nærmere gjennomgang. I notatet gis det en beskrivelse av hvordan sikkerhet og beredskap er ivaretatt under og etter selskapsdannelsene og vi har foretatt en sammenlikning av de to sektorene. Notatet inneholder ingen vurdering av om sikkerhet og beredskap har vært tilstrekkelig ivaretatt eller hvor hensiktsmessig virkemiddelbruken er.

Notatet er utarbeidet av Statskonsult på oppdrag fra Utvalg for sikring av landets kritiske infrastruktur (Infrastrukturutvalget). Notatet bygger i hovedsak på studier av offentlige dokumenter (stortingsdokumenter og NOUer), forsknings- og utredningsrapporter. Det er i tillegg innhentet noen opplysninger via telefon.

Definisjon av kritisk infrastruktur

Infrastrukturutvalget har utarbeidet følgende (foreløpige) definisjon av hva som er kritisk infrastruktur:

> «Kritisk infrastruktur defineres som de objekter, systemer og tjenester som er så viktige for samfunnet at deres manglende funksjonalitet eller ødeleggelse vil medføre svekkelse av rikets sikkerhet, alvorlig svekkelse av den nasjonale økonomi, alvorlig svekkelse av statens myndighetsutøvelse, betydelig tap av liv og helse, og/eller betydelig tap av den nasjonale trygghetsfølelse.»

Hva menes med sikkerhet og beredskap?

Sikkerhet og beredskap er et vidt begrep som i utgangspunktet kan omfatte alt fra forebygging av mindre driftsforstyrrelser som i en kort periode kan føre til svikt i tjenesteproduksjonen til beredskapsarbeid i en krigssituasjon. Med en så vid definisjon vil mye av beredskapsarbeidet være tjenesteleverandørens ansvar. Det er beredskapstiltak som gjøres for å møte utfordringer knyttet til naturkatastrofer, terrorisme, krise og krig som vi særlig tenker på når vi i dette notatet skriver om sikkerhet og beredskap.

2 Energisektoren

Innenfor energi har vi konsentrert oss om elektrisk kraft. Petroleumssektoren og beredskap innenfor den holdes utenfor.

2.1 Beskrivelse av utviklingen på sektoren

2.1.1 Generell omtale

I Norge dekkes kraftforbruket i all hovedsak gjennom elektrisk kraft. Forbruket av elektrisk kraft har vist en sterk vekst de siste årene og energiforsyningens sårbarhet for svikt i nedbøren har økt. Det henger særlig sammen med at kapasitetsutnyttelsen av produksjonsapparatet har økt vesentlig i de senere årene. Det har også utnyttelsen av det sentrale overføringsnettet. Økt sårbarhet for svikt i nedbøren har ført til økt oppmerksomhet omkring forsyningssikkerheten. Dette gjelder særlig fordi økningen i forbruket forventes å bli større enn økningen i produksjons- og overføringskapasiteten også i årene fremover.

I dag er nesten all produksjon av kraft i Norge basert på vannkraft. Vannkraft vil også i fremtiden utgjøre hovedtyngden av kraftproduksjonen, selv om en mindre del an energiforbruket vil komme fra gasskraft eller alternative energikilder.

Kraftforsyningen kan inndeles i tre delsystemer; produksjonsanleggene (om lag 900), overfø-

ringsnettet (knytter regionene sammen, knytter Norge og utlandet sammen) og distribusjonsnettet (kopler forbrukerne til overføringsnettet).

Virksomhetene varierer i størrelse og har ulik selskapsmessig organisering. Strukturen i markedet er i stadig endring gjennom oppkjøp og fusjoner.

Etter at energiloven trådte i kraft, har det skjedd store strukturendringer på området. 1. januar 2004 var det til sammen 320 selskaper med omsetningskonsesjon i Norge. 178 selskaper hadde nettvirksomhet på en eller annen måte. 46 av selskapene var rene nettselskaper mens 132 selskap drev både konkurranseutsatt virksomhet (produksjon og/eller omsetning) og nettverksomhet.

Antall kommunale og fylkeskommunale foretak har sunket mens antall aksjeselskap har økt. Pr. 1. januar 2004 var 73% av alle selskap i kraftsektoren organisert som kraftselskap[1]. Kun 8% var organisert som kommunalt/fylkeskommunalt /interkommunalt foretak.

På tross av at mange kommuner og fylkeskommuner de siste årene har realisert betydelige verdier gjennom salg av kraftaksjer, er de fortsatt tungt inne på eiersiden. Pr. 1. januar 2004 eide kommuner og fylkeskommuner om lag 55% av landets produksjonskapasitet. Staten, gjennom Statkraft SF, eide om lag 30% mens de resterende 15% var fordelt på private selskaper.

2.1.2 Historisk utvikling

Kraftforsyningen i Norge har tradisjonelt vært sett på som et offentlig ansvar. Det offentlige eierskapet ble først og fremst etablert og utviklet for å sikre lokalt næringsliv og lokale innbyggere sikker og rimelig tilgang på kraft.

Fram til 1985 var statens eierskap og oppgaver i kraftforsyningen samlet i NVE som også styrte statens forskjellige kraftverk. NVE besto av fire direktorater, underlagt et felles hovedstyre og en generaldirektør. Ved Stortingets behandling av St.prp. nr. 57 (1984-85) ble Statkraft skilt ut fra NVE som en egen statlig forvaltningsbedrift underlagt OED. I 1990 ble NVE omdannet til et direktorat samtidig med at Elektrisitetstilsynet ble ble overført til det daværende Kommunaldepartementet fom. 1. januar 1991.

Energiloven av 1990 trådte i kraft 1. januar 1991. Loven hadde som mål å gi forbrukerne rimeligere kraft ved at effektiviteten i bransjen ble høyere. Kraftselskapene skulle i større grad legge til grunn økonomiske kriterier ved vurderinger av fremtidige investeringer. Siden forbrukerne fikk økt mulighet til å kjøpe kraften der den var billigst, motiverte dette produsentene til å legge større vekt på rasjonalisering og effektivitet, samt mer kritisk vurdering av lønnsomheten i nye prosjekter.

I forbindelse med St.prp. nr. 100 (1991-92) ble det vedtatt å etablere et organisatorisk skille mellom statens egen kraftproduksjon og statens anlegg for overføring av kraft. Statens andel av sentralnettet, transformatorer, koplingsanlegg og utenlandsforbindelser ble skilt ut som eget statsforetak, Statnett SF. Valg av statsforetaksformen ble for Statnetts del begrunnet med at selskapet ville ha en viktig sektorpolitisk rolle hvor noen av oppgavene ville ligge i grenselandet mellom forvaltning og forretning.

Nettjenester i forbindelse med overføring og fordeling av kraft skulle fortsatt være monopoltjenester. Begrunnelsen for å regulere overføringsnettet som et naturlig monopol var todelt. For det første består kostnadene knyttet til kraftoverføring for en stor del av faste kostnader og etablering av parallelle nett ville være samfunnsøkonomisk ugunstig. For det andre er lik tilgang til nettet viktig for å kunne oppnå konkurranse om produksjon og omstilling. Norges vassdrags- og energidirektorat (NVE) regulerer i dag nettdelen av markedet gjennom et monopolkontrollregime.

I tabell 10.1 følger en kort oversikt over deler av utviklingen fra energiloven ble vedtatt i 1990 og trådte i kraft i 1991.

2.1.3 Virkemiddelbruk

Kraftsektoren reguleres først og fremst gjennom energiloven og vassdragsloven med tilhørende forskrifter og retningslinjer. Selv om markedskreftene har fått mer innpass i kraftsektoren, reguleres virksomheten fortsatt gjennom konsesjoner.

- *Anleggskonsesjon* – anlegg for produksjon, omforming, overføring og fordeling av elektrisk energi med høy spenning, kan ikke bygges eller drives uten konsesjon[2]
- *Områdekonsesjon* – gis for bygging og drift av anlegg for fordeling av elektrisk energi med spenning opp til et nivå som fastsettes av departementet[3]
- *Omsetningskonsesjon* – gjelder andre aktører enn staten. Det kan knyttes ulike vilkår til konsesjonen[4].

[1] Kilde: OEDs faktahefte for 2004

[2] Energiloven, §3-1
[3] Energiloven, §3-2
[4] Energiloven §4-1

Tabell 10.1 Oversikt over utviklingen fra den nye energiloven trådte i kraft i 1991

År	Hendelse
1991	Energiloven trer i kraft. Statkraftverkene splittes i Statkraft SF (produksjon) og Statnett SF (nett) Om lag 70% av alle kraftselskap i Norge organisert som kommunale eller fylkeskommunale foretak
1993-97	Etablering og utvikling av en norsk (Statkraft Marked) og nordisk (Nord Pool) kraftbørs
2000	Sårbarhetsutvalgets innstilling foreligger
2002	Ansvaret for Statskraft SF overføres fra OED til NHD Om lag 70% av alle kraftselskap i Norge organisert som aksjeselskap, om lag 7% organisert som kommunale eller fylkeskommunale foretak
2002-03	«Kraftkrise» m/påfølgende tiltak for bedre forsyningssikkerheten Kraftforsyningens beredskapsorganisasjon får bl.a. utvidede fullmakter mhp. rasjonalisering

Statnett eier det meste av sentralnettet (om lag 80%). Andre energiverk med eierandeler i sentralnettet leier disse ut til Statnett. Statnett har systemansvar for sentralnettet, dvs. et juridisk og økonomisk ansvar for å utvikle, drive og vedlikeholde sentralnettet. Statnett og de andre netteierne inngår i Kraftforsyningens beredskapsorganisasjon (KBO), jf. pkt. 2.2.1.

Omsetningskonsesjonen er det viktigste virkemiddelet for å sikre alle aktører lik tilgang til nettet. Netteiers kostnader knyttet til drift, vedlikehold osv. dekkes ved at den som overfører kraft i nettet betaler en godtgjørelse – kalt overføringstariff eller nettleie – til netteier. NVE har ansvar for å føre kontroll med nivået på tariffene for å hindre at monopolet misbrukes.

2.1.4 Hensynet til beredskap og sårbarhet

Beredskapstankegangen har alltid vært en viktig del av norsk kraftforsyning med myndighetene som hovedansvarlig instans. Kraftforsyningens sivilforsvarsnemd, som hadde som formål å sikre kraftforsyningen mot skader som følge av krigshandlinger, ble opprettet i 1948. Ved en lovendring i 1986 ble nemnda nedlagt og arbeidet ble lagt inn under NVE. Ved omorganiseringen i 1991 ble nemda omgjort til seksjon for beredskap i sikkerhetsavdelingen i NVE.

I energiloven (Ot.prp. nr 12 (1989-90)) er beredskap omtalt i §§ 6-1 til 6-7. Loven omhandler Kraftforsyningens beredskapsorganisasjon, vedtaksmyndighet, forhold knyttet til sikringstiltak, pålegg og finansiering av beredskap. Det er blitt foretatt en rekke mindre endringer i loven opp gjennom årene. Eksempelvis ble loven i 1993 utvidet til også å gjelde tiltak mot naturgitte forhold, teknisk svikt eller tilsiktede ødeleggelser i fred.

I St. meld nr 29 (1998-99) om energipolitikken vises det til at investeringene i energianlegg er redusert de siste årene, mens forbruket har økt. Statnett har ansvaret for investeringer i sentralnettet. Meldingen peker på at det kan være behov for å ta i bruk spesielle virkemidler for å sikre at investeringer som er nødvendige for å gi leveringssikkerhet blir foretatt. Fra 2001 ble det innført en ordningen med kvalitetsjusterte inntektsrammer for ikke-levert energi (KILE). Ordningen innebærer at selskapene gis en økonomisk straff ved leveringsavbrudd.

I forbindelse med Ot. prp nr 56 (2000-2001) ble det foretatt en gjennomgang av energiloven. Som følge av denne gjennomgangen ble Beredskapsrådet nedlagt. Bakgrunnen var at ansvaret for beredskapsarbeid nå var samlet i NVE, og at alle rådets saker ble forberedt av NVE. Det ble gjort enkelte presiseringer og endringer knyttet til rasjoneringsansvaret og systemansvaret. Det ble laget ny forskrift om rasjonering av kraft. NVE er rasjoneringsmyndighet med ansvar for planlegging og gjennomføring av tiltak.

I St.meld nr 17 (2001-2002) samfunnssikkerhet – veien til et mindre sårbart samfunn gis det en bred omtale av kraftforsyningen. I meldingen vises det til Sårbarhetsutvalgets påpekning av at energimyndighetene gjennom det siste tiåret hatt et hovedfokus mot tilrettelegging av effektivt fungerende kraftmarkeder. Bransjens effektiviseringsbestrebelser i den samme perioden har også ført til reduksjon av reparasjonsressurser. Regjeringen pekte på at en fortsatt effektivisering av virksomheten ikke må gå på bekostning av nødvendig arbeid med sikkerhet og vedlikehold. Det ble vist til at det var behov for en langsiktig analyse av konsekvenser av mulig ustabilt klima. Det var også behov for en gjennomgang og revisjon av

beredskapskrav ved dammer og vassdragsanlegg.

St.meld. nr. 18 (2003-2004) om forsyningssikkerheten for strøm mv. kom som en følge av kraftkrisen i den nedbørfattige sesongen 2002-2003. Meldingen redegjør for ulike tiltak som ble gjort i denne forbindelse.

Stortinget ba i 2004 Regjeringen foreta en grundig evaluering av energiloven, spesielt når det gjelder oppdekningsplikten og forsyningssikkerheten, og komme tilbake til Stortinget med eventuelle forslag til endringer, jf. Stortingsvedtak nr. 360 av 18. mai 2004. Departementet behandlet dette anmodningsvedtaket i revidert nasjonalbudsjett inneværende år (ss 307-317). I OEDs svar vises det til at prinsippet om oppdekningsplikten er i strid med organiseringen av kraftmarkedet som følger av EØS-avtalen. Når det gjelder forsyningssikkerheten, vises det til St.meld. nr. 18 (2003-2004) og de tiltakene som ble lagt fram der. Det vises bl.a. til at Statnett SF med hjemmel i energiloven har fått presisert sitt systemansvar knyttet til svært anstrengte kraftsituasjoner. Dette er også fulgt opp gjennom endring av NVEs forskrifter for systemansvar med virkning fra og med 2005.

2.1.5 Utredninger om beredskap og sårbarhet

I prosjektet «Beskyttelse av samfunnet, del 3» (BAS3), som Forsvarets forskningsinstitutt (FFI) gjennomførte i perioden 1999-2001, rettes oppmerksomheten mot samfunnets avhengighet av elektrisitet og den sårbarheten som utvikles i kraftforsyningen i takt med den pågående markedsmessige og teknologiske utviklingen.

FFI beskriver kraftforsyningen som sårbar både overfor fysiske påkjenninger, og angrep mot sine informasjonssystemer. FFI påpeker at konsekvensene for samfunnet kan bli store ved langvarig strømbortfall, og selv ved kortvarig svikt stopper mange samfunnsfunksjoner opp. Som en konsekvens av dette anbefaler FFI at kraftforsyningen sikres gjennom en rekke tiltak, inklusive sikring av IT-systemer, satsing på personell og kompetanse og bedre gjenopprettings- og reparasjonsmuligheter m.m. FFI kostnadsberegnet tiltakene til ca 750 millioner kroner fordelt over 10 år i 2001. På lengre sikt anbefaler FFI også å sikre kraftforsyningen utover det anbefalte nivået, gjennom markedsmessige grep som sikrer nyinvesteringer og investeringer i beredskapstiltak.

Sårbarhetsutvalget la mye av FFIs arbeid til grunn for sine vurderinger omkring kraftforsyning og beredskap. I utvalgets innstilling[5] pekes det på at sårbarheten innenfor kraftsektoren øker når virksomheter og funksjoner sentraliseres (personell- og materiellreserver bygges ned), når det nedbemannes (tilgangen på fagkompetanse reduseres) og når bruk av elektroniske informasjons- og kommunikasjonssystemer øker (økt kompleksitet). Innenfor kraftproduksjon og -forsyning drøfter utvalget bl.a.:

- *Fysisk sårbarhet* – overføringsnettet, transformatorstasjonene inn til byer og tettsteder og sjøkabler pekes ut som særlig sårbare. Samtidig understrekes det at mange lokale anlegg er for dårlig sikret.
- *Sårbarhet som følge av at kraftmarkedet er åpnet for markedskrefter* – økt fokus på effektivitet og inntjening kan medføre mindre robuste infrastrukturinvesteringer, høyere avkastningskrav på investeringer, økt avhengighet av andre lands kraftproduksjon og –kapasitet m.m.
- *Vassdragssikkerhet, flomsikkerhet og sikkerhet mot dambrudd* – konsekvensene knyttet til dambrudd anses som de mest alvorlige.

2.2 Aktører og virkemidler for å ivareta beredskap

2.2.1 Sentrale aktører

Her konsentrerer vi oss om de sentrale aktørene i forhold til beredskap; Olje- og energidepartementet (OED), Norges vassdrags- og energidirektorat (NVE) og Kraftforsyningens beredskapsorganisasjon (KBO) hvor både vassdragsregulanter, kraftprodusenter og netteiere inngår.

Olje- og energidepartementet

Innenfor energi- og vassdragssektoren har OED det overordnede ansvaret for kraftforsyningsberedskap og beredskapsoppgaver knyttet til flom, leirskred, dambrudd og andre ulykker i landets vassdrag. Beredskapsarbeidet utføres i stor grad av Norges vassdrags- og energidirektorat (NVE) etter de retningslinjer departementet gir. OED fører tilsyn med NVEs beredskapsarbeid og ivaretar behovet for samordning med andre departementer som Justis- og politidepartementet.

Norges vassdrags- og energidirektorat (NVE)

NVE leder den nasjonale kraftforsyningsberedskapen. Gjennom sine forskrifter stiller NVE krav og gir pålegg om beredskapstiltak til den enkelte tiltakshaver, og fører tilsyn med tiltakshavernes oppfølging av beredskapsarbeidet.

[5] NOU 2000:24 *Et sårbart samfunn*

Innenfor kraftforsyningsberedskapen prioriteres kraftsystemets evne til raskt å gjenopprette sin funksjonsevne ved skade. Historisk er det klimaet og naturen som har gitt opphav til de mest ødeleggende hendelsene og de største påkjenningene i fredstid, men samfunnet må også i økende grad være forberedt på terror- og sabotasjehandlinger.

Kraftforsyningens beredskapsorganisasjon

Kraftforsyningens beredskapsorganisasjon (KBO) er en landsomfattende organisasjon bestående av NVE og de virksomhetene som står for kraftforsyningen, dvs. alle enheter som eier eller driver kraftproduksjon med tilhørende vassdragsregulering, overføring og distribusjon av elektrisk kraft og fjernvarme.

Ved krigsberedskap overtar KBO ansvaret for landets kraftforsyning. Alle kraftforsyningsenheter plikter å rette seg etter direktiver fra overordnet myndighet i KBO. KBO skal i tillegg kunne løse oppgaver i fred ved skade på kraftanlegg som følge av naturgitte forhold, teknisk svikt, terror- eller sabotasjeaksjoner samt i forbindelse med rasjonering etter energiloven. Etter energikrisen vinteren 2002 -03 har KBO fått utvidede fullmakter knyttet til rasjonering.

KBO er delt inn i sentralt nivå, regionnivå, distrikts-/fylkesnivå og lokalt nivå.

Sentralt nivå tilsvarerer Kraftforsyningens sentrale ledelse (KSL) og består av beredskapsmyndighet (NVE) og systemansvarlig (Statnett). Sentralt nivå ledes av NVEs direktør eller den han bemyndiger. Kraftforsyningens regionsjefer (KRS) er KBOs kommandoledd på regionalt nivå. Regionsjefene utpekes fra systemansvarlig og deres geografiske ansvarsområder følger Statsnetts regioninndeling. Kraftforsyningens distriktssjefer (KDS) er KBDs kommandoledd på distrikts-/fylkesnivå. Distriktssjefene utpekes fra enhet i KBO.

Direkte utgifter knyttet til KBO dekkes over NVEs driftsbudsjett.

Statnett

Statnett er en sentral aktør innenfor kraftforsyning som største eier og systemansvarlig for sentralnettet og utenlandsforbindelsene. I likhet med andre virksomheter kan de pålegges beredskapsinvesteringer/-forpliktelser, energilovens kap.6.

Statnett har gjennom systemansvaret et spesielt ansvar. I forskrift om systemansvaret i kraftsystemet ble det fra 1. januar 2005 tatt inn en bestemmelse om at systemansvarlig har ansvaret for kontinuerlig å utrede og utvikle nødvendige virkemidler for å håndtere perioder med en svært anstrengt kraftsituasjon. Det er NVE som gjør vedtak om bruk av slike virkemidler.

2.2.2 Virkemiddelbruk

Lov- og regelverk

Beredskapstankegangen har vært – og er – basert på et regelstyrt regime med beredskapsforpliktelser pålagt alle virksomheter. Beredskap innenfor kraftforsyningssektoren er først og fremst regulert gjennom lov og regelverk (energiloven og vassdragsloven med tilhørende forskrifter).

De viktigste reguleringene finner vi følgende steder:

- *Energilovens beredskapskapittel (kapittel 6)* inneholder bestemmelser om kraftforsyningens beredskapsorganisasjon (KBO), vedtaksmyndighet, pålegg om sikringstiltak, fordeling av utgifter og vedrelag ved gjennomføring av sikringstiltak, meldeplikt ved bygging eller endring av kraftforsyningsanlegg og gebyr til dekning av utgifter ved beredskapsarbeidet.
- *Energiforskriftens*[6] *beredskapskapittel (kapittel 6)* inneholder bl.a. utfyllende bestemmelser om KBO, sikringstiltak, forebyggende sikkerhet, økonomiske rammer og statlig tilskudd, gebyr og gjennomføring og tilsyn.
- NVE vedtok 16. desember 2002 en ny forskrift om *beredskap i kraftforsyningen* som inneholder ulike typer krav knyttet til beredskap i kraftforsyningen, herunder om ulike aktørers oppgaver, plikter, ansvar m.m. Det er også utarbeidet en veiledning til denne forskriften.

Økonomiske virkemidler

Utgifter knyttet til NVEs - inklusive KBOs - beredskapsarbeid dekkes gjennom en gebyrordning som gjør at utgiftene utlignes på eiere og brukere av kraftanlegg. Satsene skal reguleres slik at de samlede gebyrer tilsvarer de faktiske utgifter Norges vassdrags- og energidirektorat har med beredskapsarbeidet. I 2004 ble det tatt inn om lag 22 mill kroner i gebyr- og avgiftsinntekter: Disse inntektene dekker NVEs utgifter til kraftforsyningsberedskap, inklusive KBO, og utgifter til driften av NVEs tilsynsvirksomhet.

NVE forvalter en tilskuddsordning for anskaffelse av reservemateriell. Søkere kan få dekket inntil 50% av utgiftene. For 2005 er det budsjettert med

[6] Forskrift av 07.12.90 nr. 959 om produksjon, omforming, overføring, omsetning og fordeling av energi.

2,6 mill kroner pluss en tilsagnsfullmakten på 2,5 mill. kroner til dette.

Kraftselskapene gis insentiver gjennom ordningen med kvalitetsjusterte inntektsrammer for ikkelevert energi (KILE). Denne ordningen gir selskapene en økonomisk straff ved leveringsavbrudd.

I arbeidet med beredskapen i vassdragene prioriteres forebygging mot leirskred. For 2005 er det bevilget 74 millioner kroner til sikrings- og miljøtiltak i vassdrag (kap 1820 post 22). Om lag 20% av denne bevilgningen dekkes gjennom distriktsbidrag fra kommuner og andre som får utført disse sikringstiltakene.

3 Telesektoren

3.1 Beskrivelse av utviklingen på sektoren

3.1.1 Generell omtale

Siden 1889 har staten hatt enerett til å drive telefonivirksomhet i Norge. Bakgrunnen for bruk av enerett var telefonens samfunnsmessige betydning, behovet for samordning, samt stordriftsfordeler. Spørsmålet om en friere økonomisk og administrativ stilling ble reist en rekke ganger, men ble avvist av Stortinget ut fra samfunnspolitiske hensyn.

I 1988 ble deler av telemarkedet liberalisert[7], og det opprinnelige Televerket ble delt i tre. Brukerutstyr og interne nett ble skilt ut i datterselskapet TBK, forvaltningsoppgavene[8] ble stort sett lagt til Statens teleforvaltning og de gjenværende monopoloppgaver ble beholdt i Televerket.

Dereguleringen av telesektoren var først og fremst en konsekvens av inter-nasjonal teknologisk og markedsmessig utvikling, som bl a førte til at en regulert telesektor smeltet sammen med en uregulert databransje. Videre var trådløs tilknytning i ferd med å bli et alternativ til det faste nettet. Regjeringen ga i St prp nr 70 (1995-96) Om avvikling av resterende eneretter i telesektoren, uttrykk for at en opprettholdelse av eneretten innenfor telekommunikasjon ville forsinke utviklingen i Norge på et område som var preget av sterk vekst. Økt konkurranse og opphevelse av skillene skulle stimulere til tjenesteutvikling på områder som kombinerer tale, data og bilde. Stortinget vedtok ved behandlingen av proposisjonen at hele telemarkedet skulle åpnes for konkurranse fra 1. januar 1998.

I 1994 ble Televerket omdannet fra forvaltningsbedrift til statsaksjeselskap. Regjeringen la vekt på at Televerket skulle få en tilknytningsform med et forretningsmessig handlingsrom tilnærmet lik konkurrentenes. Begrunnelsen for å velge aksjeselskapsformen var at denne organisasjonsformen var den mest vanlige for bedrifter som opererer i markeder med konkurranse. I tillegg ble det lagt vekt på at denne selskapsformen er kjent internasjonalt. I desember 2000 ble Telenor børsnotert og delprivatisert. I denne forbindelse ble forvaltningen av det statlige eierskapet overført fra Samferdselsdepartementet til Nærings- og handelsdepartementet.

3.1.2 Reguleringen av en liberalisert telesektor

Liberalisering av telesektoren førte til behov for en reregulering av sektoren. De viktigste grunnene til at det var behov for en sektorspesifikk regulering var knyttet til følgende:

- *Markedssvikt:* Fordi Telenor var en dominerende aktør på markedet, ville det lett kunne dannes et «naturlig» monopol med risiko for misbruk av markedsmakt.
- *Nettinfrastruktur:* Dereguleringen kunne føre til dårlig utnyttelse av nettene og mulig oppbygging av parallelle nett. Gjennom reguleringer ønsket man å sikre god og effektiv utnyttelse av nettinfrastrukturen.
- *Samfunnsmål:* Gjennom et nytt reguleringsregime ville man også sikre at samfunnsmål fortsatt ble ivaretatt.

Det sentrale dokumentet i denne sammenheng var den nye teleloven (Ot.prp.nr. 36 (1994-95) Om lov om telekommunikasjon). Tidligere lover på dette området hadde i stor grad vært fullmaktslover til forvaltningen, uten spesifiserte reguleringshjemler. Regjeringen ønsket å stramme dette inn, og i den nye loven er hjemler for å regulere gjort tydeligere.

Gjennom det nye regelverket ønsket man å oppnå:

- at alle operatører og leverandører skulle bidra til å oppfylle målet om landsdekkende tjenester
- at nettoperatører tillater sammenknytting og dermed samvirke mellom nett
- at brukerne får åpen adgang til offentlige nett
- at det utvikles regelverk for datasikkerhet, personvern m.v.
- rettferdig konkurranse.

Regelverket fokuserer på å etablere et konkurranseutsatt marked der nye aktører får innpass.

[7] Avvikling av enerett på terminalutstyr og interne telenett.

[8] Statens teleforvaltning ble opprettet i 1987. Oppgavene var bl.a. forvaltning av frekvenser, fastsettelse av forskrifter, tildeling av konsesjoner og godkjenning av utstyr og leverandører.

Hovedmålene i telepolitikken har i følge offentlige dokumenter og andre kilder, i hovedsak ligget fast. Telepolitikken har i offentlige dokumenter blitt knyttet til distriktspolitiske, sikkerhetspolitiske, fordelingspolitiske og næringspolitiske målsettinger. Hovedmålene i telepolitikken har hele tiden vært knyttet til *lik tilgang* til teletjenester over hele landet og *kvalitet* på tjenestene.

I tillegg har *pris* på tjenestene på ulike måter vært sentralt.

3.1.3 Hensynet til sikkerhet og beredskap

Problemstillinger knyttet til sikkerhet og beredskap var ikke de mest sentrale i forbindelse med fristillingen. Men i tillegg til de mer generelle samfunnspolitiske målene, blir også oppgaver eller mål innenfor sikkerhetspolitikk, forsvarspolitikk og sosialpolitikk drøftet. I flere stortingsmeldinger og -proposisjoner på 90-tallet blir det trukket fram en rekke oppgaver på teleområdet som er viktige ut fra spesielle samfunnshensyn. Slike oppgaver omtales i telepolitikken som «spesielle samfunnspålagte oppgaver». Oppgaver under denne kategorien er:

- telegram og telextjenesten mot utlandet og skip
- tjenester til totalforsvaret
- nød og sikkerhetstjenesten langs kysten og i nære havområder
- ytelser på Svalbard
- betalingstelefoner (telefonautomater).
- ytelser til funksjonshemmede.

St. meld. nr 8 (1991-92) Om televirksomheten i Norge dreide seg om avvikling av eneretter og etablering av konkurranse. Opprettholdelse av enerettene på fastnett og telefoni, ble i hovedsak begrunnet i behovet for tilfredstillende dekning. Hensynet til sikkerhet blir nevnt som viktig framover, men meldingen drøfter ikke spesielt problemstillinger knyttet til dette. Det blir vist til at Televerket pga sin sterke markedsstilling ikke ville ha behov for særskilte bevilgninger til spesielle samfunnspålagte oppgaver, her blir Kystradioen og telefon for døve nevnt spesielt. Dette var for øvrig ikke i tråd med Televerkets egen innstilling.

St. prp. nr 43 (1993-94) Om tilknytningsform for samferdselsbedriftene behandler spørsmålet om tilknytningsform for NSB, Postverket og Televerket. Sikkerhetsmessige hensyn blir trukket fram som ett av flere statlige mål på teleområdet. Samferdselsdepartementet foreslo i meldingen at det i stiftelsesdokumentet for Telenor skulle tas inn en spesiell bestemmelse om samfunnspålagte oppgaver. Denne bestemmelse skulle bli værende inntil annet ble fastsatt i lov, konsesjonsvilkår eller avtale. I stiftelsesdokumentet ble det på denne bakgrunn tatt inn en bestemmelse om at Telenor skulle videreføre Televerkets samfunnsoppgaver vederlagsfritt.

Den nye teleloven – lov om telekommunikasjon (Ot.prp. nr.36 (1994-95) – hadde en egen bestemmelse om sikring av telenett mv. Bestemmelsen ga myndighetene hjemmel for pålegg om sikringstiltak. Sikringstiltakene kunne pålegges av hensyn til rikets sikkerhet, personvern, taushetsplikt eller andre viktige samfunnsinteresser. Loven sa videre at omkostningene av slike tiltak skulle bæres av dem som gjennomfører dem.

Telenor var et såkalt §10-selskap fram til børsnoteringen i 2000[9]. Det ble derfor lagt fram egne meldinger om Telenors virksomhet annethvert år. St. meld. nr 21 (1995-96) Om Telenor AS var den første av disse meldingene. Meldingen tok blant annet opp spørsmålet om spesielle samfunnspålagte oppgaver. Dette gjaldt ytelser til totalforsvaret og nød- og sikkerhetstjenesten langs kysten.

Telenor utførte disse tjenestene uten kompensasjon. Dette ble begrunnet ut fra Telenors sterke markedsstilling. Samferdselsdepartementet varslet imidlertid at de vil komme tilbake til finansieringen av disse tjenestene. Samferdselsdepartementet viste også til at Telenor ikke hadde et tilfredstillende system for dokumentasjon av kostnadene på dette området.

I St. prp nr 70 (1995-96) Om avvikling av eksisterende eneretter i telesektoren. ble det vist til at de samfunnspålagte oppgavene skulle videreføres på dagens nivå. Om finansieringen av tjenestene skrev departementet følgende:

«De spesielle samfunnspålagte oppgavene er tjenester som ytes samfunnet som helhet og er ikke spesielt knyttet til brukerne av teletjenestene. Kostnadene, .., bør derfor ikke pålegges aktørene i telemarkedet. Regjeringen legger derfor til grunn at kostnaden skal dekkes over respektive departementers budsjetter.»

Det ble vist til at Telenor hadde beregnet kostnadene knyttet til de samfunnspålaget oppgavene til 180 mill. kroner. Det ble antydet at dette var for høyt og at departementet ville komme tilbake til saken i statsbudsjettet for 1998. Dette ble gjort i St. prp. nr 1 Tillegg nr 1 (1997-98) Justisdepartementet. Etter forhandlinger med Telenor hadde Staten ved Justisdepartementet inngått avtaler om dekning av utgiftene til tre kategorier spesielle sam-

[9] §10-selskapene har en egen bestemmelse i vedtektene om at saker av vesentlig eller prinsipiell betydning skal legges fram for generalforsamlingen.

funnspålagte oppgaver (kystradioen, Svalbard og totalforsvaret). Bevilgningen var på totalt 107 mill. kroner i 1998, fordelt med 3,5 mill til Svalbard og 52 mil. til Kystradioen og det resterende beløp til totalforsvaret.

Totalforsvarets råd for sikring av tele- og informasjonssystemer (TRSTI) ble opprettet i 1998 og erstattet det tidligere Totalforsvarets sambandsnemd som ble ledet av Telenor. TRSTI ble nedlagt i 2005.

St. meld nr 47 (2000-2001) Telesikkerhet og beredskap i et telemarked med konkurranse ble lagt fram i mai 2001. Meldingen var en bred gjennomgang av sikkerhets- og beredskapsspørsmål på teleområdet. I meldingen vises det til at telekommunikasjon er et område som mange samfunnsfunksjoner er avhengige av og at konsekvensene av svikt understreker viktigheten av å iverksette forebyggende tiltak innenfor telesikkerhet og beredskap.

Meldingen viser til at siden ikke alle som er viktige for totalforsvaret har abonnement i Telenor, bør alle operatører omfattes av samme type beredskapsforpliktelser som Telenor hadde ivaretatt etter liberaliseringen. Det vises videre til at det kan være hensiktsmessig og effektivitetsfremmende og la flere aktører konkurrere om samfunnsoppgavene. En forutsetning er at de har evne til å ivareta oppgavene. Videre bør mobiltelefoni inngå som del av totalforsvaret.

Meldingen tillegger Post- og teletilsynet et myndighetsansvar for telesikkerhet og -beredskap.

Når det gjelder finansiering av sikkerhet og –beredskap, skriver Samferdselsdepartementet at Post- og teletilsynets ordinære driftsutgifter knyttet til sikkerhet og beredskap vil kunne finansieres med gebyrer på linje med tilsynets øvrige arbeid. Når det gjelder øvrige tiltak, vil dette måtte vurderes i hvert enkelt tilfelle og finansieres over Samferdselsdepartementets budsjett der dette er aktuelt. Operatørene vil selv være ansvarlige for å sikre et minimumsnivå av sikkerhet i sine nett. I meldingen vises det til at TIFKOM-prosjektet (se nedenfor) fremmet forslag med en samlet ramme på ca. 2 mrd. kroner over 5 år. Samferdselsdepartementet legger opp til et vesentlig lavere enn nivå enn dette; med et nivå på minimum 200 mill. kr over en 5-årsperiode.

De samfunnspålagte tjenestene hadde vært pålagt Telenor i konsesjon. Dette ble endret i den nye ekom-loven. I Ot. prp. nr 58 (2002-2003) var målsettingen bl.a å gi myndighetene virkemidler for å kunne styrke konkurransen. De spesielle samfunnspålagte oppgavene blir videreført i sin helhet, bl.a. for å kunne oppfylle sikkerhets- og beredskapsmessige hensyn også i fremtiden. De samfunnspålagte oppgaver vil bli ivaretatt på annen måte enn gjennom konsesjon, enten som følge av avtale eller ved pålegg. Lovforslaget ville ikke innebære endringer av innholdet i forpliktelsene slik de inntil da hadde vært nedfelt i gjeldende rett; lov, forskrift eller konsesjon.

Regjeringen fremmet i november 2004 forslag om realisering av et første utbyggingsområde av et felles digitalt radiosamband for nød- og beredskapsetatene. Saken har vært opp i Stortinget flere ganger de siste 6 –7 årene.

3.1.4 Utredninger om telesikkerhet

I løpet av 90-tallet ble det gjennomført flere utredninger om telesikkerhet og -beredskap. De mest sentrale er kort omtalt i dette avsnittet.

I 1994 ble det besluttet å starte et samarbeidsprosjekt, Beskyttelse av samfunnet (BAS), mellom Forsvarets forskningsinstitutt (FFI) og Direktoratet for sivilt beredskap (DSB) med bakgrunn i at den sivile beredskapssektor i vid forstand trengte et mer helhetlig grunnlag for ressursallokering og et bedre system for den langsiktige planlegging. Prosjektet som konkluderte med at spesielt de tre funksjonene kraftforsyning, telekommunikasjon og ledelse/informasjon skiller seg ut som nødvendige for all samfunnsvirksomhet. Svikt innen en av disse funksjonene vil kunne medføre svikt i de fleste andre samfunnsfunksjoner.

Prosjektet ble etterfulgt av nytt prosjekt med oppdrag å utrede sårbarhet og sårbarhetsreduserende tiltak innen telekommunikasjon. Dette prosjektet fikk betegnelsen Beskyttelse av samfunnet 2 (BAS 2), og ble gjennomført i perioden september 1997 - februar 1999. BAS2-prosjektet ble gjennomført etter oppdrag fra Justisdepartementet, Samferdselsdepartementet og Direktoratet for sikkerhet og beredskap.

For å følge opp FFIs anbefalinger i BAS2-prosjektet, foreslo Totalforsvarets råd for sikring av tele- og informasjonssystemer (TRSTI), etter oppdrag fra Samferdselsdepartementet, at det burde nedsettes et nytt prosjekt som skulle bearbeide FFIs anbefalinger for å fremskaffe grunnlag for et stortingsfremlegg om telesikkerhet og -beredskap i et fritt konkurransemarked (forkortet til TIFKOM).

TIFKOM-prosjektet ble opprettet i september 1999 og leverte sin rapport i mars 2000 (Teleberedskap i et fritt konkurransemarked). Prosjektet konkluderte med at det var nødvendig å styrke robustheten i de norske telenettene og gir anbefalinger

om hvilket nivå en bør legge seg på for å sikre dette. Forslagene fra arbeidet er omtalt og drøftet i St.meld.nr 47 (2000-2001) Telesikkerhet og beredskap.

NOU 2000: 24 Et sårbart samfunn har en bred gjennomgang av sikkerhet og beredskap på IKT-området og drøfter blant annet hvilke konsekvenser liberaliseringen har for hensynet til sikkerhet og beredskap.

3.2 Aktører og virkemiddelbruk for å ivareta sikkerhet

3.2.1 Sentrale aktører

Myndighetsorganer er Samferdselsdepartementet og Post- og teletilsynet. Det overordnete ansvaret ligger i Samferdselsdepartementet. SD har også ansvar for å ivareta koordinering med andre departementer.

St.meld. nr 47 (2000 – 2001) tillegger Post- og teletilsynet et myndighetsansvar for telesikkerhet og -beredskap. Post- og teletilsynet skal:

- Sette krav til telesikkerhet og teleberedskap.
- Forestå ulike former for forebyggende og skadebøtende tiltak for å gjøre telenettene mer robuste
- Føre tilsyn med at pålagte tiltak blir iverksatt.
- Bevisstgjøring, kompetanseheving og veiledning overfor operatører, brukere og andre aktører.

Seksjonen som arbeider med sikkerhet og beredskap i Post- og teletilsynet har for tiden 10 ansatte. Finansiering av Post- og teletilsynets arbeid med sikkerhet og beredskap skjer gjennom de generelle gebyrene til Post- og teletilsynet.

Senter for informasjonssikring ble opprettet som et 3-årig prøveprosjekt finansiert av NHD (overført til MOD i 2004). Opprettelsen av senteret var en oppfølging av Sårbarhetsutvalgets innstilling. Senterets oppgave er å koordinere arbeidet knyttet til IKT-sikkerhet i Norge og å arbeide med å kartlegge trusselbilde mot IKT-systemer. Finansiering og videre drift av senteret er til vurdering[10].

Det er en rekke tilbydere av elektronisk kommunikasjon. I følge Post- og teletilsynets statistikk var det i 2004 46 tilbydere av fasttelefon, 23 tilbydere av mobiltelefon og 128 av internett. Telenor og Tele2 har markedsandeler på fasttelefon på henholdsvis 68 og 22 %. Innenfor mobiltelefoni har Telenor og Netcom markedsandeler på hhv. 55 og 29% (av totalomsetning). Selv om Telenors markedsandel er avtakende vil Telenor fortsatt ha en sentral rolle i sikkerhets- og beredskapsspørsmål fordi selskapet eier store deler av infrastrukturen. Blant annet gjelder dette anlegg i fjell som er spesielt viktige i denne sammenheng.

[10] St.prp.nr. 1 (2004-2005) Moderniseringsdepartementet.

3.2.2 Virkemiddelbruk for å ivareta sikkerhet og beredskap

Avsnittet gir en oversikt over virkemiddelbruken på sikkerhet og beredskap.

Lov og regelverk

§ 2-10 i lov om elektronisk kommunikasjon omhandler sikkerhet og beredskap. Loven omhandler tilbyders ansvar for å tilby nett med nødvendig sikkerhet for brukerer i «fred, krise og krig». Loven gir myndighetene hjemmel til å pålegge tilbyder spesielle tiltak, bl.a omfatter dette.:

- utarbeidelse av beredskapsplaner og å bidra i beredskapsøvelser
- innføring av spesielle funksjoner i systemene
- fysisk sikring av installasjoner

Det er gitt forskrift til loven som bla gir nærmere bestemmelser om beredskap og sikkerhet[11].

Loven omtaler også hvordan utgifter til sikkerhets- og beredskapstiltak skal dekkes inn. Tilbyder skal i utgangspunktet dekke kostnader ved sikkerhets- og beredskapstiltak etter denne paragrafen. Tilbyderes reelle merkostnader forbundet med levering av sikkerhets- og beredskapstiltak, skal kompenseres av staten. Siden loven er forholdsvis ny, har man i liten grad erfaringer med hvordan en slik kostnadsdeling vil kunne bli i praksis.

Loven åpner for å nekte tilbyder tilgang til markedet dersom dette er nødvendig av hensyn til offentlig sikkerhet, helse eller andre særlige forhold.

Økonomiske virkemidler

Tilskudd eller kjøp av tjenester benyttes i noen grad for å ivareta sikkerhets- og beredskapshensyn. Spesielle samfunnspålagte oppgaver (herunder beredskap og sikkerhet) ble de første årene etter selskapsdannelsen utført av Telenor AS etter pålegg fra Samferdselsdepartementet. Fra og med 1998 er disse oppgavene blitt finansiert ved at staten kjøper tjenestene av Telenor. Det vil si at staten gjør avtaler med Telenor AS om å levere spesifi-

[11] http://www.lovdata.no/for/sf/sd/td-20040216-0401-008.html

Tabell 10.2

År	mill. kroner
1998	35,0
1999	20,7
2000	37,7
2001	26,0
2002	23,2
2003	48,1
2004	55,0
2005	14,2

serte tjenester, mot dekning av merkostnader (Tillegg til St prp nr 1 (1997–98)). Forvaltningen av dette tilskuddet er nå overført til Post- og teletilsynet.

Tabellen viser bevilgningene til samfunnspålagte oppgaver vedrørende totalforsvaret i perioden 1998 til 2005. Deler av bevilgningen var fram til 2004 knyttet til nedbetaling av tidligere investeringer i sikkerhet og beredskap, bl.a Telenors anlegg i fjell.[12]

Ordningen med spesielle samfunnspålagte oppgaver (SSO) til totalforsvaret ble i sin nåværende form faset ut i 2004, jf. St.meld. nr. 47 (2000–2001). 2005 vil være et overgangsår. Post- og teletilsynet arbeider med den videre utformingen av ordningen.

Bruk av anbudskonkurranser for å ivareta sikkerhets- og beredskapsoppgaver ble vurdert i St.meld. nr 47 (2000-2001). Samferdselsdepartementet skrev bl.a. følgende:

«Prinsipielt er det intet til hinder for at andre aktører (enn Telenor) kan konkurrere om å levere de tjenestene som omfattes av USO-forpliktelsen, eller utføre spesielle samfunnspålagte oppgaver. I et etablert og velfungerende marked kan det være hensiktsmessig og effektivitetsfremmende å la flere aktører konkurrere om samfunnsoppgavene. En forutsetning for å innføre konkurranse om disse oppgavene vil imidlertid være at flere aktører har opparbeidet betryggende evne til å ivareta oppgavene på en tilfredsstillende og kontinuerlig måte i hele eller deler av landet.»

Andre virkemidler

Det er en rekke ulike virkemidler som kan benyttes i sikkerhets- og beredskapsarbeidet. Post- og teletilsynet har blant sine oppgaver å bidra til bevisstgjøring, kompetanseheving og veiledning overfor operatører, brukere og andre aktører og å arrangere felles øvelser mellom operatørene. Informasjon til befolkningen er også et virkemiddel som benyttes for å ivareta sikkerhet og beredskap.

I St. meld.nr 47 (2000-2001) omtaler ulike virkemidler på dette området, blant annet:

- Ny prioritetsordning i telenettene som sikrer prioritet til viktige abonnenter
- Tilgang til det planlagte nødnettet også for andre brukere enn politi, brann og helse.
- Investeringer i transportabelt beredskapsutstyr
- Klassifisering av teleinfrastrukturen
- Sikkerhetsevaluering av offentlige telenett
- Samøvelser hvert annet år
- Transportabelt beredskapsutstyr (alle aktører som er viktige i beredskapssammenheng bør ha dette)
- Utredning av konsekvenser av krav om nasjonal autonomi

4 Finansiering av sikkerhets- og beredskapstiltak

I dette kapitlet trekker vi fram noe av det som er skrevet om finansiering av sikkerhet og beredskap på områder der statlige virksomheter er skilt ut i selskaper. Det har i visse sammenhenger blitt pekt på at en konkurransesituasjon med sterkt prispress kan gi nedprioritering av sikkerhet med mindre sikkerhet anses som et konkurransefortrinn. På energiområdet har eksempelvis investeringsnivået gått ned i årene etter energiloven. Dette har gitt en bedre utnyttelse av ressursene, men kan også ha gått på bekostning av sikkerhet.

Både lov om elektronisk kommunikasjon og energiloven gir retningslinjer for finansiering av sikringstiltak:

- I lov om elektronisk kommunikasjon er dette omtalt på følgende måte i lovens § 2-10:
  «Tilbyder skal i utgangspunktet dekke kostnader ved sikkerhets- og beredskapstiltak etter denne paragrafen. Tilbyderes reelle merkostnader forbundet med levering av sikkerhets- og beredskapstiltak, skal kompenseres av staten med basis i fyldestgjørende dokumentasjon som fremskaffes av tilbydere. Med merkostnad menes kostnad som vil falle bort uten pålegget, utover kostnaden ved en ren kommersiell tilpasning.»

  I energiloven har § 6-4 følgende ordlyd:
  «Selskaper som driver virksomhet som omfattes av dette kapittel, kan pålegges for egen regning å sette i verk de sikringstiltak som departementet i hvert enkelt tilfelle finner påkrevd.

[12] FFI rapport 2000/00131: Finansiering og organisering av beredskap innen telekommunikasjon og kraftforsyning.

Medfører gjennomføringen av et pålegg vesentlige utgifter for selskapet som ikke oppveies av motsvarende fordeler, fastsetter departementet det vederlag selskapet skal ha.»

Gjennom lovverket pålegges tilbyder å finansiere tiltakene, men det åpnes opp for at staten kan dekke deler av utgiftene. Vi har ikke undersøkt hvordan disse lovene følges opp. Vi ser imidlertid av bevilgningene til denne type tiltak, at beløpene er lave. På teleområdet går alle midlene foreløpig til Telenor. Ekom-loven er imidlertid forholdsvis ny og Post- og teletilsynet arbeider med den konkrete oppfølgingen.

Spørsmålet om finansiering av sikkerhets- og beredskapstiltak har vært berørt i flere offentlige dokumenter de siste årene. I St meld nr 25 (1997-98) Hovedretningslinjer for det sivile beredskaps virksomhet og utvikling i tiden 1999-2002 skriver Justisdepartementet følgende om de «beredskapsmessige konsekvenser ved endring av tilknytningsformer for statlige virksomheter»:

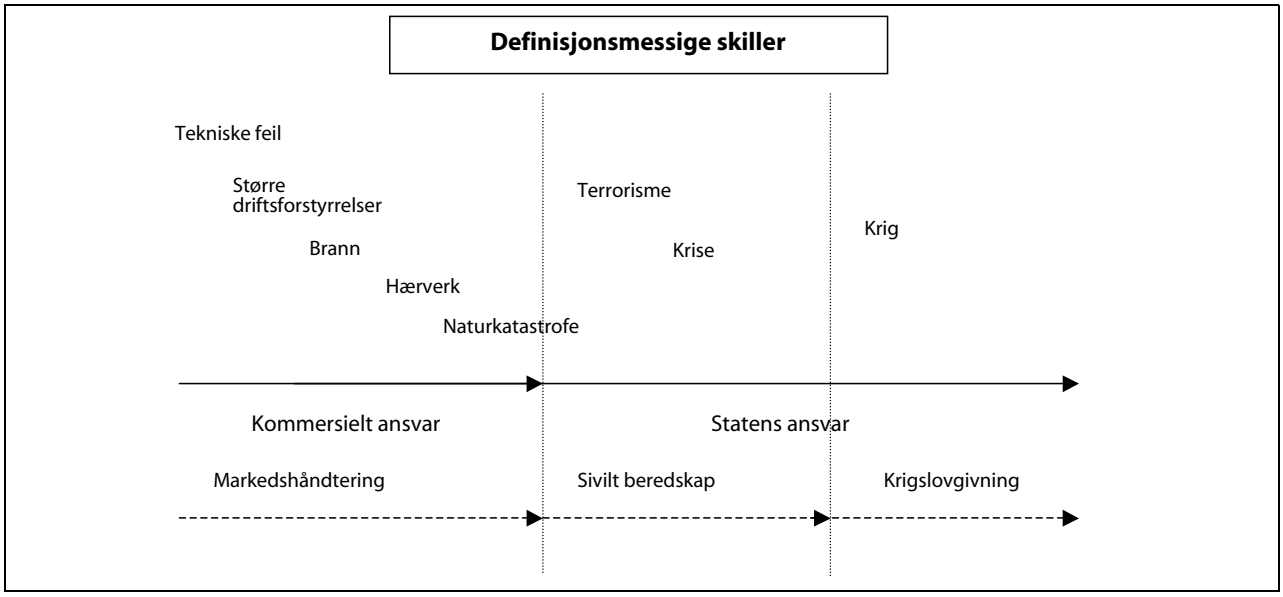
«Utviklingen (med endring i tilknytningsform) stiller således det sivile beredskap overfor særskilte utfordringer. Det er viktig å opprettholde et forsvarlig beredskapsnivå i flere av de omdannede selskaper. En statlig finansiering av slike tjenester vil kunne innebære et betydelig økt bevilgningsbehov over programområde 05. Dette er utgifter som tidligere har vært en kostnad knyttet til disse virksomhetenes drift og ikke vært synliggjort ved statlige bevilgninger bortsett fra mindre bevilgninger over 05-området.»

Sårbarhetsutvalget skriver følgende om finansiering av beredskapstiltak på energiområdet:

«Det gis til en viss grad tilskudd til investeringer i beredskapstiltak, men for en stor del overlates finansieringen av dette til den enkelte virksomhet. Lov- og regelverket åpner for at dette er utgifter som virksomhetene selv må dekke, jf. energilovens §6-4. Gitt de store endringene i rammevilkårene det siste tiåret har det vært pekt på at denne finansieringsordningen svekker beredskapen og øker sårbarheten. Innenfor dagens regime legges det sterkere avkastningskrav på virksomhetene. Dette gjelder også monopolvirksomheten. Nettmonopolene inntektsreguleres, det vil i praksis si at NVE setter et tak på hvor mye nettselskapene kan tjene samtidig som de forutsetter en årlig effektivitetsforbedring. En slik regulering gjør at beredskapstiltak må »konkurrere« med andre tiltak og kostnader innenfor en fastsatt inntektsramme. Beredskapsinvesteringer reduserer inntjeningen. »

I St meld nr 47 (2000-2001) om telesikkerhet skriver Samferdselsdepartementet følgende om finansiering av beredskapstiltak:

«For de øvrige telesikkerhets- og teleberedskapstiltak vil det måtte foretas en nærmere konkret vurdering av hvilke finansielle virkemidler som er best egnet i det enkelte tilfelle. Det er viktig at det ved vurderingen sikres at finansieringen ikke gir utilsiktede konkurransevridninger eller skaper ulik belastning for noen av de berørte parter. Finansiering av konkrete tiltak vil kunne skje gjennom gebyrer, avgifter, egenfinansiering (operatørfinan-



Figur 10.1 Utfordringer og ansvarsfordeling (Kilde: FFI-rapport 2000/001331 – noe forenklet)

siering), kundefinansiering eller bevilgninger over statsbudsjettet. Hvilken finansieringsmåte som passer best vil avhenge av det konkrete tiltak. Endelig valg av regulerings- og finansieringsmåte må besluttes i det enkelte tilfelle. I tilfeller der det eventuelt kan være hensiktsmessig at tiltak finansieres med bevilgninger over statsbudsjettet, vil Samferdselsdepartementet komme konkret tilbake med bevilgningsforslag i forbindelse med de årlige budsjettforslagene»

Forsvarets forskningsinstitutt (FFI) skrev i 2000 en rapport om finansiering og organisering av beredskap innen telekommunikasjon og kraftforsyning[13].

Forsvarets forskningsinstitutt har i et prosjekt illustrert et syn på fordeling av ansvar for ulike typer sikkerhetsmessige utfordringer. [Figur 9.1]

Utfordringer som ligger til venstre i figuren vil være et kommersielt ansvar, mens når man beveger seg over mot høyre i figuren vil myndighetene (staten) få et større ansvar. En slik figur kan være et utgangspunkt for å diskutere ansvarsdelingen ved finansiering av sikkerhets- og beresdskapstiltak.

5 Oppsummering

5.1 Hensynet til sikkerhet og beredskap i fristillingen

Gjennom fristilling er statlige monopolordninger blitt avviklet og konkurransemarkeder etablert. Det er flere årsaker til at de ulike sektorene ble liberalisert, men både på tele- og kraftområdet var effektivisering og bedre utnyttelse av ressursene viktige hensyn.

På begge områdene ble det i forbindelse med fristillingen understreket at de overordnete samfunnspolitiske målsettingene ville ligge fast etter fristillingene. Dette var i hovedsak målsettinger knyttet til lik tilgang til tjenestene over hele landet, målsettinger om tilnærmet like priser(tele) mv. Hensynet til sikkerhet og beredskap er ikke spesielt drøftet i stortingsdokumenter knyttet til fristillingene, men forpliktelser på dette området for de berørte aktørene ble i stor grad videreført.

Hensynet til sikkerhet og beredskap ble på begge sektorer ivaretatt gjennom bestemmelser i lovverket. Lovverket ga myndighetene hjemmel for å pålegge aktørene å gjennomføre og dekke kostnadene ved ulike typer sikringstiltak.

På kraftsektoren har NVE gjennom hele perioden hatt et ansvar for sikkerhet og beredskap, og Kraftforsyningens beredskapsorganisasjon ble omtalt i energiloven fra 1990. På teleområdet fikk ikke Post- og teletilsynet et tilsvarende ansvar før i forbindelse med St. meld nr 47 (2000-2001), dvs. flere år etter at Telenor var blitt aksjeselskap, men omtrent samtidig med at selskapet ble børsintrodusert.

Sikkerhet og beredskapshensyn er blitt tatt opp med jevne mellomrom i årene etter fristillingen. Dette har ført til større og mindre endringer i organisering, regulering og finansiering av området. Ett inntrykk er at det har vært gjort mest endringer i etterkant på teleområdet. Dette kan skyldes at det tradisjonelt har vært stor oppmerksomhet omkring sikkerhet og beredskap innenfor kraftsektoren fordi dette området er svært utsatt for vær og vind. Kraftsektoren besto av mange ulike aktører også før energiloven trådde i kraft, slik at myndighetene hadde lenger tradisjon for å jobbe med ulike aktører i denne type spørsmål. På teleområdet hadde ansvaret for sikkerhets- og beredskapsspørsmål i stor grad blitt ivaretatt av Televerket.

Årsakene til at spørsmålet om sikkerhet og beredskap er tatt opp i årene etter fristillingene varierer. På kraftområdet ble dette spørsmålet viet oppmerksomhet etter flommen i 1996, men i særlig grad etter den nedbørfattige sesongen og kraftkrisen i 2002/2003. På teleområdet ble spørsmålet grundig drøftet i stortingsmeldingen i 2000. Dette falt sammen i tid med at forvaltningen av eierskapet til Telenor ble overført fra Samferdselsdepartementet til Nærings- og handelsdepartementet. Mindre endringer er tatt opp i forbindelse med andre revisjoner av lov- og regelverk på området.

De rådgivende organene er avviklet på begge områder. På kraftområdet ble dette begrunnet med at rådet hadde fått mindre betydning fordi beredskapsarbeidet er samlet i NVE. På teleområdet kan tilsvarende begrunnelse ha blitt brukt.

5.2 Virkemidler for å ivareta sikkerhet og beredskap

Tabellen nedenfor gir en oppsummering av virkemiddelbruken på området. Det er klare likheter i hvilke virkemidler som benyttes på de to områdene. Lovregulering er det sentrale virkemiddelet. Vi ser også at tilsynene på begge områder har en svært viktig rolle på sikkerhets- og beredskapsområdet.

Den vesentligste forskjellen i virkemiddelbruk finner vi på det organisatoriske. På energisiden er

[13] FFI/RAPPORT-2000/00131

Tabell 10.3

	Energi	Tele
Lov	Ja	Ja
Konsesjon*	Ja	Ja
Tilsyn	NVE	Post- og teletilsynet
Annen organisering	KBO	nei
Finansiering av tilsyn	Inngår i generelle gebyrer til tilsynet	Inngår i generelle gebyrer til tilsynet
Finansiering over statsbudsjettet (tilskudd/kjøp av tjenester)	2,6 mill. i 2005	14 mill. kr i 2005
Beredskapsøvelser	Ja	Ja
Beredskapsplaner	Ja	Ja
Eierstyring	Muligheten er til stede gjennom eierskapet i Statnett og Statkraft	Nei

* Det er konsesjonsplikt på begge områder, men det pålegges ikke spesielle oppgaver knyttet til konsesjonen.

det etablert en beredskapsorganisasjon der alle enheter som produserer eller distribuerer strøm er medlem. Tilsvarende finner vi ikke på teleområdet. Det er også ulikheter knyttet til eierskapet. Staten er fortsatt eneeier i Statnett og Statkraft. Dette gir mulighet for styring gjennom foretaksmøte/generalforsamling. Dette er en mulighet som i veldig liten grad benyttes, men kan være en type «sikkerhetsforanstaltning» bl.a. i forhold til beredskap.

5.3 Finansiering av beredskapstiltak

Finansiering av beredskap på områder der det har skjedd selskapsetableringer er blitt tatt opp i flere sammenhenger. Det er blitt pekt på at avvikling av monopoler kan være gunstig for beredskap fordi det vil være flere aktuelle leverandører å spille. En konkurransesituasjon kan imidlertid føre til prispress som gjør at det ikke investeres nok i sikkerhet og beredskap.

Sentrale problemstillinger er blant annet følgende:

- Hvor går grensen mellom statens ansvar og leverandør/tilbyders ansvar for finansiering av sikkerhets- og beredskapstiltak?
- Hvordan skal en eventuell statlig støtte innrettes for
  a) Ikke å virke konkurransevridende
  b) For at ressursene skal kunne utnyttes så effektivt som mulig.

Litteraturliste

Norges offentlige utredninger

NOU 1985:9 Energilovgivningen
NOU 2000:24 Et sårbart samfunn - Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet
NOU 2003:34 Mellom stat og marked – selvstendige organisasjonsformer i staten

Stortingsmeldinger

St meld nr 25 (1997-98) Hovedretningslinjer for den sivile beredskaps virksomhet og utvikling i tiden 1999-2001
St meld. nr. 17 (2001-2002) Samfunnssikkerhet – veien til et mindre sårbart samfunn
St meld. nr. 8 (1991-92) Om televirksomheten i Norge
St meld. nr. 21 (1995-96) Om Telenor AS
St meld. nr. 17 (1997-98) Om Telenor si verksemd
St meld. nr. 24 (1998-99) Om enkelte regulatoriske spørsmål i telesektoren
St meld. nr. 47 (2000-01) Telesikkerhet og beredskap i et telemarked med fri konkurranse
St meld. nr. 46 (1992-93) Om langsiktig kraftutveksling med utlandet
St meld. nr. 11 (1995-96) Om organiseringen av krafthandelen med Sverige

St.meld. nr. 29 (1998-99)	Om energipolitikken
St.meld. nr. 18 (2003-04)	Om forsyningssikkerheten for strøm mv.

Stortingsproposisjoner

St.prp. nr. 57 (1984-85)	Om endringer i Norges vassdrags- og elektrisitetsvesens organisasjon
St.prp. nr. 100 (1990-91)	Omorganisering av Statkraft
St.prp. nr. 81 (1991-92)	Om omorganisering av utenlandshandelen med elektrisk kraft
St.prp. nr. 37 (1994-95)	Om oppgjørsordningen for utenlandshandelen med kraft og enkelte forhold knyttet til ELSAM-avtalen
St.prp. nr. 1 (1995-96)	Olje- og energidepartementet
St.prp. nr. 43 (1993-94)	Tilknytningsform for samferdselsbedriftene
St.prp. nr. 70 (1995-96)	Avvikling av resterende eneretter i telesektoren
Tillegg nr. 1 (1997-98)	Om endring av proposisjonen om Statsbudsjettet 1998 som følge av opphevelse av eksisterende eneretter i telesektoren
St.prp. nr. 1	Samferdselsdepartementet, for budsjetterminen 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004 og 2005
St.prp. nr. 95 (2000-2001)	Statens eierandel i Telenor ASA
St.prp. nr. 1 (2004-2005)	Moderniserngsdepartementet

Odelstingsproposisjoner

Ot.prp. nr. 73 (1988-89)	Om lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (Energiloven)
Ot.prp. nr. 43 (1989-90)	Om lov om produksjon, omforming, overføring, omsetning og fordeling av energi m.m. (Energiloven)
Ot.prp. nr. 56 (2000-01)	Om lov om produksjon, omforming, overføring, omsetning og fordeling av energi m.m. (Energiloven)
Ot.prp. nr. 61 (1993-94)	Om lov om omdanning av forvaltningsbedrifta Televerket til aksjeselskap
Ot.prp. nr. 36 (1994-95)	Om lov om telekommunikasjon
Ot.prp. nr. 31 (1997-98)	Om lov om endringer i lov av 23 juni 1995 nr 39 om telekommunikasjon
Ot.prp. nr. 58 (2002-2003)	Om lov om elektronisk kommunikasjon

Annet

Lovdatabasen:Diverse lover
Departementenes hjemmesider: www.odin.dep.no
Post- og teletilsynets hjemmesider: www.npt.no
Olje- og energidepartementet: Faktahefte, 2004
FFI-rapport: Finansiering og organisering av beredskap innen telekommunikasjon og kraftforsyning, 2000
Post- og teletilsynet: Det norske telemarkedet 2004
Statskonsult: I godt selskap, rapport 1998:21
Statskonsult: Statlig eierskap og sektorstyring, rapport 1999:16
Statskonsult: Spiller det noen rolle?, rapport 2001:17
Statskonsult: Virkemiddelbruk og sektorstyring, rapport 2001:19

Vedlegg 11

Navigasjonssystemer og samfunnssikkerheten

Arbeidsnotat til Infrastrukturutvalget

Hans M. Synstnes. Rådgiver, Nasjonal sikkerhetsmyndighet, 9. februar 2005.

1 Bakgrunn

1.1 Innledning

Utvalget for sikring av landets kritiske infrastruktur (Infrastrukturutvalget) skal vurdere hvordan hensynet til rikets sikkerhet og vitale nasjonale interesser på best mulig vis kan ivaretas overfor virksomheter som ikke er offentlige. Eksempler på områder som utvalget skal vurdere er kraftsektoren, telesektoren, vannforsyningen, m.m. Utvalgets arbeid skal omfatte alle typer installasjoner og systemer som er nødvendige for at samfunnet skal fungere tilnærmet normalt. [1]

NSM er bedt om å komme med et innspill om samfunnets avhengighet av navigasjonssystemer.

1.2 Generelt om navigasjonssystemer

Samfunnets økende avhengighet av kritisk infrastruktur er etter hvert godt dokumentert gjennom eksempelvis Beskyttelse av samfunnet-prosjektene (BAS) og sårbarhetsutvalget.[2] Navigasjonssystemer fremstår som et konkret eksempel på samfunnets avhengighet av kritisk infrastruktur. Likevel ble sikkerhetsutfordringer tilknyttet navigasjonssystemer verken omhandlet i BAS-prosjektene eller i sårbarhetsutvalgets NOU – *Et sårbart samfunn*. En årsak til at BAS-prosjektene ikke har inkludert navigasjonssystemer har vært føringer om å ha et nasjonalt fokus.[3]

Navigasjonssystemene er først og fremst en understøttende infrastruktur til en rekke andre infrastrukturer og aktiviteter i samfunnet. Understøttelsen skjer i form av tids- og posisjoneringsinformasjon. Navigasjonssystemenes leveranser av tids- og posisjoneringsdata underbygger de gjensidige avhengighetsforhold som preger moderne infrastruktur. Med andre ord vil fravær av, eller manipulerte navigasjonsdata, påvirke funksjonaliteten i andre infrastrukturer. Akkumulert vil funksjonssvikt i navigasjonssystemene kunne ha betydning både for samfunnssikkerheten og den nasjonale sikkerheten.

Frem til i dag har særlig amerikanske Global Positioning System (GPS) stått sentralt. Gjennom 24 satellitter og ulike bakkeinstallasjoner betjener GPS en rekke samfunnsfunksjoner med navigasjonsinformasjon. Siden såpass mange kritiske samfunnsfunksjoner har gjort seg avhengige av GPS alene, utgjør dette en sårbarhet. Sårbarheten vil imidlertid fra 2008[4] reduseres ettersom et eget europeisk navigasjonssystem, Galileo, vil være operativt. Galileo og GPS vil være kompatible og interoperable systemer. Ved siden av disse systemene benyttes også det russiske satellittbaserte navigasjonssystemet GLONASS av enkelte aktører i Norge.

Galileo vil bidra til at samfunnet moderniseres og effektiviseres. Samtidig innebærer utformingen og driften av et slik system en rekke sikkerhetsmessige utfordringer. Ulike sikkerhetsmessige utfordringer tilknyttet samfunnssikkerheten vil bli forsterket, mens andre vil bli skapt. Til forskjell fra GPS har Norge en viss innflytelse på utviklingen av Galileo-systemet. Målsetningen bør i et samfunnssikkerhetsperspektiv være å bidra til at Galileo blir et så pålitelig og sikkert system som mulig i fred, krise og krig.

Systemet vil bidra til å forme vårt fremtidige samfunn, og vil selvsagt også ha sikkerhetspolitiske implikasjoner. Systemet vil mellom annet bidra til å forsterke globaliseringsprosessene. Dette illustreres ikke minst gjennom systemets globale brukerflate, og gjennom at land som Kina, Ukraina, India, Russland, Israel og Canada blir involvert i prosjektet gjennom bidrag tilknyttet utviklingen, utveksling av teknologi og brukerrettigheter. I tillegg vil ulike bakkeinstallasjoner bli

[1] Kongelig resolusjon – Etablering av utvalg for sikring av landets kritiske infrastruktur

[2] NOU 2000: 24 Et sårbart samfunn – Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet

[3] Jfr Forsker Janne Hagen FFI/BAS-prosjektene

[4] EU opererer offisielt med at systemet skal være operativt fra 2008. Realismen i dette er noe uklar, enkelte mener 2010 er et mer realistisk tidspunkt for et operativt Galileo.

plassert i ulike verdensdeler. En avtale signert mellom USA og EU fra juni 2004 legger grunnlaget for full kompatibilitet og interoperabilitet mellom Galileo og GPS. Avtalen stipulerer videre at vedrørende sivile signaler skal Galileos signaler fremstå som internasjonal standard.[5]

1.3 Bruksområde for navigasjonssystemer

Eksempler på bruksområder for navigasjonssystemene er innen alle deler av transportsektoren, energisektoren, landbrukssektoren, telekommunikasjon, finanssektoren, fiskerisektoren, miljøsektoren, nødetatene og nettverksbaserte militærvesen.

Galileosystemet vil, som GPS gjør i dag, gi korrekt tidsangivelse i tillegg til posisjoneringsdata. I Galileosatelittene vil det være installert atomklokker som gjør nøyaktig tidsangivelse mulig. Kombinasjonen av synkronisert posisjons- og tidsangivelse gir et svært stort effektiviseringspotensial – ikke minst for objekter som er i bevegelse. Presis tidsangivelse fremstår eksempelvis også som viktig for korrekte finanstransaksjoner. På samme tid som effektiviteten i infrastrukturer økes vil imidlertid sårbarheter kunne bli forsterket eller skapt.

Tolkning av mandat

Infrastrukturutvalgets mandat er noe snevert i forhold til de muligheter og utfordringer satellittbaserte navigasjonssystemene GPS og Galileo anskueliggjør. Mandatet angir et nasjonalt fokus hvor nasjonale aktører og nasjonale virkemidler fremstår som sentralt. Ettersom Galileo er et flernasjonalt system, og GPS et amerikansk system, kan systemet vanskelig ses innenfor en nasjonal politisk og juridisk ramme. Virkemidlene vil bare i begrenset grad være nasjonale, men snarere være preget av fellesløsninger og fellesforetak. Mandatet til infrastrukturutvalget kan derfor sies å være noe mangelfullt i forhold til å kunne fange inn helheten i de sikkerhetsmessige utfordringer som tilligger beskyttelsen av kritisk infrastruktur samfunnet er avhengig av.

2 Global Positioning System

2.1 Hva er GPS?

GPS er et satellittbasert globaldekkende navigasjonssystem under kontroll av det amerikanske forsvarsdepartementet. GPS ble utviklet for militært bruk, men systemet ble i 1980 årene stilt til disposisjon for sivil bruk. Systemet har spilt en viktig rolle i forhold til økonomisk utvikling og vekst, samt tjenester og effektivitet innen en rekke infrastrukturer verden over. En fortsatt økende bruk og økt presisjonsnivå i GPS vil innebære nye muligheter, men også sårbarheter relevant for samfunnssikkerheten og den økonomiske veksten.[6]

Det ligger mekanismer inne som vil kunne forstyrre den sivile bruken, mens amerikanske og allierte militære styrker er utstyrt med spesielle militære GPS-mottagere skal kunne operere uhindret.[7] Norge har tilgang til den militære del av GPS, GPS/Precise Positioning Service (GPS/PPS) gjennom egen avtale mellom USA og NATOs medlemsland.[8]

2.2 Sårbarheter tilliggende GPS

Svakhetene ved GPS kan grovt deles inn i kategorier som 1) feilkilder tilliggende systemet, 2) feilkilder som resultat av villede hendelser og 3) sårbarheter tilliggende bakkeinfrastruktur.[9] [10] Det verst tenkelige scenarioet vil oppstå dersom GPS settes ut av spill gjennom direkte angrep på satellittene. Dette scenarioet fremstår likevel som lite sannsynelig, selv om det på ingen måte avskrives av amerikanske myndigheter.[11]

Mer relevant er problematikken rundt utilsiktet interferens av signalene i GPS. Amerikanske Volpe National Transportation Systems Center har utredet ulike sårbarheter tilliggende GPS. Rapporten fra Volpe påviser at forstyrrelser fra andre radiotjenester, eksempelvis VHF-radio og radar om bord i ulike fartøy, kan medføre interferens. Et annet problem er at naturformasjoner eller høye bygninger kan skygge for signalene, eller reflektere dem slik at feil posisjon oppgis.

Volpe-rapporten behandler også feilkilder utløst av villede hendelser. Bruk av jammeutstyr er

[5] European Commission Directorate-General for Energy and Transport, GALILEO – The final countdown. Desember 2004. S. 3.

[6] U.S. Space-Based positioning, Navigation and Timing Policy. December 15, 2004., s 2.

[7] Sikkerhetspolitikk i verdensrommet - av Forsker Terje Wahl ved FFI.

[8] Jfr Lars Giske NRS.

[9] «Vulnerability assessment of the Transportation Infrastructure Relying on The Global Positioning System» Prepared by John A. Volpe National Transportation Systems Center – For Office of the Assistant Secretary for Transportation Policy U.S. Department of Transportation (2001).

[10] «Study into impact on capability of UK Commercial and Domestic Services Resulting from loss of GPS Signals» QinetiQ (2001).

[11] «Vulnerability assessment of the Transportation Infrastructure Relying on The Global Positioning System» Prepared by John A. Volpe National Transportation Systems Center – For Office of the Assistant Secretary for Transportation Policy U.S. Department of Transportation (2001). Side s. 2.

en kilde til tilsiktet interferens. De fleste militærvesen har kraftig jammeutstyr, gjerne montert på fly, som kan forstyrre eller avskjære GPS-signalene over store områder. Samtidig finner man på Internett nøyaktige beskrivelser av hvordan man kan skaffe seg lett bærbart utstyr til å jamme GPS-mottakere i over hundre kilometers avstand (se eksempel i vedlegg).[12] Med eget utstyr kan man også sende ut falske signaler som får mottakerne til å vise feil posisjon.

Se eget vedlegg om mer informasjon om kilder for GPS signalfeil. [13]

2.3 Modernisering av GPS

Gjennom *U.S. Space-Based positioning, Navigation and Timing Policy* fra desember 2004, setter USA klare målsettinger for sin fremtidige navigasjonspolitikk. En rekke ambisiøse målsetninger er nedfelt i dette policydokumentet, herunder en betydelig oppgradering av GPS-systemet. Det overordnede målet er å sikre at USA opprettholder posisjonerings, navigasjon og tidsangivelsessystemer, back-up systemer og tjenestenektkapasiteter. Målsetningen er å styrke tids- og posisjoneringssignalenes integritet, konfidensialitet og tilgjengelighet. En slik utbedring skal igjen være et grunnlag for økt økonomisk vekst, bedret sikkerhet i infrastrukturer og bedret nasjonal sikkerhet.[14]

2.4 GPS og norske sikkerhetsinteresser

Ettersom GPS er amerikansk kontrollert er det begrenset hva Norge kan gjøre i forhold til systemets robusthet, sikkerhet og i særlige situasjoner tilgjengeligheten til signalene.

Likevel fremstår GPS som sentralt for norske sikkerhetsinteresser ettersom sentral kritisk infrastrukturer er såpass avhengig av navigasjonsdata. En naturlig konsekvens av dette må være at norske myndigheter vurderer enkelte tiltak for å håndtere sårbarheter tilliggende GPS. Ulike virkemidler kan være:

- FoU-arbeid for å kartlegge hvilke avhengighetsforhold, sårbarheter og beskyttelsestiltak som tilligger bruk av navigasjonssystemer
- Gjennomføre risiko- og sårbarhetsanalyser for å kartlegge konsekvenser av forringelse av signaltrafikken, eller fravær av navigasjonsdata.
- Utarbeide kriseplaner og system for krisehåndtering dersom navigasjonsdataene uteblir eller er forringet.
- Øve alternative handlingsmønstre dersom GPS-signalene forringes eller faller ut
- Forberede overgang til interoperabilitet med Galileo – hvilket sikrer en reserveløsning dersom GPS svikter.
- Vurdere ulike back-up løsninger (LORAN C). Norge er i ferd med å avvikle LORAN C, mens andre land som eksempelvis Frankrike og Storbritannia ønsker å opprettholde LORAN C. Systemet er i Norge brukt primært maritimt og av Forsvaret.

3 Galileo

3.1 Hva er Galileo?

Galileo er et europeisk initiativ for å opprette et nytt globalt system for satellittnavigasjon. Galileosystemet fremstår som den første fellesstrategiske europeiske infrastrukturen. Navigasjonssystemet må således ses som et viktig strategisk tilfang til, og fasilitator for, den felleseuropeiske forsvars- og sikkerhetspolitikken. Et egenkontrollert navigasjonssystem vil gjøre EU mer uavhengig av USA.

Generelt vil systemet få store teknologiske, økonomiske, industrielle og politiske ringvirkninger, ikke minst for de europeiske nasjonene. Systemet vil få betydning for et mangfold av sektorer (jfr pkt 1.3).

Systemet opprettes som et felles foretak mellom European Space Agency (ESA) og EU, men vil etter hvert bli et EU-kontrollert og drevet system. Galileosystemet vil bestå av rundt 30 satellitter (27 operative og 3 reserve). To kontrollsentre skal opprettes i Europa. Ulike andre understøttende bakkesegmenter[15] vil plasseres rundt om på kloden.[16] Svalbard fremstår her som et alternativ for utplassering av bakkesegment.

Selve driften av det operative Galileosystemet vil bli utøvd av en privat aktør.[17]

---

[12] Vedlegg: Utdrag fra «The Instant Lessons of the Iraq War» Main Report. Eight Working Draft: May 14, 2003. Anthony H Cordesman, Arleigh A Burke Chair for Strategy. Center for Strategic and International Studies (US).

[13] Vedlegg: Oversikt over sårbarheter i navigasjonssystemer. www.romsenter.no

[14] U.S. Space-Based positioning, Navigation and Timing Policy. December 15, 2004, s 3.

[15] L-band Sensor Stations (GSS), C-band Up-Link Stations (ULS) og S-band Telemetry and Telecommand Stations (TTC) – i tillegg til 2 Galileo Control Centre (GCC).

[16] ESA/PB-NAV(2004)42 European Speace Agency – Programme Board on Satellite Navigation – Galileo IOV Ground Stations site selection. 23.11.2004.

[17] Tildelingen står mellom konsortiet «Inavsat» bestående av European Aeronautic Defence and Space Company (EADS), Thales og Inmarsat og konsortiet «Eurely» bestående av Alcatel og Finmeccania.

3.2 Sikkerhetsfokus i Galileoprosjektet

Medlemslandene i EU har erkjent at Galileo innebærer store sikkerhetsmessige utfordringer på ulike plan. Av den grunn nedlegger medlemslandene betydelige ressurser for at Galileo skal bli et sikkert og pålitelig system. Innsatsen som nedlegges på sikkerhetssiden viser med tydelighet at EU-landene anser Galileo som en særlig vital del av den samlede kritiske infrastrukturen i Europa.

Galileo Security Board (GSB) har fremstått som det organet i EU som har håndtert de sikkerhetsmessige utfordringene tilliggende Galileoprosjektet. EUs ministerråd vedtok imidlertid i juni 2004 at Galileo etter hvert skal bli monitorert og beskyttet gjennom den organisatoriske nyvinningen European Global Navigation Satellite System (GNSS) Supervisory Authority (GSA). Etableringen av Galileo Safety og Security Committee under GSA vil trolig skje omkring oktober/november 2005.[18] Administrative Board under GSA, hvor en representant fra hvert EU-medlemsland vil sitte forsøkes etablert så fort som mulig på nyåret.[19] Oppgavene som i dag løses av GSB vil bli videreført av GNSS Supervisory Authority og GSB følgelig nedlagt.

NSM har i dag observatørstatus i GSB og underliggende arbeidsgrupper. NSM og Norsk Romsenter (NRS) deltar på møtene i GSB, samt noen av møtene i arbeidsgruppene.

Norge er også med i et gradert flerlandssamarbeidet innen Galileoprosjektet, hvilket muliggjør tilgang på sikkerhetsgradert informasjon og mulighet for norsk industri til å konkurrere om sikkerhetsgraderte oppdrag. En egen bilateral sikkerhetsavtale mellom Norge og EU, som muliggjør utveksling av sikkerhetsgradert mellom de to parter, er også inngått.

3.3 Joint Action – EUs krisehåndtering

EU vier som nevnt de sikkerhetsmessige sidene av Galileosystemet særlig oppmerksomhet. Målsetningen er å sikre politiske og juridiske mekanismer som gjør at EU kan opprettholde kontroll dersom Galileo utsettes for skadeverk. For situasjoner hvor bruken av systemet kan ha betydning for sikkerheten til EU eller unionens medlemsland, har EUs råd nedsatt noen viktige prinsipper i *Council Joint Action 2004/552/CFSP of 12 July 2004 on the aspects of the operation of the European satellite radio-navigation system affecting the security of the European Union.*[20]

Council Joint Action legger opp til at krisehåndteringen vil skje i et samspill mellom konsesjonæren, EU ved GNSS/GSA og nasjonene. Myndighetsorganer i EU sikrer seg her muligheten til å gi pålegg i spørsmål vedrørende overordnede sikkerhetsbehov – uten å spesifisere hvilke tiltak eller virkemidler som vil være aktuelle.

3.4 Særlig om Public Regulated Service

Galileos betydning for samfunnssikkerheten illustreres gjennom systemets ulike brukernivåer. Tjenester vil bli levert på flere nivåer med hensyn til signalenes konfidensialitet, integritet og tilgjengelighet. For det øverste nivået, Public Regulated Service (PRS), vil tilgangen være strengt myndighetskontrollert, og begrenset til applikasjoner ment for mellom annet redningstjeneste, politi, drift av annen særlig kritisk infrastruktur og trolig fremtidig nettverksbaserte militærvesen

Nasjonene innen EU står fritt til å inngå i PRS delen av Galileo. De som ønsker å delta må imidlertid delta med å finansiere og utvikle PRS. Det er også sannsynelig at Norge kan delta i PRS – foreløpig er det ikke gjort noen politisk vurdering omkring hvorvidt Norge ønsker å inngå i PRS delen.

De nasjoner som velger å involvere seg i PRS vil være i en teknologisk frontposisjon, og vil kunne utnytte dette til fordel for den nasjonale samfunnssikkerheten.

3.5 Sårbarheter tilliggende Galileo

En sikkerhetsmessig målsetning med Galileo er å fjerne eller redusere sårbarheter vi i dag kjenner fra GPS slik disse er beskrevet tidligere i dette notatet, og skape økt redundans og dermed redusert samfunnsårbarhet. I tillegg er det en målsetning å gjøre Galileo mer presist og enda mer pålitelig enn dagens GPS. Selv om begrunnelsen for Galileo i første rekke er sivil, har erkjennelsen av de sikkerhetsmessige og militære implikasjonene for eieren av et slikt system etter hvert fått større fokus. Ulike trusler i denne sammenhengen nødvendiggjør behovet for å beskytte seg mot:

- systemsvakheter som kan forstyrre signalenes integritet og tilgjengelighet
- ondsinnede aktørers bruk av systemet

[18] Jfr Jeremy Godet fra EU Kommisjonen under møte i GSB WG 4 - 15 desember 2004.

[19] Jfr Jeremy Godet fra EU Kommisjonen under møte i GSB WG 4 - 15 desember 2004.

[20] Council Joint Action 2004/552/CFSP of 12 July 2004 on the aspects of the operation of the European satellite radio-navigation system affecting the security of the European Union. Paragraf (4).

- skadeverk og/eller ødeleggelse av satellitter, bakkeinstallasjoner, korreksjonsmekanismer og mottakerutstyr
- ondsinnet påvirkning av signalenes konfidensialitet, integritet og tilgjengelighet
- kompromittering av ESA, EU eller nasjonal Galileo-relatert informasjon eller Galileo-relaterte objekter.

3.6 Norge og Galileo

Regjeringen har nå vedtatt å søke om å få starte forhandlinger om deltagelse på EU-siden av Galileo. Dette vil bidra til at norske behov innen satellittnavigasjon kan bli tatt vare på i den videre utviklingen av systemet, og det vil gi norske høyteknologibedrifter anledning til å konkurrere om utviklingsoppdrag til satellitter og bakkestasjoner i Galileo. Norge bidrar med totalt 152 millioner kroner til utviklingsfasen av prosjektet. Dersom Norge også blir med i utbyggingsfasen, har industrien håp om større kontrakter.

Det nasjonale koordineringsansvaret for Galileo ble i høst formelt overført til Nærings- og handelsdepartementet (NHD). NHD har igjen utpekt Norsk Romsenter (NRS) til nasjonalt prosjektkontor (NPO) i forbindelse med Galileo. Overføringen av koordineringsansvaret til NHD og NRS vil bedre den nasjonale koordineringen av Galileoprosjektet. NHD og NRS vil også forhandle frem en konkret samarbeidsavtale med EU.

Selv om NHD har overtatt koordineringsansvaret for Galileo har Fiskeridepartementet fremdeles ansvar for å koordinere den nasjonale navigasjonspolitikken.

4 Navigasjonssystemer, norske sikkerhetsinteresser og mulige virkemidler

I motsetning til GPS åpnes det i Galileoprosjektet for at Norge kan delta i både utforming og driften av systemet. Følgelig foreligger det både politiske og faglige muligheter for Norge selv om vi ikke er en del av EU. Nedenfor skisseres ulike utfordringer og virkemidler tilleggende navigasjonssystemer. Forslagene er ikke beskrevet i detalj, men bør være et grunnlag for videre diskusjon i Infrastrukturutvalget.

4.1 Internasjonal deltagelse som forutsetning for innsikt

Innsikt i utvikling og drift av Galileosystemet oppnås best gjennom aktiv og målrettet deltagelse i nedsatte komiteer og arbeidsgrupper samt faste staber innen EU og ESA. Med innsikt menes her eksempelvis førstehåndskunnskap om styrker og svakheter ved systemet, innsikt i krisehåndteringsprosesser, bedre forutsetning for norsk deltagelse i felles reaksjonsmønster mot uønskede hendelser. Deltagelse gir dessuten mulighet til å påvirke løsninger.

4.2 Tverrsektoriell tilnærming nasjonalt

Navigasjonssystemer vil levere tjenester til de fleste samfunnssektorene hvilket skaper behov for permanente sektorovergripende koordineringsordninger nasjonalt. Ideelt burde en slik tverrsektoriell koordinering ta utgangspunkt i en nasjonal strategi som beskriver navigasjonssystemenes betydning. Løsninger som sikrere sektorovergripende koordineringsordninger er vesentlig både i en normalsituasjon og under kriser hvor uteblivelse eller forringelse av navigasjonssignaler spiller en rolle.

4.3 Forskning og utvikling

Forskning rundt sårbarheter og muligheter i navigasjonssystemene vil gi oss et bedre grunnlag for å forebygge uønskede konsekvenser av forringede eller tapte navigasjonsdata. Basert på frembrakt kunnskap om dette vil både offentlige og private aktører ha et bedre beslutningsgrunnlag for å kunne både forebygge og håndtere kriser grunnet svikt ved navigasjonssystemer.

Forskningsinnsats bør også rettes mot hvordan navigasjonssystemer bidrar til å forme fremtidssamfunnet på ulike områder. Hvilke sikkerhetsmessige utfordringer forsterkes eller skapes i kjølvannet av økende avhengighet av navigasjonsdata bør belyses. Ikke minst bør det fokuseres på gjensidige avhengighetsforhold innen kritisk infrastruktur.

4.4 Nasjonal industri og kompetanse

Norske bedrifters leveranser av varer og tjenester vil innebære fordeler med hensyn til sikkerhetsutfordringer tilknyttet Galileo. Leveranser av varer og tjenester vil sikre kompetanse nasjonalt, hvilket kan bidra til å forstå og takle sikkerhetsutfordringer tilliggende avhengigheten av navigasjonssystemer. Det er derfor viktig at det legges til rette for at norske bedrifter kan konkurrere seg til kontrakter.

Teknologi utviklet med henblikk på navigasjonssystemer vil også kunne bli nyttiggjort i andre sammenhenger som kan bidra til styrket samfunnssikkerhet.

4.5 Sårbarhetsforståelse og krisehåndtering

Et annet virkemiddel norske myndigheter kan bruke er å pålegge private og offentlige virksomheter å planlegge for krisehåndtering og reserveløsninger dersom tjenester fra navigasjonssystemene uteblir eller er forringet. Risiko- og sårbarhetsvurderinger må her gjennomføres av aktuelle aktører for å identifisere sårbarheter og forebyggende sikkerhetstiltak.

Krisehåndtering vil også kunne skje på nasjonalt nivå dersom forstyrrelsene blir såpass omfattende at nasjonale sikkerhetsinteresser står på spill. I en slik situasjon vil det kunne oppstå behov for både sivile og militære virkemidler til å håndtere den oppståtte krisen. En ansvars- og rolleavklaring vil i så fall være nødvendig.

4.6 Forbud mot produksjon, salg og bruk av visse kategorier utstyr

I dag finnes det utstyr kommersielt tilgjengelig som kan avskjære eller forringe navigasjonssignalene. Gjennom juridiske virkemiddel bør det derfor vurderes forbud mot, eller restriksjoner for, produksjon, salg og bruk av visse kategorier utstyr som kan benyttes til å forringe eller avskjære navigasjonssignalene.

4.7 Merking og gjenfinning

Et ytterligere virkemiddel vil være å vurdere pålegg om å installere mottakere i visse kategorier gods eller objekter. Dette vil bedre sikkerheten ettersom et slik system vil gjøre det lettere å kunne forebygge spredning av materiell som kan nyttes eksempelvis i terroranslag. Dersom eksempelvis forflytinger av containere kan underkastes et slik system vil muligheten for å benytte containere til frakt av farlig materiell kunne avta.

4.8 Galileo PRS

Norge bør vurdere å slutte seg til PRS-delen av Galileo-systemet, ettersom dette vil kunne bidra til å redusere samfunnssårbarheten. Galileo PRS vil ha mer robuste signaler. I tillegg vil kryptering av navigasjonssignalene fra satellittene gi en bedre beskyttelse mot villedning. For samfunnsviktig infrastruktur vil Galileo PRS være viktig, ikke minst fordi sivile offentlige brukere ikke vil få tilgang til motstykket til Galileo PRS, GPS PPS og M-koden, i fremtiden. Deltagelse i PRS krever statlig kontrollmekanismer.

4.9 Galileo-infrastruktur i Norge

Dersom Norge skulle få tildelt Galileo bakkeinfrastruktur (Svalbard) vil det være viktig å fastsette hvilke lokale sikringstiltak som er nødvendig for å beskytte nettopp bakkeinfrastrukturen. Likeledes må mobilt utstyr som sensitive mottakerutstyr bli tilstrekkelig sikret.

4.10 Beskyttelse av informasjon

Av hensyn til egen nasjonal sikkerhet, og hensynet til alliertes sikkerhet er det avgjørende at Norge evner å beskytte sensitiv informasjon i henhold til gitte standarder. Beskyttelse av informasjon reguleres av nasjonale regelverk (særlig sikkerhetsloven), NATOs sikkerhetsregelverk, ESAs sikkerhetsregelverk, EUs sikkerhetsregelverk og de bilaterale sikkerhetsavtaler Norge har inngått med andre nasjoner og internasjonale organisasjoner.

4.11 Bruk av felles mottakere

For å utnytte at Galileo og GPS er kompatible og interoperable bør innføring av mottakere som kan ta i mot signaler for begge systemene anbefales.

5 Kilder

«Vulnerability Assessment of the Transportation Infrastructure Relying on The Global Positioning System» Prepared by John A. Volpe National Transportation Systems Center – For Office of the Assistant Secretary for Transportation Policy U.S. Department of Transportation (2001)

- «Study into impact on capability of UK Commercial and Domestic Services Resulting from loss of GPS Signals» QinetiQ (2001)
- «The *Instant Lessons* of the Iraq War» Main Report. Eight Working Draft: May 14, 2003. Anthony H Cordesman, Arleigh A Burke Chair for Strategy. Center for Strategic and International Studies (US).
- Kongelig resolusjon – Etablering av utvalg for sikring av landets kritiske infrastruktur, 29.10.2004
- Council Regulation (EC) No 1321/2004 of 12 July 2004 on the establishment of structures for the management of the European satellite radio-navigation programmes.
- Council Joint Action 2004/552/CFSP of 12 July 2004 on the aspects of the operation of the European satellite radio-navigation system affecting the security of the European Union.

– European Commission Directorate-General for Energy and Transport, GALILEO – The final countdown. December 2004.
– Sikkerhetspolitikk i verdensrommet - av Forsker Terje Wahl ved FFI.
– ESA/PB-NAV(2004)42 European Speace Agency – Programme Board on Satellite Navigation – Galileo IOV Ground Stations site selection. 23.11.2004.
– U.S. Space-Based positioning, Navigation and Timing Policy. December 15, 2004.
– St meld 14 (2004 – 2005) På den sikre siden – sjøsikret og oljevernberedskap
– The International Spectator, Volume XXXIX, no 2 April – June 2004. *Towards a Europaen Space Strategy?,* av Simonetta Cheli og Jean-Pierre Darnis.
– www.romsenter.no
– www.europa.eu.int
– www.esa.int

Vedlegg 12

Notat 2005-056
Kritisk infrastruktur og offentlig eierskap

Utarbeidet for Utvalget for sikring av landets kritiske infrastruktur
ECON Analyse, desember 2005

1 Innledning

De siste 10-15 år er det skjedd omfattende omorganisering av en rekke viktige infrastrukturindustrier i OECD-området. Endringene omfatter både eierskapet, der slike bedrifter er blitt hel- eller delprivatisert, og de regulatoriske rammebetingelsene og virkemidlene som brukes. Drivkreftene bak disse endringene har i stor grad vært knyttet til mål om å øke kostnadseffektiviteten i driften og utbyggingen av infrastrukturen, og dels vært mer ideologisk motivert. Et spørsmål som da har oppstått, er i hvilken grad og på hvilken måte denne type virksomheters betydning som kritisk infrastruktur for samfunnet er ivaretatt.

Kritisk infrastruktur kan defineres på flere måter, men en mulig definisjon er følgende:

> *«Kritisk infrastruktur defineres som de objekter, systemer og tjenester som er så viktige for samfunnet at deres manglende funksjonalitet eller ødeleggelse vil medføre svekkelse av rikets sikkerhet, alvorlig svekkelse av den nasjonale økonomi, alvorlig svekkelse av statens myndighetsutøvelse, betydelig tap av liv og helse, og/eller betydelig tap av den nasjonale trygghetsfølelse.»*

Utøvelsen av viktige samfunnsfunksjoner er i økende grad avhengig av leveranser av varer og tjenester fra aktører som opptrer i konkurranse i markedet. I den forbindelse er det interessant å drøfte følgende problemstillinger:

Hvilke drivkrefter har ligget bak omorganiseringen og endringer i eierskapet til ulike typer kritisk infrastruktur i Norge de siste 10-15 årene?

Hvilke incentiver har dagens aktører til å ivareta samfunnsinteresser med hensyn til kritisk infrastruktur?

Det faller utenfor rammen å gjøre en fullstendig samfunnsøkonomisk *evaluering* av dagens organisering av viktige infrastruktursektorer. Blant annet drøfter vi ikke hva som er det samfunnsøkonomisk *optimale* sikkerhetsnivået i lys av samfunnets betalingsvilje for sikkerhet og kostnadene ved realisering av ulike sikkerhetsnivåer. Målet er i stedet å beskrive de sentrale samfunnsøkonomiske drivkreftene bak endringene i organiseringen og eierskapet og identifisere hvilke betingelser som må være oppfylt for at samfunnets sikkerhetsinteresser skal ivaretas over tid.

I samfunnsøkonomisk forstand kan spørsmålet om samfunnets sikkerhetsinteresser med hensyn til kritisk infrastruktur ses langs to dimensjoner:

- *Drift* av den eksisterende infrastrukturen, herunder beredskap for håndtering av situasjoner hvor funksjonaliteten til infrastrukturen er truet.
- *Investeringer og videreutvikling* av infrastrukturen for å vedlikeholde dagens funksjonalitet og/eller møte endringer i samfunnets behov og teknologiutvikling.

For hel- eller delprivatiserte infrastrukturbedrifter, er spørsmålet om det er avvik mellom bedrifts- og samfunnsøkonomisk lønnsomhet i disse sammenhengene, og hvis det er tilfellet, om det er tatt i bruk velfungerende regulatoriske virkemidler som sikrer at viktige samfunnsøkonomiske hensyn likevel ivaretas. Konkurranseutsatte aktørers beslutninger påvirkes av bedriftsøkonomiske incentiver og pålegg fra myndighetene på forskjellige måter:

- De bedriftsøkonomiske incentivene avhenger av produktprisene som kan oppnås i markedet og kostnadene ved å frambringe de ulike produktene. De bedriftsøkonomiske incentivene kan imidlertid også avhenge direkte av offentlig virkemiddelbruk og reguleringer. For eksempel kan en leverandør av infrastrukturtjenester som har karakter av naturlig monopol (for eksempel et nettselskap i kraftsektoren) få sine inntekter bestemt gjennom fastsatte regler for hvilke priser eller inntekter leverandøren maksimalt kan kreve av kundene. Myndighetene kan også inngå avtaler med private aktører om leveranser av sikkerhets- og beredskapstjenester.

– Direkte virkemiddelbruk kan bestå i påbud eller forbud knyttet til sikkerhetsinteresser. Det kan for eksempel være kvalitetskrav, krav om opprettholdelse av beredskap eller sikkerhetsstandarder.

Eierskap gir *residual styringsrett* over beslutningene til bedriften. Med residual styringsrett menes retten til å fatte beslutninger om forhold som ikke er regulert gjennom lover og regler eller avtaler mellom bedriften på den ene siden og kunder, myndigheter, långivere og andre interessenter på den andre siden. For offentlig eide bedrifter som lever i konkurranse, har samfunnet altså mulighet til å påvirke bedriftens beslutninger direkte gjennom å bruke sin styringsrett som eier. Dersom det for slike bedrifter viser seg vanskelig å skape regulatoriske rammer som sikrer at de ivaretar samfunnsmessige mål, kan man i siste instans sikre disse hensynene ved å instruere bedriften.

For å belyse betydningen av de betydelige regulatoriske og eiermessige endringene som har skjedd de siste årene for ivaretakelsen av samfunnets hensyn til samme bedriftenes betydning som kritisk infrastruktur, skal vi kort beskrive de endringene som er skjedd innenfor tre sektorer:
– Kraftforsyning
– Telekommunikasjon
– Petroleum

Kraftforsyning og *telekommunikasjon* peker seg ut som analyseobjekter ved at de representerer to helt sentrale infrastrukturer i ethvert moderne samfunn. Det er en høy grad av gjensidig avhengighet mellom kraft og tele på den ene siden og så å si alle andre typer infrastruktur på den andre siden. I begge sektorer har det dessuten skjedd gjennomgripende endringer i eierskap, organisering og fordeling av ansvar for sikkerhet og infrastruktur de siste 10-15 årene. *Petroleumsvirksomheten* er interessant som følge av den omfattende omorganiseringen av sektoren med hensyn til eierskap og fordeling av ansvar for sikkerhet og infrastruktur i løpet av de siste 5 årene. Til sammen spenner de tre sektorene ut et interessant utfallsrom for de økonomiske drivkreftene bak forskjellige organisasjonsmodeller for kritisk infrastruktur.

2 Kraftforsyning

2.1 Kraftforsyning som kritisk infrastruktur

Elektrisitet er en uunnværlig innsatsfaktor i et moderne samfunn. Elektrisitet brukes blant annet som innsatsfaktor i en rekke produksjonsprosesser, til oppvarming, belysning og drift av elektriske apparater. De aller fleste husholdninger, bedrifter og offentlige aktører har svært høy betalingsvilje for å være tilknyttet elnettet. Tilsvarende er betalingsviljen for å unngå rasjonering, avbrudd og andre kvalitetsavvik (for eksempel spenningsvariasjoner) høy. Det henger sammen med at kostnadene ved avbrudd i forsyningen er svært store, selv ved kortere avbrudd. USA og flere vesteuropeiske land (Sverige, Danmark, Italia, Finland, Storbritannia) ble i 2003 rammet av omfattende avbrudd i sentralnettet, som synliggjorde de store samfunnsmessige konsekvensene ved avbrudd i forsyningen. Undersøkelser foretatt av SINTEF Energiforskning og SNF tyder på kostnadene ved avbrudd og redusert leveringskvalitet har økt de siste 10-15 årene (jf. Samdal et al., 2002).

Nordel, samarbeidsorganisasjonen for de nordiske systemansvarlige nettselskapene, har definert *leveringssikkerhet* som følger:[1]
– Med *energisikkerhet* menes kraftsystemets evne til, med en bestemt kvalitet, å levere ønsket mengde energi til forbrukerne.
– Med *effektsikkerhet* menes kraftsystemets evne til, med en bestemt kvalitet, å levere ønsket mengde effekt til forbrukerne.
– *Leveringssikkerhet* er en felles betegnelse for både energi- og effektsikkerhet.

I praksis innebærer opprettholdelse av leveringssikkerheten følgende på kort og lang sikt:
– Løpende balanse mellom forbruk og produksjon. Her er særlig systemansvarliges driftskoordinering viktig. Opprettholdelse av balansen stiller videre en rekke tekniske krav til utformingen av produksjonsanlegg, forbruksinstallasjoner og nettet samt tilgjengeligheten av anleggene i driftssituasjonen (herunder tilstrekkelig produksjonskapasitet i reserve for å ivareta spennings- og frekvensregulering, bortfall av annen kapasitet osv.).
– På lang sikt er investeringer i nett og produksjon en forutsetning for opprettholdelse av sikkerheten. Både reinvesteringer (utskifting av gamle anlegg) og nyinvesteringer er nødvendig.
– I tillegg er det nødvendig med en tilstrekkelig beredskap mot forskjellige typer ekstraordinære situasjoner, enten det skyldes naturforhold (for eksempel ekstremvær) eller tredjepartsaktivitet (for eksempel sabotasje eller hackerangrep).

[1] Se Nordels årsrapport for 2000.

Det norske vannkraftsystemet gir dessuten opphav til særlige utfordringer med hensyn til tørrårssikring og behovet for transport av energi fra produksjons- til forbruksområder.

2.2 Den norske kraftsektoren

Det norske bruttoforbruket av elektrisitet var i 2004 totalt 120 TWh, der alminnelig forsyning stod for 74,3 TWh. I 1990 var bruttoforbruket 105,7 TWh. Den årlige produksjonen er ca. 118 TWh i et år med normalt tilsig (basert på nedbørsdata for 1970-1999), hvorav vannkraft står for mer enn 99 prosent. De årlige tilsigsvariasjonene kan imidlertid være store, og den årlige produksjonen har variert mellom 104,4 TWh i 1996 og 142,7 TWh i 2000.

Overføringsnettet er delt i tre nivåer administrativt: Sentral-, regional- og distribusjonsnett. Offentlige eiere kontrollerer ca. 85 prosent av den samlede nettkapitalen.

- Statnett SF eier nærmere 90 prosent av sentralnettet, og leier inn de resterende anleggene (anlegg med spenningsnivå fra 132 kV og oppover samt utenlandskabler). Statnett er det systemansvarlige nettselskapet og har ansvar for å opprettholde den løpende balansen mellom produksjon og forbruk i kraftsystemet. Statnetts eierandel i sentralnettet har økt de siste årene.
- Det er ca. 80 netteiere i regionalnettet (anlegg med spenningsnivå fra 33-132 kV).
- Det er ca. 130 nettselskaper i distribusjonsnettet (spenning fra 22 kV og nedover). Disse har normalt områdekonsesjon innenfor et definert geografisk område.

Det finnes mer enn 100 uavhengige kraftprodusenter. Ca. 88 prosent av produksjonskapasiteten er i offentlig eie (stat, kommuner og fylkeskommuner). Da er statens andel i Norsk Hydro og kommunalt eierskap i Hafslund ikke inkludert. Av det resterende er ca. halvparten belagt med hjemfall til staten. Den offentlige eierandelen har økt noe etter innføringen av energiloven i 1991 som følge av at flere private verk er solgt til offentlige selskaper og ved at hovedvekten av investeringene i ny produksjon er gjort av offentlige aktører.

2.3 Samfunnsøkonomisk begrunnelse for valg av organisering og eierskap

2.3.1 Bakgrunnen for energiloven

Energilovutvalget i 1985 (jf. NOU 1985:9) identifiserte den fragmenterte strukturen som en hovedsvakhet ved den norske kraftsektoren. Det foreslåtte hovedvirkemidlet var å redusere antall enheter fra datidens ca. 320 til rundt 20 vertikalt integrerte verk. Dette virkemidlet skulle også bidra til prisutjevning.

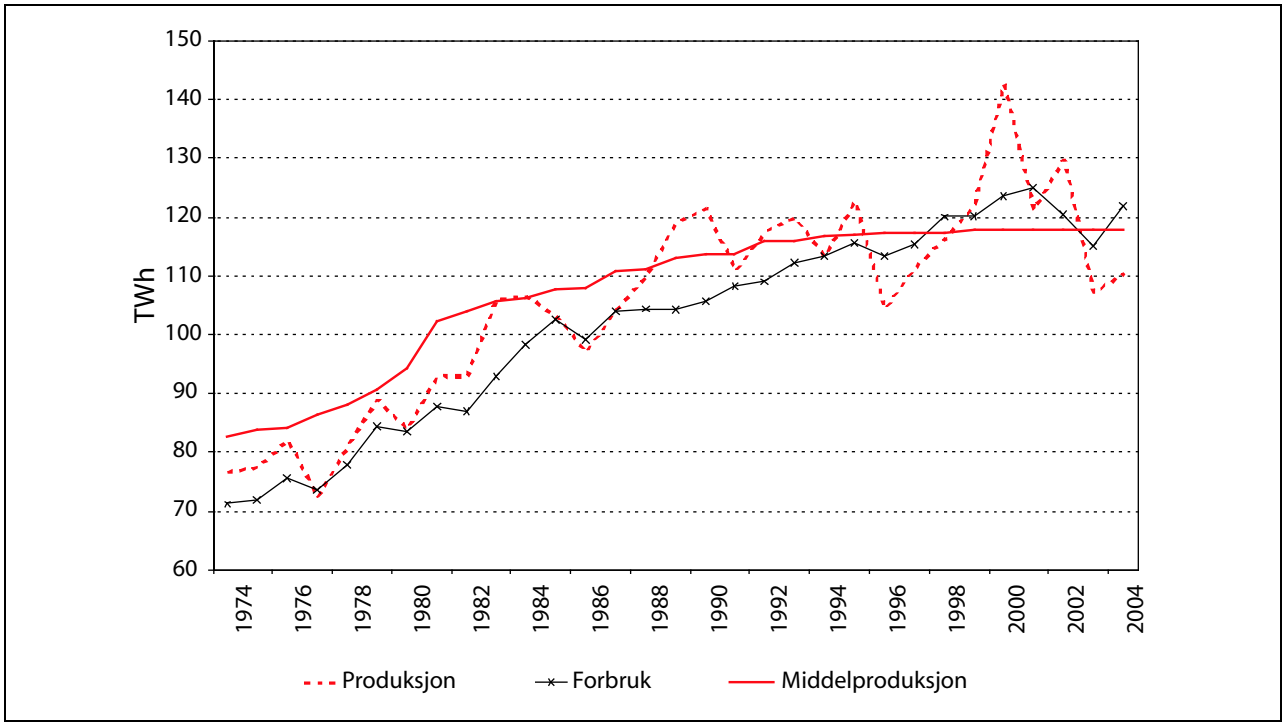
Den endelige energiloven av 1990 inneholdt ingen pålegg om strukturendringer, men baserte seg i stedet på en grunnleggende reform av systemet for omsetning av kraft. Hovedbegrunnelsen for energiloven var å utnytte de norske kraftressursene mer effektivt på kort og lang sikt. I økonomiske fagmiljøer og hos myndighetene var oppfatningen at for mye kapasitet var utbygd og til for høye kostnader. Videre stod ulike kundegrupper overfor forskjellige kraftpriser, noe som pr. definisjon leder til samfunnsøkonomisk ineffektiv ressursutnyttelse. Det var betydelige prisforskjeller både mellom regioner og mellom alminnelig forsyning og kraftintensiv industri.[2]

Det er viktige forskjeller i kostnadsstruktur mellom ulike deler av kraftforsyningen. I produksjon og omsetning av kraft til sluttbrukere er det mulig med konkurranse mellom uavhengige produsenter og leverandører. Kraftnettet er derimot et naturlig monopol.[3] Storbritannia og enkelte andre land hadde allerede gjennomført kraftmarkedsreformer med dette som utgangspunkt. Forskjellene i kostnadsstruktur gjør det både mulig og ønskelig ut fra et samfunnsøkonomisk perspektiv med separat organisering av nettet på den ene siden og produksjonen og omsetningen på den andre siden. Nettselskapene skal være nøytrale og legge til rette for et velfungerende marked med full tredjepartsadgang til nettet på ikke-diskriminerende vilkår.

I tillegg var og er teknologien for produksjon og overføring av kraft gitt på et overordnet plan i overskuelig framtid. Selv om vindkraft, gasskraft og andre teknologier for kraftproduksjon i økende grad er aktuelle, og selv om det stadig skjer nyvinninger innen overføringsteknologi (toveiskommunikasjon, nye typer kabler osv.), er systemet og teknologien prinsipielt den samme som siden det tidlige 1900-tallet. Størsteparten av elektrisiteten produseres i sentrale verk, mates inn i et overføringsnett og fordeles videre til sluttkundene i et radielt

[2] Prisforskjeller som skyldes ulike nettforhold er derimot samfunnsøkonomisk riktig. Standardreferansen om samfunnsøkonomisk optimale kraftpriser er Schweppe et al. (1988). Se også Bråten (2001) for en drøfting med utgangspunkt i norske forhold. Litteraturen om optimale priser i kraftsektoren har åpenbare analogier til transportkostnader i andre markeder.

[3] Et naturlig monopol er kjennetegnet ved at gjennomsnittskostnaden pr. overført enhet er fallende. Mer presist uttrykt er det vanlig å anta at kostnadsfunksjonen i kraftoverføring er subadditiv.



Figur 12.1 Den norske kraftbalansen 1974-2004

Kilde: NVE

distribusjonsnett. Videre innebærer kostnadsstrukturen i sektoren samt tilgangen på stedbunden vannkraft at det neppe er effektivt at alle forbrukere produserer sin egen elektrisitet lokalt. I stedet er det bygd ut et sentralt produksjonsapparat som er koblet sammen med forbruket via sentralnettet.

2.3.2 Valg av organisatorisk løsning og eierskap

De viktigste organisatoriske valgene ved innføringen av energiloven var følgende:

- Kraftselskapenes lokale oppdekningsplikt ble fjernet. Langsiktige kontrakter mellom produksjonsverk og distribusjonsverk ble opphevet for å legge til rette for konkurranse.
- Statkraft ble delt i en produksjonsdel, Statkraft SF, og en nettdel, Statnett SF, hvor sistnevnte fikk tildelt systemansvaret og eierskapet til statens anlegg i sentralnettet. Skillet mellom statens sentralnett/systemansvar og produksjon var nødvendig av hensyn til effektiv konkurranse i produksjon. For øvrig bestod de gamle selskaps- og eierstrukturene i stor grad de første årene.
- Det ble etablert en markedsplass, Statnett Marked, med utgangspunkt i den såkalte Samkjøringen. Statnett Marked er senere omdøpt til Nord Pool og utvidet til å omfatte Sverige (1996), Finland (1998) og Danmark (1999 og 2000).
- Nettselskapene ble gjort til gjenstand for regulering av tillatte inntekter fra NVE, i første omgang i form av avkastningsregulering (som gav nettselskapene kostnadsdekning inklusive avkastning på investert kapital). Siktemålet med reguleringen var i utgangspunktet primært å begrense nettselskapenes adgang til å ta monopolpriser av kundene.
- Behovet for løpende driftskoordinering ble ivaretatt gjennom Statnett, som ble slått sammen med Samkjøringen.
- Beredskapshensyn ble ivaretatt gjennom egne bestemmelser i energiloven og et sett av forskrifter og retningslinjer. Systemansvarlig (Statnett) ble sett på som særlig viktig i beredskapen sammen med Kraftforsyningens Beredskapsorganisasjon.

Et særtrekk ved den norske kraftreformen sammenlignet med for eksempel Storbritannia, var at det ikke skjedde noen privatisering samtidig med at markedsbasert kraftomsetning ble innført. I St.prp. nr. 100 (1990-1991) og Innst. S. nr. 28 (1991-1992) argumenterer Olje- og energidepartementet for at «kraftproduksjonsanlegg ( ) er verdier av nasjonal betydning som staten må ha et særlig ansvar for. Det er ikke ønskelig at staten gir fra seg

en direkte og nær kontroll med betydelige deler av disse ressursene.» Tilsvarende heter det at «det sentrale overføringsnett vil ha en funksjon som instrument i den statlige sektorpolitikk på energiområdet.» Det heter videre om Statnett at selskapet bør kunne oppnå en rimelig avkastning på investert kapital. Samtidig må kravene til den tekniske standarden og beredskapen i sentralnettet fastsettes «ut fra en vurdering av de samfunnsmessige kostnadene ved strømbrudd ved en gitt driftssikkerhet samt kostnader ved tap i overføringsnettet». Alt i alt legges det opp til en balanse mellom et variert offentlig virkemiddelsett og desentraliserte beslutninger på forretningsmessig basis både for Statkraft og Statnett, men den samfunnsøkonomiske målfunksjonen er klarere uttrykt for Statnetts vedkommende.

2.3.3 Utviklingen av virkemiddelapparatet

Siden 1991 er virkemiddelbruken overfor kraftsektoren utvidet og utviklet på flere måter, men hele tiden innenfor de markedsbaserte rammene i energiloven av 1990. Nedenfor beskriver vi noen av de mest relevante for leveringssikkerheten og beredskapen i sektoren.

Nettreguleringen

Avkastningsregulering er godt egnet til å sette tak på nettariffene, men stimulerer ikke til kostnadseffektivitet (jf. Laffont og Tirole, 1993). Kostnadsøkninger kan veltes direkte over på kundene. I 1997 gikk NVE derfor over til inntektsrammeregulering, som gjør det lønnsomt for nettselskapene å redusere kostnadene ved at de får beholde en andel av gevinsten i form av økt overskudd. Samtidig vil inntektsrammeregulering *isolert sett* gjøre det lønnsomt å redusere investeringene, noe som kan føre til for lav leveringskvalitet på sikt.

For å stimulere til reinvesteringer og ivareta kvalitetshensyn ble den såkalte KILE-ordningen (Kvalitetsjustering av inntektsrammer ved ikkelevert energi) innført fra 2001. Nettselskapene påføres en økonomisk straff ved avbrudd som varer mer enn 3 minutter. Avbrudd gir opphav til en inntektsreduksjon basert på mengden ikkelevert energi og avbruddssatser pr. kWh. Avbruddssatsene varierer fra 7 kr/kWh til 99 kr/kWh avhengig av kundetype og hvorvidt avbruddet er varslet eller ikke. Analyser av nettselskapenes tilpasning til KILE-ordningen tyder på at ordningen gir signaler som tas hensyn til i selskapenes beslutninger om investeringer og vedlikehold (jf. SINTEF, 2003 og ECgroup, 2004). Det er ikke gitt at ordningen gir tilstrekkelige incentiver til at leveringskvaliteten holdes på et akseptabelt nivå, men det kan også være at den virker for sterkt. KILE er primært et *langsiktig* virkemiddel for å stimulere til investeringer og vedlikehold, og kan ha gode samfunnsøkonomiske egenskaper med hensyn til leveringssikkerheten hvis ordningen er hensiktsmessig utformet. Det er videre verdt å merke seg at forskjeller i naturgitte rammevilkår kan tas hensyn til på forskjellige måter.[4]

Fra 2007 skal nettreguleringen revideres. I henhold til NVEs forslag skal ordningen med kvalitetsincentiver videreføres og utvides til å omfatte kortvarige avbrudd (se NVE, 2005b). I tillegg skal nettselskapene betale direkte kompensasjon til de berørte kundene ved avbrudd som varer mer enn 12 timer. Samtidig kan oppdateringsreglene for inntektsrammene og valg av parametre som referanserente bidra til lønnsomhet i forskjellige typer investeringer. I distribusjonsnettet har dessuten selskapene tilknytnings- og leveringsplikt, som også har konsekvenser for investeringene. I påvente av vedtak om endelig modell fra 2007 er det ikke mulig å trekke konklusjoner om investeringsincentivene i reguleringen.

Systemansvaret

Innholdet i systemansvaret er presisert og til dels utvidet gjennom et sett av forskrifter og Olje- og energidepartementets eierstrategi for Statnett:

- Systemansvarsforskriften, som ble innført i 2002, regulerer Statnetts rettigheter og plikter som systemansvarlig. I kjølvannet av den anstrengte forsyningssituasjonen høsten 2002 og vinteren 2003 har Statnett fått et særlig ansvar for å utvikle virkemidler til å håndtere svært anstrengte kraftsituasjoner.[5] Statnett har de siste årene blant annet søkt om konsesjon for gassturbiner som reservekapasitet i Møre og Romsdal.
- Statnett har etablert et eget marked for regulerkraftopsjoner (RKOM) for å ivareta behovet for effektreserver.
- Olje- og energidepartementet har presisert innholdet i eierstyringen av Statnett til at selskapet har et eksplisitt pålegg å gjennomføre

[4] I den gjeldende reguleringen spiller for eksempel hvert enkelt selskaps faktiske historiske kostnader en viktig rolle for inntektsrammene til selskapet. Det gir en innebygd kompensasjon for ugunstige rammevilkår ettersom kostnadene må antas å reflektere nettopp rammevilkårene.

[5] Det er ikke opplagt hvordan «svært anstrengte kraftsituasjoner» skal defineres. Statnett er i skrivende stund (desember 2005) i ferd med å utvikle en pakke av aktuelle virkemidler som skal godkjennes av NVE.

samfunnsøkonomisk lønnsomme nettinvesteringer, selv om de ikke skulle være bedriftsøkonomisk lønnsomme (se for eksempel St.prp. nr. 1 2001-2002). Dette er konkret eksempel på at en eier bruker den residuale styringsretten til å nå mål som desentraliserte beslutninger i bedriften kan gjøre det vanskelig å nå.

Det skjer også endringer i organiseringen av systemansvaret på nordisk plan. Den nordiske samarbeidsorganisasjonen Nordel er omdannet til et organ for de systemansvarlige nettselskapene i Norden, og har gjennomført en rekke tiltak for å bedre virkemåten til det felles nordiske markedet (forankret i en egen nordisk systemdriftsavtale). De nordiske energiministrene har gått inn for en økt integrasjon av systemansvaret (jf. Akureyrierklæringen).[6] For tiden pågår det utredningsarbeid i regi av så vel de systemansvarlige nettselskapene som Nordisk Ministerråd om hvordan systemansvaret i Norden kan samordnes ytterligere.

Beredskap

NVE, Statnett og Kraftforsyningens Beredskapsorganisasjon har sentrale roller i beredskapsøyemed. I de siste årene er energilovens bestemmelser om beredskap revidert, og det er innført en egen forskrift om beredskap med virkning fra 2003. Det er også innført en egen forskrift om kraftrasjonering.

Det regulatoriske rammeverket for beredskapen bygger videre på tidligere retningslinjer og anbefalinger fra BAS3-prosjektet om sårbarhetsreduserende tiltak i den norske kraftforsyningen. Prosjektet ble gjennomført av Forsvarets Forskningsinstitutt (FFI) i 1999-2001 på oppdrag fra flere norske myndigheter (se blant annet Fridheim et al., 2001). Konklusjonene i BAS3-prosjektet er at sårbarheten vil øke i framtiden som følge av økt IKT-avhengighet, personellknapphet, effektivisering og internasjonalisering. FFI anbefaler flere tiltak som spenner fra fysisk sikring til kompetanseutvikling og bedre rutiner for beredskapsarbeidet. Et fellestrekk ved tiltakene er at de alle kan la seg realisere innenfor et markedsbasert system, men det kan være nødvendig å sørge for finansiering via nettselskapenes inntektsrammer eller statsbudsjettet. På lang sikt anbefaler FFI at det gjøres investeringer i ny produksjons- og nettkapasitet samt beredskapstiltak.

Ved vedvarende energiknapphet som følge av tørrår eller andre forhold kan det være aktuelt med rasjonering dersom ikke økte markedspriser sørger for en tilstrekkelig reduksjon i forbruket (effektknapphet håndteres av systemansvarlig i henhold til systemansvarsforskriften). Rasjonering innføres altså først når markedsmekanismene ikke lenger fungerer etter hensikten, og kan i praksis skje gjennom frivillig sparing, kvoterasjonering eller sonevise utkoblinger. Rasjoneringsmyndigheten, som utpekes av Olje- og energidepartementet i henhold til energiloven, besitter en rekke virkemidler gjennom *Forskrift om planlegging og gjennomføring av rekvisisjon av kraft og tvangsmessige leveringsinnskrenkninger ved kraftrasjonering*. Rasjoneringsforskriften kommer til anvendelse på alle som «helt eller delvis eier eller driver nett eller produksjon, den som driver organisert markedsplass ( ) samt omsettere og sluttbrukere» (forskriftens § 2), det vil i praksis si samtlige aktører i kraftmarkedet.

Regelverket pålegger blant annet rasjoneringsmyndigheten å sørge for at det til enhver tid foreligger planer for hvordan rasjonering skal gjennomføres. Videre finnes det bestemmelser om prioritering av forbrukere i rasjoneringssituasjoner og rekvisisjon av kraft. I kjølvannet av vinteren 2002/2003 ble det gjennomført en rekke forberedende tiltak i form av planlegging, informasjon og møter mellom NVE, andre myndigheter med ansvar for sikkerhet og beredskap, interesse- og forbrukerorganisasjoner, systemansvarlig og markedsaktører. Kraftforsyningens beredskapsorganisasjon ble også inkludert i arbeidet.

Produksjon og forbruk

Virkemiddelapparatet overfor kraftproduksjonen er rettet inn mot en rekke mål, herunder miljøhensyn, ressursforvaltning og inndragning av grunnrente gjennom skattesystemet.

Når det gjelder rammebetingelser for investeringer, har det vært gjort mest overfor nye fornybare energikilder som vindkraft. Det planlagte norsk-svenske elsertifikatmarkedet vil imidlertid kunne gi betraktelig økt lønnsomhet i både vindkraft og vannkraft, særlig småskala vannkraft. Utbyggere av nye fornybare energikilder vil med et slikt marked bli tildelt elsertifikater som sluttbrukerne er pliktige til å kjøpe, og sertifikatprisen vil på den måten gi et visst beløp i støtte til utbyggerne. Det gjenstår også å se om høyere forventede kraftpriser som følge av handel med CO2-kvoter og en generelt strammere kraftbalanse i Norden og Nord-Europa vil gi høyere produksjonsinvesteringer i de kommende årene.

[6] Se pressemelding fra Nordisk Ministerråd 2. september 2004.

På forbrukssiden er det gitt støtte til omlegging av energiforbruket og installering av alternative oppvarmingsløsninger. Forbruksavgiften på elektrisitet er også økt betraktelig siden 1990 - avgiften har primært en fiskal begrunnelse (jf. NOU 1996:9), men vil også påvirke etterspørselen av elektrisitet i forhold til alternative oppvarmingsløsninger.

2.4 Oppnåelse av sikkerhetsmål

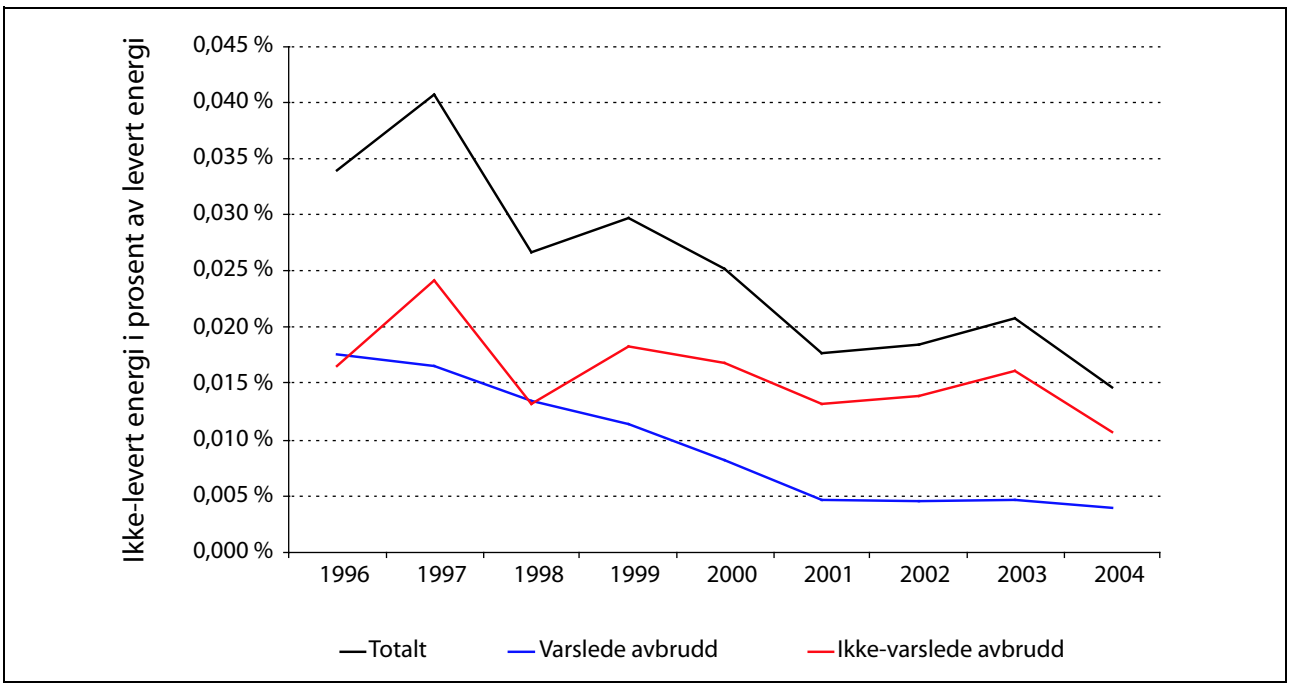
2.4.1 Erfaringer

Leveringssikkerhet i praksis

Statistikk fra NVE viser at ikke-levert energi til norske nettkunder har gått betraktelig ned siden registreringen av avbruddsdata ble innført i 1995. Nedgangen skyldes i hovedsak at antall varslede avbrudd er redusert betraktelig. Også ikke-varslede avbrudd har imidlertid vist en nedadgående trend, selv om de årlige variasjonene kan være store. Det finnes foreløpig bare data for andre typer kvalitetsavvik som kortvarige avbrudd og spenningsvariasjoner på sentralnettsnivå. Fra 2005 er imidlertid alle nettselskaper pliktige til utvidet rapportering av kvalitetsforhold gjennom innføringen av en egen forskrift om leveringskvalitet.

Antall utfall i sentralnettet med store konsekvenser har vært begrenset, og normal forsyning er blitt gjenopprettet i løpet av kort tid. Den største enkelthendelsen var et utfall på Vestlandet i februar 2004, hvor en tilnærmet normal situasjon var gjenopprettet i løpet av ca. 1 time. Det synes klart at det norske nettet er mindre sårbart enn for eksempel det svenske overfor utfall av denne typen (jf. blant annet DSB, 2003). Det desentrale norske vannkraftsystemet, med om lag 600 produksjonsenheter med en installert effekt over 1 MW og høy reguleringsevne, bidrar også til sikkerheten (men systemet er til gjengjeld sårbart for tørrår). Norske distribusjonsnett har også vært vesentlig mindre utsatt for store utfall enn i Sverige.

Direktoratet for samfunnssikkerhet og beredskap konkluderer i en rapport fra 2003 at den norske beredskapen for håndtering av konsekvensene av omfattende avbrudd er styrket de siste årene, men at det er ønskelig med ytterligere tiltak. DSB er blant annet opptatt av risikoen for at dereguleringen av kraftsektoren får konsekvenser for vedlikehold, investeringer og kompetanse i selskapene. SINTEF Energiforskning konkluderer i en sårbarhetsstudie for Nordisk Ministerråd med at sårbarheten med hensyn til energiknapphet er «middels» (medium risk state), mens risikoen er lav for effektknapphet. Når det gjelder omfattende blackouts, er risikoen på et middels nivå, men situasjonen vurderes å være den samme som før dereguleringen av de nordiske kraftmarkedene. Det er likevel en viss usikkerhet med hensyn til endrede vedlikeholdsrutiner og tilgang på kvalifisert teknisk personell (se Doorman et al., 2004).



Figur 12.2 Ikke-levert energi i prosent av levert energi. 1995-2004

Kilde: NVE

Investeringer

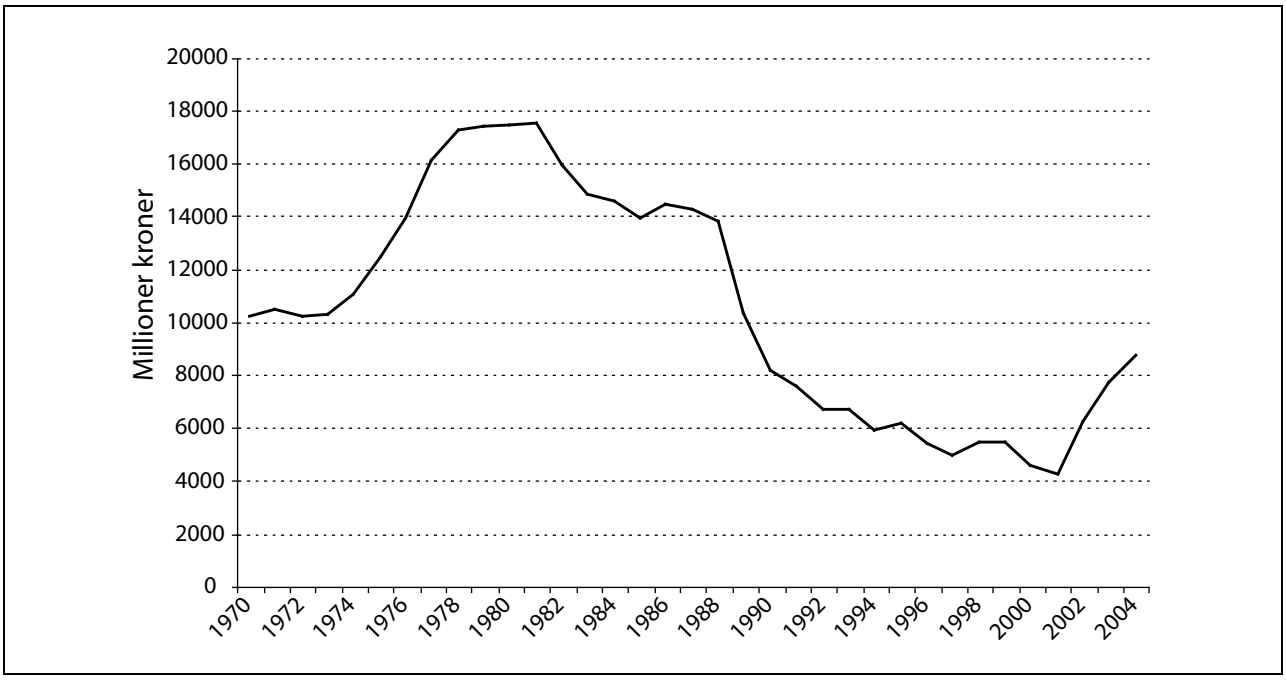
Investeringene i det norske kraftsystemet har falt sterkt siden midten av 1980-tallet, og har de siste årene vært på en fjerdedel av toppnivået rundt 1970 (målt i faste priser). Fra 2003 har investeringene økt betraktelig. Det er for tidlig å si om dette representerer et trendbrudd, men tall fra Statistisk sentralbyrås investeringsstatistikk for industri, bergverksdrift og kraftforsyning tyder på at investeringsnivået vil holde seg høyt og til og med øke i 2005-2006. Det er imidlertid klart at en rekke prosjekter er under utbygging eller kan bli bygd ut:

- Statnett har varslet at de vil investere for ca. 4 milliarder kroner fram mot 2010. Det omfatter både reinvesteringer og nyinvesteringer i sentralnettet. I tillegg kommer ca. 3,5 milliarder i investeringer i nye utenlandsforbindelser, inklusive NorNed-kabelen til Nederland.
- I produksjonssystemet har tilgangen vært beskjeden på 1990-tallet. Ifølge tall fra NVE er imidlertid nærmere 2 TWh ny vannkraft under utbygging (eller endelig investeringsbeslutning er fattet), og flere vindkraftverk er gitt konsesjon. Naturkraft har fattet beslutning om bygging av et 430 MW gasskraftverk på Kårstø, og flere andre gasskraftprosjekter både med og uten CO2-håndtering er under utvikling.

Det er uansett ikke grunnlag for å hevde at investeringene har vært for lave samfunnsøkonomisk sett:

- Investeringene i det norske kraftsystemet var betydelige i årene fram mot midten av 1980-tallet. Kapasiteten i produksjonsapparatet og nettet var rikelig ved inngangen til 1990-tallet, og anleggene var relativt nye. I tillegg har de nordiske kraftreformene lagt til rette for en mer effektiv handel på tvers av landegrensene, slik at norske og svenske tørrårsutfordringer i større grad kan løses ved import i stedet for store innenlandske investeringer i flerårsmagasiner og termisk kraftproduksjon.[7]
- NVE har i samarbeid med SINTEF Energiforskning nylig utarbeidet en rapport om alderen på norske nettanlegg. NVE konkluderer med at det er behov for en vesentlig økning i reinvesteringene på sikt, men at dagens nivå på reinvesteringene faktisk er i overkant av det estimerte behovet for perioden 2004-2008 (se NVE, 2005a).
- Det er heller ikke samfunnsøkonomisk ønskelig å unngå samtlige avbrudd eller kvalitetsavvik. For kunder med særlige krav til leveringskvalitet kan det ofte være billigere å installere lokale reserveløsninger.

[7] Utviklingen av det nordiske markedet er primært begrunnet i handelsgevinstene som oppstår ved at en kan utnytte de ulike nordiske kraftressursene mer effektivt samlet sett. Det nordiske markedet kan vanskelig løse ekstreme tørrårsutfordringer. For eksempel har det norske sentralnettet bare kapasitet til å importere maksimalt 15-20 TWh i løpet av et år ifølge informasjon fra Statnett.



Figur 12.3 Investeringer i den norske kraftsektoren. Milliarder 2005-kroner

Kilde: Statistisk sentralbyrå (nasjonalregnskapet)

2.4.2 *Økonomiske incentiver til å ivareta beredskap og sikkerhet og rollen til andre virkemidler*

Det avgjørende spørsmålet om dagens organisering av kraftsystemet vil gi de riktige investeringene og ivareta sikkerhetshensyn på lang sikt. Her er det viktige forskjeller mellom nett og produksjon.

Produksjon

Det er omdiskutert i hvilken grad liberaliserte kraftmarkeder gir tilstrekkelig med investeringer i produksjon. Det kan være behov for å tilpasse selve markedsdesignet for å gi tilstrekkelige investeringsincentiver for private aktører (eller offentlige med bedriftsøkonomiske mål). I det britiske markedet har en blant annet hatt en ordning med et påslag (uplift) i forhold til prisen som klarerer markedet (skaper likhet mellom tilbud og etterspørsel) i den enkelte driftstimen. Også i andre markeder (blant annet Chile) er administrative ordninger tatt i bruk for å stimulere til investeringer utover hva prissignalene i markedet gir opphav til.

Gitt at rammebetingelsene er riktig utformet, vil den samfunnsøkonomiske verdien av ny produksjonskapasitet reflekteres i de forventede framtidige kraftprisene. Det er imidlertid ikke gitt at det kravet er oppfylt. Den samfunnsøkonomiske verdien av å unngå langvarige avbrudd kan være høyere enn det som er reflektert i markedsprisene på kraft. Støm brukerens betalingsvilje for leveranser er med, men *ringvirkninger* ved at sluttbruken ikke lenger kan produsere sine tjenester fanges ikke opp. Når produksjon stopper opp, oppstår det et tap som er større enn produsentenes tap. KILE-kostnadene er dessuten beregnet for utfall med en begrenset varighet. Dersom utfallet varer lengre, vil det påløpe ytterligere kostnader som også må inkluderes (jf. ECON, 2005, Statnett, 2005 og Fridheim et al., 2001).

I den grad markedet ikke er velfungerende og/eller rammebetingelsene er gale, *kan* offentlig eierskap tenkes å være et virkemiddel for å sørge for at tilstrekkelig produksjonskapasitet bygges ut. Endringer i markedsdesign, rammebetingelser og skatteregler kan imidlertid være vel så egnede virkemidler. Beredskapshensyn kan i prinsippet ivaretas gjennom forskjellige typer offentlige pålegg, jf. beredskapsforskriften. Slike pålegg medfører kostnader, som kan dekkes via statsbudsjettet eller andre finansieringsordninger i den grad tiltakene ikke er bedriftsøkonomisk lønnsomme. Her er det heller ingen prinsipielle forskjeller mellom private og offentlige aktører med bedriftsøkonomiske målfunksjoner.

I Norge har for øvrig Statnett fått et særlig ansvar for å finne virkemidler og instrumenter som kan ivareta leveringssikkerheten i svært anstrengte kraftsituasjoner, for eksempel i forbindelse med tørrår.

Nett

I nettet er det mye som tyder på at visse typer investeringer vil være vanskelige å gjennomføre på bedriftsøkonomisk grunnlag. Det gjelder særlig i sentralnettet og i noen grad også regionalnettet, hvor investeringer kan ha en rekke nyttevirkninger som er vanskelige å måle og dermed prissette i et marked eller gjennom et nettreguleringsregime (jf. Joskow og Tirole, 2005, og Bråten, 2001). Det skyldes ikke minst at bidraget til leveringssikkerheten fra en investering kan være svært vanskelig å beregne og verdsette. Ulike prosjekter i nett, produksjon og forbruk kan dessuten være gjensidig avhengige. Skjev fordeling av informasjon mellom aktører og asymmetri i incentiver mellom nettselskaper, andre infrastrukturselskaper og konkurranseutsatte aktører skaper dessuten rom for strategisk atferd, som kan resultere i så vel over- som underinvesteringer. Mange av de samme problemstillingene er relevante også på lavere nettnivåer, ikke minst når utbygging av lokal kraftproduksjon får et visst omfang.

I fravær av perfekte økonomiske og juridiske reguleringsmekanismer for samfunnsøkonomisk riktige nettinvesteringer er eierskapet til Statnett SF sannsynligvis et egnet virkemiddel for å ivareta sikkerhetshensyn i kraftsystemet på lang sikt. De viktigste funksjonene i Statnett i det henseende er selve systemansvaret (den løpende systemdriften) og muligheten til både å fatte beslutninger om hvilke investeringer som skal gjøres og finansiere investeringene selv. Det betyr likevel ikke at private (eller for den saks skyld kommunale) investeringer i overføringskapasitet i sentralnettet bør utelukkes, men Statnett bør ha et helhetsansvar. I distribusjonsnettet er det grunn til å anta at argumentet for offentlig eierskap er svakere, men det er behov for supplerende virkemidler i form av kvalitetskrav, leverings- og tilknytningskrav osv. Eventuelt kan staten definere beredskapsbehov og sørge for tilstrekkelig finansiering via inntektsrammene eller statlige overføringer (i noen grad skjer dette allerede i dag gjennom beredskapsforskriften og inntektsrammereguleringen).

Videre er det heller ingen entydig empirisk sammenheng mellom offentlig eierskap og sys-

temsikkerhet. I Sverige har store avbrudd i distribusjonsnettet rammet så vel offentlige selskaper (Vattenfall) som ikke-offentlige. Sverige er også blitt rammet av store avbrudd i sentralnettet, som eies og drives av Svenska Kraftnät. Svenska Kraftnät er organisert som et affärsverk under Miljö- och samhällsbyggnadsdepartementet.[8]

2.5 Oppsummering

Den samfunnsøkonomiske hovedbegrunnelsen for energiloven av 1990 var å utnytte de norske kraftressursene mer effektivt både på kort og lang sikt. Hovedgrepet bestod i å innføre markedsbasert kraftomsetning med utgangspunkt i et skille mellom produksjon og salg som konkurranseutsatt virksomhet og nettet som et naturlig monopol. Dette innebar blant annet at Statnett ble skilt ut fra Statkraft, men det statlige eierskapet ble beholdt i begge de nye selskapene. Eierskapet i den norske kraftsektoren er i all hovedsak offentlig også etter 14 år med markedsbasert kraftomsetning, både i produksjon og nett.

I kjølvannet av energiloven er det utviklet et omfattende og sammensatt virkemiddelapparat for å ivareta sikkerhetshensyn. Virkemidlene er dels økonomiske, for eksempel ved å inkludere kundenes kostnader ved avbrudd som en del av reguleringen av nettselskapene. Dels består virkemidlene i forskrifter, påbud og retningslinjer som fordeler ansvar og plikter for beredskap og sikkerhet mellom myndigheter og selskaper.

Kraftprodusenter har i utgangspunktet incentiver til å ha en god beredskap overfor uforutsette hendelser for å unngå inntektstap ved bortfall av produksjon. Vedvarende knapphet på produksjonskapasitet vil resultere i høyere markedspriser, som i sin tur vil utløse investeringer i ny kapasitet. Det er imidlertid usikkert om samfunnets verdsetting av reservekapasitet for å unngå langvarige avbrudd reflekteres godt nok i markedsprisene.

I *nettet* er nytten av investeringer ofte vanskelig å måle, og kompleksiteten i investeringene kan gjøre det vanskelig å fordele kostnadene på en hensiktsmesig måte. Det medfører i sin tur at økonomiske og juridiske reguleringsmekanismer ikke alene vil gi de riktige investeringsincentivene, særlig i sentralnettet.

Statlig eierskap til Statnett kombinert med en eksplisitt *samfunnsøkonomisk* målfunksjon for selskapets investeringspolitikk kan være et egnet virkemiddel til å ivareta leveringssikkerheten i sentralnettet. De viktige funksjonene i Statnett er i denne sammenhengen selve systemansvaret og muligheten til å fatte investeringsbeslutninger. I andre deler av kraftsystemet finnes det en rekke andre virkemidler enn eierskap som kan styrke beredskapen og investeringsincentivene innenfor et markedsbasert kraftsystem (forskrifter, skattesystem, finansiering av beredskapstjenester gjennom offentlige tilskudd osv.).

3 Elektronisk kommunikasjon

3.1 Elektronisk kommunikasjon som kritisk infrastruktur

Begrepet *elektronisk kommunikasjon* dekker tele, IT og media. Utviklingen i kommunikasjonsteknologi og etterspørselen etter digitale tjenester har ført til en økende sammensmelting eller *konvergens* mellom forskjellige infrastrukturer for overføring av tele- og datasignaler. Det er derfor hensiktsmessig å se på alle former for elektronisk kommunikasjon og ikke bare tradisjonell telefoni.

Elektroniske kommunikasjonsteknologier er på samme måte som elektrisitet uunnværlige i et moderne samfunn. Elektronisk kommunikasjon legger til rette for ulike transaksjoner mellom næringsliv og kunder og mellom offentlig sektor og innbyggerne. Dessuten er elektronisk kommunikasjon svært viktig for at andre kritiske infrastrukturer skal kunne fungere tilfredsstillende. Betalingsformidling, trafikkavvikling i samferdselssektoren, utøvelsen av forskjellige offentlige funksjoner og driften av kraftforsyningen er bare noen eksempler.

Tradisjonelt har fasttelefoni vært den sentrale infrastrukturen for det som i dag betegnes som elektronisk kommunikasjon. I St.meld. nr. 47 (2000-2001) defineres *telesikkerhet* ved at teleinfrastrukturen oppfyller følgende krav:

- *Tilgjengelighet* - at systemet er sikret mot avbrudd i sin forventede funksjon og at systemet har tilgang til nødvendig datainnhold
- *Integritet* - at systemet er sikret mot manipulering med systemets funksjon og datainnhold
- *Konfidensialitet* - at systemets funksjon og datainnhold er sikret mot innsyn

[8] Modellen med statlig heleierskap til det systemansvarlige nettselskapet er for øvrig langt fra enerådende internasjonalt. I Finland er Fingrid eid med 12 prosent av den finske staten, 25 prosent av det delprivatiserte energiselskapet Fortum, 25 prosent av kraftprodusenten PVO, som er dominert av private finske industribedrifter og 38 prosent av private institusjonelle investorer. Det britiske National Grid er privatisert og børsnotert. I Tyskland er systemansvaret delt mellom fire selskaper, hvorav to er børsnotert (E.ON og RWE) og to har dominerende utenlandsk eierskap (Vattenfall Europe og Energie Baden-Württemberg).

Videre defineres *teleberedskap* som «planer og faktiske gjennomførte tiltak som er gode nok til å kunne møte de forhold som innebærer ekstraordinær risiko», for eksempel i forbindelse med sikkerhetspolitiske kriser eller krig. Tilsvarende definisjoner kan gjøres gjeldende for andre kommunikasjonsteknologier som fyller de samme behovene hos brukerne som tradisjonell telefoni.

Ivaretakelse av sikkerheten stiller krav til den kortsiktige driften og koordineringen av de ulike teleinfrastrukturene, men også investeringene. Det gjelder både med hensyn til innføring av nye teknologier for elektronisk kommunikasjon og utvikling av robuste nettstrukturer som er mindre sårbare for hendelser som kan ramme enkeltanlegg (redundans).

3.2 Den norske ekomsektoren

Nett for elektronisk kommunikasjon består generelt av aksessnett ut til den enkelte bruker og transportnett som kobler sammen større geografiske områder (jf. St.meld. nr. 47, 2000-2001). I tillegg kommer tjenestenett for formidling av informasjon i nettverk med tjenestenoder tilknyttet transportnettet, drifts- og støttesystemer og brukerutstyr (for eksempel telefoner og datamaskiner).

Det finnes etter hvert en rekke forskjellige typer nettverk for elektronisk kommunikasjon. Den norske ekomsektoren deles gjerne inn i følgende hovedsegmenter (jf. Post- og teletilsynet, 2005):

- *Fasttelefoni.* Telenor er den dominerende aktøren både som eier av infrastruktur og tjenesteleverandør. BaneTele eier og disponerer også et landsdekkende nett for fasttelefoni, blant annet bestående av linjer som leies inn fra Jernbaneverket og et antall kraftselskaper. I tillegg finnes det et femtitalls tjenesteleverandører uten egne nett.
- *Mobiltelefoni.* Telenor og NetCom er de to dominerende aktørene med egne landsdekkende GSM-nett, mens Teletopia også har et eget nett enkelte steder. Både Telenor og NetCom har dessuten bygd ut UMTS-nett. Innen mobiltelefoni finnes det et 20-talls tjenesteleverandører som leier kapasitet.
- *Bredbånd.* Innen bredbånd finnes det etter hvert et betydelig antall aktører med egne lokale aksessnett, både tradisjonelle teleselskaper og nye aktører som kraftselskaper og kabel-tv-selskaper.
- *Leide linjer (overføringskapasitet).* Leide linjer eller overføringskapasitet brukes til sammenkobling av lokale nett, dataoverføring, overføring av kringkastingssignaler med mer. Telenor dekker hele landet med transport- og aksessnett, men det finnes også andre aktører med mer begrenset utbygd kapasitet. BaneTele, Song Networks og enkelte kraftselskaper er blant de viktigste konkurrentene til Telenor (se igjen Post- og teletilsynet, 2005).

I tillegg til de kommersielle tilbyderne av elektronisk kommunikasjon finnes det også egne nødnett beregnet på spesielle brukere, som Forsvarets Digitale Nett (FDN). Det er også vedtatt at det skal bygges et nytt digitalt nødnett for politi, brannvesen og helsevesen. Både eksisterende og planlagte nødnett skal være landsdekkende. Også Jernbaneverket er i ferd med å bygge ut et eget nett for mobilkommunikasjon beregnet på det norske tognettet (GSM-R). Telenor spiller likevel fortsatt en sentral rolle ved at betydelige deler av trafikken også i andre nett, også nødnettene, går via deler av Telenors nett..

Ifølge Statistisk sentralbyrå hadde ca. 60 prosent av norske husholdninger internett-tilgang i 2004, ca. halvparten av disse igjen via bredbånd. Andelen som potensielt har tilgang, er vesentlig høyere. 95 prosent av husholdningene hadde mobiltelefon, mens 30 prosent var tilknyttet kabel-tv. Post- og teletilsynets oversikt over det norske telemarkedet første halvår 2005 viser at andelen husstander med bredbåndstilknytning har økt til 37 prosent. Mer enn 100 000 husstander har tatt i bruk bredbåndstelefoni. Antall fasttelefoniabonnement er redusert med nærmere 10 prosent siden 2001, og 17 prosent av norske husstander er i dag uten fasttelefon (se Post- og teletilsynet, 2005). I samme periode har antall mobiltelefoniabonnementer (inklusive kontantkort) økt med vel 35 prosent. Totalt er det i dag ca. dobbelt så mange mobilabonnementer som fasttelefoni. Trafikken fra fasttelefoninettet målt i minutter er redusert med ca. 20 prosent siden 2001, mens trafikk fra mobilnett er om lag doblet siden 1999.

3.3 Samfunnsøkonomisk begrunnelse for organisering og eierskap

3.3.1 Bakgrunnen for omorganiseringen av telesektoren

Den norske telesektoren var inntil slutten av 1980-tallet dominert av det statlige Televerket, som hadde monopol på en rekke former for telekommunikasjon (se Hagen, 2003, og Hagen og Nafstad, 2003, for historiske og komparative framstillinger

av utviklingen i telepolitikken og -reguleringen i Norge og andre land).

Fra et samfunnsøkonomisk perspektiv ble telesektoren lenge ansett som et naturlig monopol på linje med for eksempel elnettet. De faste kostnadene ved etablering av teleinfrastrukturen var høye, mens de variable kostnadene ved den løpende utnyttelsen av telenettet var små. Gjennomsnittskostnaden pr. trafikkenhet var fallende.[9] Standardmodellen i den vestlige verden var å organisere telesektoren i vertikalt integrerte monopoler. Som oftest var monopolene offentlig eid, men med USA som et viktig unntak, hvor det regulerte private monopolet AT&T var dominerende. Offentlig eierskap var ofte en erstatning for monopolregulering, og gjorde det også mulig å bruke teleselskapene til å forfølge andre politiske mål enn samfunnsøkonomisk effektiv ressursutnyttelse i sektoren.

Utviklingen av nye teknologier for overføring av tele- og datasignaler - fiberoptikk, digital teknologi, mobiltelefoni, overføring via elnettet - har imidlertid endret kostnadsstrukturen og de samfunnsøkonomiske karakteristikaene i telesektoren radikalt. Det naturlige telemonopolet har gradvis skrumpet inn, og i dag er det i praksis mulig med konkurranse i så å si alle ledd av kommunikasjonsinfrastrukturene. Virkningene av konkurransen kan blant annet observeres ved at en økende andel av norske telefonikunder, både husholdninger og bedrifter, ikke lenger har fasttelefoniabonnement.[10]

I takt med teknologiutviklingen har også den samfunnsøkonomiske tenkningen omkring organiseringen av telesektoren endret seg. De siste 20 årene har det skjedd omfattende endringer i eierskapet og reguleringen av telemonopolene. I Storbritannia er British Telecom privatisert og underlagt prisregulering, mens AT&T ble splittet opp i USA. Fra ca. 1990 har EU spilt en nøkkelrolle som pådriver i Europa, som får konsekvenser også for Norge gjennom EØS-avtalen. Utviklingen av nye markeder og organisasjonsformer har også reist spørsmål om mulige konflikter mellom tradisjonelle statlige roller i telesektoren (for eksempel rollen som eier til kommersielle bedrifter kontra rollen som regulator for egne og andre bedrifter).

3.3.2 Valg av organisatorisk løsning og eierskap

Som nevnt ovenfor var den norske telesektoren dominert av det statlige Televerket inntil slutten av 1980-tallet. Andre markeder for elektronisk kommunikasjon var i liten grad utviklet. Den norske telesektoren er imidlertid blitt gradvis omorganisert. I 1988 ble Televerkets monopol på terminalutstyr opphevet. En annen viktig milepæl var innføringen av konkurranse innen mobiltelefoni i 1991, da NetCom fikk konsesjon til å levere mobiltelefonitjenester. I 1995 ble Televerket omdannet til et statlig aksjeselskap, Telenor, og i 1998 ble Telenors monopol på fasttelefoni opphevet.

I likhet med markedsreformen i kraftsektoren ble det ikke lagt opp til noen privatisering av Telenor i første omgang. Innslaget av privat eierskap i telesektoren og mer generelt markedene for elektronisk kommunikasjon økte i stedet ved at nye aktører (som NetCom i mobilmarkedet) etablerte seg. Også andre kommunale kraftselskaper og Statnett etablerte egne teleselskaper. Et særtrekk ved de offentlige teleselskapene med utspring i kraftsektoren, som Enitel og selskapene under ElTele-paraplyen, var at de eide egne fysiske infrastrukturer for telekommunikasjon. Mye av televirksomheten og -infrastrukturen i kraftselskapene er senere solgt eller leid ut til aktører som BaneTele.[11] I motsetning til i kraftsektoren ble det imidlertid ikke foretatt noen vertikal oppsplitting av Telenor i monopolvirksomhet og konkurranseutsatt virksomhet. Dette var i tråd med den dominerende modellen internasjonalt.

BaneTele disponerer et landsdekkende tele- og bredbåndsnett, både transport- og aksessnett. I privatmarkedet leverer BaneTele infrastruktur til tjenesteleverandører, men har ingen kunder selv. I bedriftsmarkedet leier selskapet ut kapasitet til operatører, bredbåndsaktører og i noen grad direkte til store bedrifter og offentlige etater. Den norske staten eier 100 prosent av aksjene i BaneTele.

Mot slutten av 1990-tallet oppstod en debatt om eierskapet i Telenor, og det ble fremmet forslag om å fusjonere Telenor med det helstatlige svenske Telia (se blant annet St.prp. nr 58, 1998-99). Fusjonsforslaget var begrunnet i behovet «for å kunne møte og utnytte de raske og omfattende strukturelle endringer som skjer på telemarkedet.» Videre var det viktig for norske myndigheter å opprettholde et sterkt teleselskap med nasjonal forankring for å sikre landsdekkende tilbud av moderne og avanserte tele- og IT-tjenester til lave priser. Dette kunne i henhold til myndighetene best sikres gjennom etableringen av et felles norsk-svensk telekonsern. Formålet var både å utnytte kostnadssynergier og styrke evnen til inno-

[9] Jf. definisjonen av naturlig monopol ovenfor.

[10] Til sammenligning er det bare de aller færreste husholdninger som ikke er tilknyttet elektrisitetsnettet.

[11] Enitel gikk etter hvert konkurs, og mye av infrastrukturvirksomheten ble overtatt av BaneTele i 2001.

vasjon, noe som ville legge til rette for økt verdiskaping. Mulighetene for å lykkes med internasjonal ekspansjon ble også tillagt vekt.

Telenor/Telia-fusjonen strandet til slutt høsten 1999, men i 2000 ble Telenor delprivatisert og børsnotert. Den norske staten eier i dag 54 prosent av aksjene i Telenor. Den sentrale begrunnelsen for endringen i eierskapet var å styrke Telenors konkurransedyktighet og forretningsmessige handlefrihet (jf. St.prp. nr. 66, 1999-2000), ikke minst internasjonalt. Det ble pekt på følgende fordeler ved en børsnotering og delprivatisering:

- Realistiske og løpende markedsvurderinger av verdiskapingen og avkastningen i Telenor.
- Tilgang til egenkapital gjennom emisjoner og mulighet til å bruke egne aksjer som betalingsmidler i forbindelse med fusjoner og oppkjøp.
- En utbyttepolitikk som ses i sammenheng med verdiskapingen i Telenor og selskapets tilgang på lønnsomme investeringsprosjekter.
- Mulighet for å tilby strategisk deleierskap som ledd i internasjonale satsinger.
- Like konkurransevilkår med børsnoterte IKT-selskaper.

Samtidig ble det understreket at opprettholdelse av en strategisk statlig eierposisjon ville medvirke til mer stabile eierforhold og dessuten hindre at Telenor ble kjøpt opp.

Også det statlige eierskapet i BaneTele har vært diskutert, men uten at det er skjedd endringer så langt.

3.3.3 Utviklingen av virkemiddelapparatet

Lovverket overfor telesektoren og andre former for elektronisk kommunikasjon har vært gjenstand for betydelige endringer i løpet av de siste 10-15 årene. Det overordnede rammeverket for reguleringen var lenge *teleloven*. Et hovedmål med det regulatoriske rammeverket har vært å legge til rette for overgangen fra monopol til konkurranse i telesektoren og andre sektorer for elektronisk kommunikasjon. Bruk av maksimalpriser for enkelte leveringspliktige tjenester og krav om kostnadsorienterte priser for ulike typer teletjenester (blant annet nettadgang for andre tjenestetilbydere) har vært sentrale virkemidler.

I 2003 ble teleloven opphevet og erstattet av en egen lov om elektronisk kommunikasjon, *ekomloven*. Den dekker alle former for elektronisk kommunikasjon, ikke bare den tradisjonelle mobil- og fasttelefonivirksomheten. Loven omfatter både regulering av priser og tilgang og sikkerhets- og beredskapshensyn. I tilknytning til loven er det også utarbeidet et sett av forskrifter, hvor den såkalte *ekomforskriften* er den sentrale. Ekomloven og -forskriften gir Samferdselsdepartementet og Post- og teletilsynet sentrale roller i reguleringen av sektoren, også ivaretakelse av beredskapshensyn.

Lovens *formål* er å sikre brukerne i hele landet gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester. Det overordnede virkemidlet er konkurranse i alle ledd i sektoren. Det gjøres altså ikke noe prinsipielt skille mellom monopolvirksomhet og konkurranseutsatt virksomhet. Det er helt i tråd med den endrede faglige oppfatningen av kostnadsstrukturen i ekomsektoren. I forarbeidene til ekomloven sies det eksplisitt at det langsiktige målet er å benytte minst mulig særregulering overfor ekomsektoren, og i stedet basere reguleringen på allmenne konkurranseregler (jf. Ot.prp. nr. 58, 2002-2003). Loven bygger med andre ord på et prinsipp om *minimumsregulering*. I tillegg bygger loven på to andre hovedprinsipper: *teknologinøytralitet* og *ikke-diskriminering*. Konkurransen mellom tjenestetilbydere og krav om tilgang til nett og tjenester på ikke-diskriminerende vilkår skal stimulere til så vel kostnadseffektiv drift som investeringer og innovasjon.

Tilbydere med *sterk markedsstilling* kan pålegges særskilte forpliktelser. Begrepet sterk markedsstilling er definert i loven ved at tilbyderen «alene eller sammen med andre har økonomisk styrke i et relevant marked som gjør at tilbyder i stor grad kan opptre uavhengig av konkurrenter, kunder og forbrukere». Den aktuelle tilsynsmyndigheten kan benytte en rekke forskjellige virkemidler som pålegg om tilgang, krav om offentliggjøring av leveringsvilkår og regulering av priser for ulike tjenester. Eksempler på slike krav finnes i ekomforskriftens § 2-3, § 2-5 og § 2-6, hvor tilbyder med sterk markedsstilling pålegges å tilby overføringskapasitet til andre tilbydere og øvrige brukere, tilgang til fast aksessnett og samlokalisering.

Prisregulering skal bare brukes som virkemiddel for å korrigere for manglende konkurranse i den grad konkurransen ikke er effektiv nok. Det skjer blant annet i markedet for mobil terminering, hvor Telenor, NetCom og andre tilbydere alle vurderes å ha sterk markedsstilling. Prisene for mobil terminering reguleres derfor fortsatt (jf. Post- og teletilsynet, 2004).

Det kreves ikke lenger konsesjon for å tilby elektroniske kommunikasjonstjenester eller -nett, men det kreves konsesjon for tilgang til knappe ressurser som frekvenser og telefonnummer. For øvrige aktører gjelder det *registreringsplikt* i henhold til ekomforskriften. Telenor hadde før ekom-

loven en konsesjon som omfattet krav til leveringspliktige tjenester og spesielle samfunnspålagte oppgaver (herunder krav om levering av telefoni til hele landet, ytelser til funksjonshemmede, telefonautomater, katalog- og opplysningstjenester, nød- og sikkerhetstjenester knyttet til kystradioen og tjenester til Svalbard). Disse videreføres gjennom egne avtaler, ved særskilte pålegg eller gjennom forskrift (der forpliktelsene er generelle for aktører med sterk markedsstilling).

Beredskap og sikkerhet

Post- og teletilsynet og Samferdselsdepartementet har et særlig ansvar for beredskap og sikkerhet i ekomsektoren gjennom bestemmelsene i ekomloven og -forskriften. I tillegg finnes det flere andre myndighetsorganer med ansvar for beredskap og sikkerhet som også har oppgaver innen elektronisk kommunikasjon, som Nasjonal Sikkerhetsmyndighet (under Justisdepartementet) og Forsvaret.

Bestemmelsene i ekomloven bygger på den tidligere reguleringen av beredskap og sikkerhet i telesektoren slik den er blitt utviklet i årene etter dereguleringen, men er også betydelig videreutviklet for å tilpasses den nye markedssituasjonen. St.meld. nr. 47 (2000-2001) inneholder en analyse av situasjonen etter dereguleringen og forslag til tiltak. De sentrale trekkene i regelverket er følgende:

- Regelverket omfatter i prinsippet samtlige tilbydere og ikke bare Telenor, noe som åpenbart er nødvendig i lys av at mange brukere, også viktige samfunnsaktører, kjøper tjenester og tilgang til kommunikasjonsnett fra andre aktører enn Telenor.
- Telenor har tidligere hatt vilkår i sin konsesjon om å utføre spesielle samfunnspålagte oppgaver (SSO). Disse er ikke lenger en del av Telenors konsesjon, men ivaretas gjennom det generelle regelverket, som altså kan gjøres gjeldende overfor alle tilbydere av ekomtjenester. Post- og teletilsynet har inngått avtale med Telenor for 2005 om videreføring av tiltak i den tidligere SSO-avtalen, og har planer om å inngå tilsvarende avtaler med andre tilbydere som skal gjelde fra 2006 (se Post- og teletilsynet, 2004).

Ekomlovens § 2-10 stiller krav til tilbydere av elektroniske kommunikasjonsnett og -tjenester om at de skal opprettholde nødvendig sikkerhet og beredskap, herunder prioritere viktige samfunnsaktører ved behov. Myndighetene kan stille detaljerte krav om tiltak for å ivareta beredskaps- og sikkerhetshensyn gjennom forskrifter, enkeltvedtak eller avtaler. Tiltakene kan omfatte alt fra beredskapsplanlegging, øvelser, fysisk sikring av viktige installasjoner, formidling av informasjon fra statlige myndigheter til innføring av spesielle funksjoner og tjenester i kommunikasjonsnett, driftssystemer og driftsorganisasjoner. Kapittel 8 i ekomforskriften inneholder en rekke slike krav:

- Alle tilbydere som leverer elektroniske kommunikasjonstjenester direkte, eller som leverer overføringskapasitet og samtrafikk til leverandører, til brukere med samfunnskritisk funksjon skal ha oversikt over slike brukere og hvilke tjenester som er nødvendige for at brukeren skal kunne utføre sine funksjoner (§8-1)
- Alle tilbydere av ekomtjenester til brukere med samfunnskritisk funksjon skal lage planer og gjennomføre tiltak som er nødvendige for å opprettholde egen beredskap og for at brukere med samfunnskritisk funksjon skal kunne ivareta sine beredskapsoppgaver
- Det kan stilles krav om at tilbydere skal kunne opprettholde nødvendig tjenestetilbud for brukere med samfunnskritiske funksjoner uten driftsstøtte og elektroniske kommunikasjonstjenester lokalisert i andre land (dette kravet omtales gjerne som krav om *nasjonal autonomi*).
- Tilbydere av ekomtjenester skal gi prioritet til brukere med samfunnskritiske funksjoner i krise- og beredskapssituasjoner.

Tiltakene nevnt ovenfor er primært rettet inn mot ekstraordinære hendelser. Lovverket inneholder i tillegg en rekke bestemmelser for å ivareta hensyn til tilgjengelighet, konfidensialitet og integritet også i normale driftssituasjoner (jf. definisjonen av telesikkerhet og -beredskap ovenfor).[12] Det finnes også andre mer tekniske reguleringer, som for eksempel *Retningslinjer for beskyttelse av elektroniske installasjoner i totalforsvaret mot elektromagnetisk puls (EMP)*.

I det såkalte TIFKOM-prosjektet[13] ble en rekke tiltak for å styrke telesikkerhet og -beredskap (og elektronisk kommunikasjon generelt) drøftet. Flere av anbefalingene fra prosjektet er senere fulgt opp i ekomloven og -forskriften, men ikke

[12] I § 2-11 stilles det krav til tilbydere om at de skal utarbeide planer for å sikre leveransene til egne kunder i minimum to uker i tilfelle konkurs, åpning av gjeldsforhandlinger eller betalingsinnstilling. Bestemmelsen er imidlertid ikke trådt i kraft.

[13] TIFKOM-prosjektet (Teleberedskap i fritt konkurransemarked) ble gjennomført i 1999-2000 med Post- og teletilsynet som prosjektansvarlig i forvaltningen.

alle. Et krav som foreløpig ikke er blitt stilt, gjelder overtakelse av Telenors fjellanlegg og oppgradering av anleggene til sikrede samlokaliseringssentra hvor forksjellige teleoperatører kan plassere vitalt utstyr. I St. meld. nr. 47 (2000-2001) pekes det på at de mest aktuelle truslene mot ekomsikkerheten i Norge i dag ikke er av fysisk karakter og at kostnadene ved tiltaket er høyere enn den forventede nytten. Videre vil krav om samlokalisering føre til en sentralisering av viktige anlegg som kan tenkes å øke sårbarheten i forhold til et mer desentralt system. Endelig legger Samferdselsdepartementet vekt på at det vil bli vanskelig å få operatørene til å velge samlokalisering frivillig. Derimot gis Post- og teletilsynet i oppgave å legge til rette for framtidig samlokalisering.

3.4 Oppnåelse av sikkerhetsmål

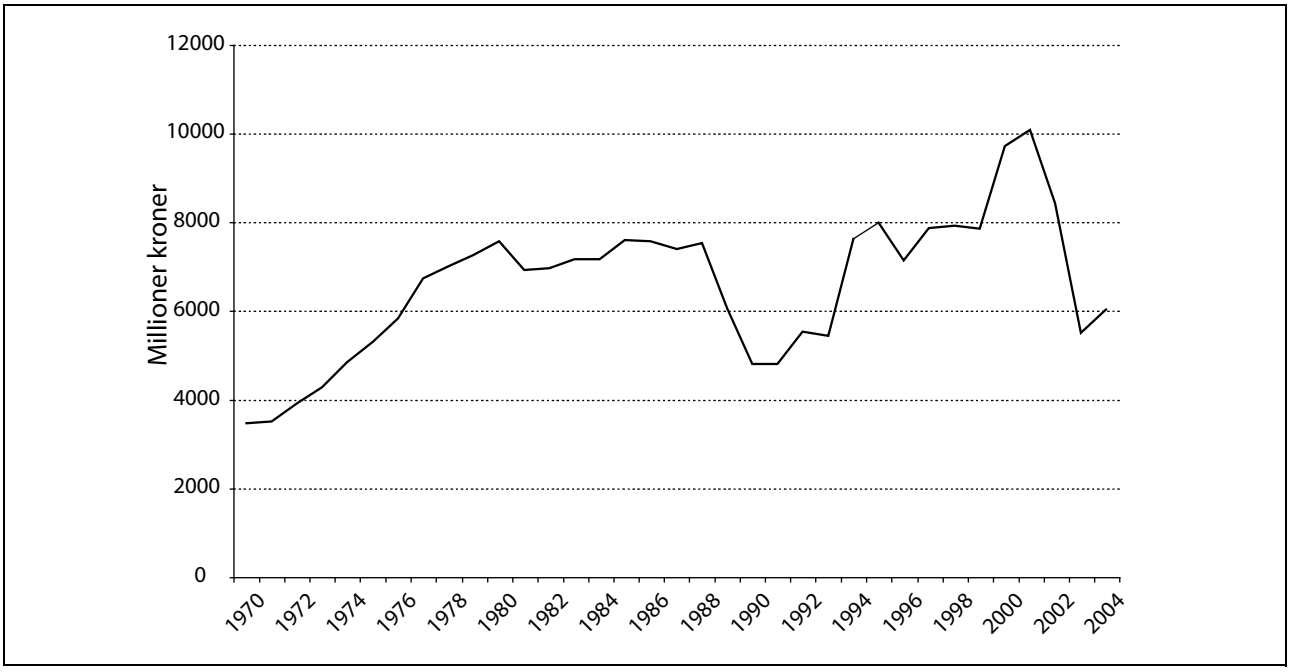
3.4.1 Erfaringer

Det finnes ingen landsomfattende statistikk over tilgjengeligheten og kvaliteten på infrastrukturene for elektronisk kommunikasjon. Det har vært enkeltepisoder hvor omfattende avbrudd har funnet sted som følge av tekniske feil, tredjepartsaktivitet i form av gravearbeider eller lignende, både i mobilnett og fasttelefoninett. Disse avbruddene har imidlertid ikke ført til omfattende kriser eller truet nasjonal sikkerhet (men har åpenbart gitt samfunnsøkonomiske tap i form av tapt arbeidstid og lignende). Datavirus, hackerangrep og lignende tredjepartsaktivitet skaper også utfordringer, men har så langt ikke gitt vedvarende problemer (utover de samfunnsøkonomiske kostnadene som påløper ved beskyttelsestiltak).

Videre har tilbudet av teletjenester og infrastruktur for elektronisk kommunikasjon gjennomgått store endringer i løpet av de siste 10-15 årene. Det finnes to landsdekkende GSM-nett og to UMTS-nett med betydelig dekning ved siden av fasttelefoni- og bredbåndsnett eid av Telenor og BaneTele. Det finnes det en rekke mer lokale nett for bredbånd basert på elnett, kabel-tv-nett osv. I tillegg til at antall aktører innen selve den fysiske infrastrukturen har økt, finnes det også et stort antall tjenestetilbydere uten egen infrastruktur i ulike markedssegmenter.

Figuren nedenfor viser utviklingen i investeringene i post- og telekommunikasjon med utgangspunkt i tall fra Nasjonalregnskapet. Tallene skiller ikke mellom post og tele, men størsteparten av investeringene finner sted i telesektoren (i 2003 utgjorde for eksempel investeringene i tele ca. 95 prosent av totalen).

Parallelt med utviklingen av nye tilbud rettet mot bedrifts- og privatmarkedet er det også bygd ut et eget digitalt nødnett i Forsvarets regi, og det er vedtatt at det skal bygges ut et nødnett for brannvesen, politi og helsevesen. Utviklingen av disse nettene er i noen grad drevet av den teknologiske utviklingen (behov for digital kommunikasjon, avlyttingssikkert utstyr etc.) og helt spesielle



Figur 12.4 Realinvesteringer i post- og telekommunikasjon 1970-2004. Millioner 2004-kroner

Kilde: Statistisk sentralbyrå, Nasjonalregnskapet

brukerbehov som det kan være vanskelig å tilfredsstille i det ordinære markedet.

3.4.2 Økonomiske incentiver til å ivareta beredskap og sikkerhet og rollen til andre virkemidler

Sårbarheten for den enkelte kunde og samfunnet som helhet overfor manglende kvalitet i ekomsektoren har økt betraktelig de siste årene. Stadig flere samfunnsprosesser avhenger av kontinuerlige og sikre leveranser av ekomtjenester. Avhengigheten vil etter all sannsynlighet øke ytterligere i framtiden. Spørsmålet blir dermed hvordan sentrale sikkerhets- og beredskapshensyn kan ivaretas innenfor det markedsbaserte rammeverket ekomsektoren er underlagt.

Det er mulig for myndighetene å definere og kjøpe tjenester knyttet til sikkerhet og beredskap. Delvis gjøres det allerede i dag gjennom eksisterende eller planlagte avtaler om sikkerhet og beredskap med Telenor og andre aktører som eier og/eller forestår drift av ekominfrastruktur. Det foregår også analyser av de tekniske og administrative spørsmål i forbindelse med innføring av prioritet i telenettene (jf. Post- og teletilsynet, 2004). Bruk av slike avtaler vil kreve at myndighetene bruker ressurser på å inngå avtaler og overvåke at de overholdes. For øvrig vil det påløpe slike transaksjons- og overvåkingskostnader også overfor offentlig eide aktører, men nivået kan selvsagt være forskjellig.

Teknologiutviklingen kan på sikt gjøre det mulig for brukerne å *diversifisere* risikoen for å bli rammet av manglende funksjonalitet, enten det skyldes tekniske feil, naturkatastrofer eller tredjepartsaktivitet. Kostnadene ved å være tilknyttet parallelle infrastrukturer for elektronisk kommunikasjon er relativt lave. Her skiller også ekomsektoren seg fra for eksempel kraftsektoren, hvor en i praksis bare kan spre risikoen ved å etablere egne reserveløsninger (nødstrømsaggregater og andre former for lokal kraftproduksjon hos den enkelte nettkunde). Dette forutsetter naturligvis at konkurransen i ekomsektoren er effektiv.[14] En annen kompliserende faktor er dessuten avhengigheten av deler av Telenors nett, som reduserer mulighetene for reell diversifisering i en del tilfeller.

Konkurransen har på sikt også implikasjoner for investeringene i den fysiske infrastrukturen, som igjen påvirker kvalitet og sikkerhet. Kvalitet og sikkerhet i infrastruktur for elektronisk kommunikasjon kan åpenbart være en konkurranseparameter. En tilbyder med utilfredsstillende kvalitet svekker sin konkurranseevne med økonomiske tap som konsekvens. Dersom det finnes en tilstrekkelig betalingsvilje for kvalitet og sikkerhet, vil sikkerhets- og beredskapshensyn kunne ivaretas i stor grad også innenfor en markedsbasert ramme ved at det investeres i nettet for å tilfredsstille kundenes etterspørsel etter sikre leveranser.

Det er likevel usikkert om konkurransen vil gi ønsket grad av redundans, som krever at det gjøres investeringer i ekstra kapasitet i nettene (for eksempel ringforbindelser). I den grad økt sikkerhet gjennom redundans utgjør et kollektivt gode, kan det imidlertid være vanskelig å realisere et optimalt investeringsnivå i markedet.[15] Dette er imidlertid noe som i så fall prinsipielt kunne løses via andre tiltak, for eksempel ved at de nødvendige investeringene bestilles og finansieres fra myndighetene (gitt at det skjer på en måte som ikke er i strid med de overordnede føringene om konkurransenøytralitet osv. som er nedfelt i gjeldende nasjonale lovverk og EU-direktiver). Det er heller ikke gitt at eventuelle problemer vil være store i praksis. Ekomaktørene vil ha incentiver til å gjennomføre felles investeringer i økt redundans og andre sikkerhetstiltak nettopp på grunn av kvalitetskravene på forbrukssiden. Antallet aktører er dessuten begrenset, slik at transaksjonskostnadene ved å komme fram til gode fellesløsninger ikke trenger å være uoverkommelige.

Det er vanskelig å se for seg at offentlig eierskap skal være noe egnet virkemiddel for å ivareta generelle sikkerhetsbehov i det ordinære markedet for elektronisk kommunikasjon. Det tradisjonelle fasttelefoninettet har fått konkurranse fra flere andre infrastrukturer. Stadig flere husholdninger, private bedrifter og offentlig sektor kjøper ekomtjenester og tilgang til infrastruktur fra andre aktører enn Telenor. Eierskap er mindre egnet som virkemiddel når sluttbrukerne er tilknyttet ulike fysiske infrastrukturer som i noen grad er uavhengige av hverandre. Den raske utviklingen i teknologi og tjenestetilbud forsterker dette forholdet. På disse punktene skiller ekomsektoren seg fundamentalt fra kraftsektoren, hvor så å si alle

[14] Utfordringene med å sikre effektiv konkurranse i ekomsektoren er blant annet drøftet i ECON og Oeconomica (2003) og Hagen (2003).

[15] Et kollektivt gode er kjennetegnet ved at den enkeltes forbruk ikke reduserer andres muligheter til å konsumere det samme godet. Eksempler på kollektive goder kan være luftkvalitet og i noen grad leveringssikkerhet i elnettet. Et genuint kollektivt gode kan ikke stykkes opp og selges i markedet enkeltvis, og det er derfor i henhold til klassisk samfunnsøkonomisk velferdsteori behov for offentlige inngrep (subsidier, skatter eller andre virkemidler) for å sikre at de kollektive godene produseres i optimalt omfang.

brukere av elektrisitet vil ønske å være tilknyttet det sentrale systemet for produksjon og overføring. Selv om betydelige trafikkmengder fortsatt går via Telenors nett, er det behov for å ivareta sikkerhet og kvalitet også i annen fysisk infrastruktur. Sikkerheten i Telenors nett er på denne måten nødvendig, men ikke tilstrekkelig for at alle brukere skal få levert ekomtjenester med et visst sikkerhetsnivå. Videre er det bare deler av Telenors nett som er relevant for andre fysiske ekominfrastrukturer.

Det er derfor behov for å etablere et regelverk som ivaretar sikkerhets- og beredskapshensyn gjennom påbud, standarder og økonomiske incentiver, uavhengig av eventuelt offentlig eierskap til én eller flere ekomaktører. Et slikt regelverk finnes i dag, og det er i stadig utvikling. Videre kan bruk av offentlig eierskap til å ivareta sikkerhetshensyn medføre konflikt mellom statens roller som regulator og sikkerhetsmyndighet på den ene siden og staten som eier av én eller flere kommersielle ekombedrifter på den andre siden.

Offentlig eierskap er på denne måten verken nødvendig eller tilstrekkelig til å ivareta samfunnets sikkerhetsinteresser innenfor en markedsbasert ramme. For enkelte brukere med særskilte behov kan egne nødnett være en egnet løsning. Det kan likevel ikke utelukkes at også slike brukere langt på vei kan få dekket sine behov i det ordinære markedet dersom dette er regulert på en hensiktsmessig måte (et annet spørsmål er hva som er den samfunnsøkonomisk riktige løsningen med hensyn til antall separate nødnett når kostnader og sikkerhets- og beredskapsbehov ses i sammenheng).

Endelig må det påpekes at utviklingen i ekomsektoren nødvendigvis også fører til at brukerne får et betydelig ansvar for egen sikkerhet (for eksempel ved å ha adekvat beskyttelse mot inntrengning i egne systemer, datavirus etc.).

3.5 Oppsummering

Omorganiseringen av den norske telesektoren med hensyn til regulering og eierskap har sin bakgrunn i teknologiske endringer som gjør det mulig å innføre konkurranse innen telefoni og andre former for elektronisk kommunikasjon. Den tradisjonelle oppfatningen av televirksomhet som naturlig monopol Den norske telereguleringen har de siste 10-15 årene vært innrettet mot å sørge for en overgang fra offentlig monopol til konkurranse. Ekomloven av 2003 reflekterer konvergensen mellom ulike teknologier for tele- og datakommunikasjon. Myndighetenes erklærte langsiktige mål er å bruke minst mulig særregulering overfor ekomsektoren og i stedet basere seg på allmenn konkranseregulering.

For å ivareta hensyn til sikkerhet og beredskap i ekomsektoren er det utviklet en rekke virkemidler som ivaretas av flere myndigheter, hvor Samferdselsdepartementet og Post- og teletilsynet har sentrale roller. Enkelte offentlige etater og virksomheter, som Forsvaret og nødetatene, har dessuten etablert eller planlegger å etablere egne digitale nødnett for å ivareta særskilte behov.

Aktørene i ekomsektoren vil dels være underlagt direkte reguleringer og påbud gjennom ekomloven, tilhørende forskrifter og andre former for krav fra myndighetenes side. Bruk av økonomiske sanksjoner (bøter, gebyrer etc.) vil gi åpenbare incentiver til å opprettholde beredskap og sikkerhet. I tillegg vil aktørene ha økonomiske incentiver gjennom eventuelle statlige kjøp av tjenester knyttet til sikkerhet og beredskap. Generelt gjør også markedet det mulig for brukerne å velge infrastrukturleverandører ut fra sikkerhets- og kvalitetshensyn. Manglende ivaretakelse av sikkerhet og beredskap kan på den måten få negative økonomiske konsekvenser for infrastrukturleverandører. For kundene kan det i noen grad dessuten bli mulig å forsikre seg mot manglende leveringskvalitet ved å være tilknyttet flere infrastrukturer.

Offentlig eierskap er et lite egnet virkemiddel for å ivareta hensyn til sikkerhet og beredskap. Det skyldes at brukerne må ventes å være tilknyttet forskjellige infrastrukturer for elektronisk kommunikasjon. En andel av brukerne - kanskje et flertall - vil bare i begrenset grad påvirkes av at offentlige eiere stiller egne krav til sikkerhet og beredskap overfor én enkeltaktør i egenskap av å være eier. Dette gjelder selv om deler av Telenors nett fortsatt spiller en viktig rolle også for andre eiere av fysisk infrastruktur. Offentlig eierskap til nett som dekker spesielle behov for visse typer brukere er et annet spørsmål.

4 Petroleum

4.1 Petroleum som kritisk infrastruktur

Petroleumssektoren spiller en viktig rolle som kritisk infrastruktur gjennom inntektene som tilføres staten som eier av oljeselskaper og som skattekreditor. Statens netto kontantstrøm fra petroleumsvirksomheten beløp seg til ca. 210 milliarder kroner i 2004, og er i statsbudsjettet for 2006 estimert til 283 milliarder kroner i 2005 (jf. St.prp. nr. 1, 2005-2006). Skatter og inntekter fra SDØE (Statens

Direkte Økonomiske Engasjement) utgjør størstedelen av nettokontantstrømmen.[16] Petroleumssektoren bidro med 21 prosent av Norges BNP i 2004.

Petroleumsvirksomheten har også et betydelig potensial for store ulykker med betydelig tap av liv og helse (jf. NOU 2000:24 og Petroleumstilsynet, 2005), og hendelser på sokkelen eller land kan medføre store miljøskader. I motsetning til kraftsektoren og ekomsektoren er derimot petroleumsvirksomheten ikke spesielt viktig for funksjonaliteten til andre kritiske infrastrukturer.

Ivaretakelse av beredskap og sikkerhet i petroleumssektoren er nødvendig både for å opprettholde inntektsstrømmen fra produksjonen av olje og gass og for å unngå miljøskader eller tap av liv. Det stiller blant annet krav til oppfyllelse av hensiktsmessige krav til helse, miljø og sikkerhet i den løpende driften av anleggene på sokkelen og tilhørende landanlegg. Det er også ønskelig med en robust petroleumsinfrastruktur som samlet sett er lite sårbar for hendelser i enkeltanlegg, enten hendelsene skyldes ulykker, svikt eller bevisste anslag. Det siste stiller krav til utviklingen av infrastrukturen og investeringene over tid.

4.2 Den norske petroleumssektoren

Petroleumsvirksomheten på den norske kontinentalsokkelen har vært i drift i over 30 år. 2004 utgjorde toppåret så langt med en samlet produksjon på 263 millioner Sm3 oljeekvivalenter, noe som gjorde Norge til verdens 7. største oljeprodusent. Oljeproduksjonen er ventet å avta fra 2007, mens produksjonen av gass vil øke fram mot 2010 og deretter nå et platå. Fra 2014 er det ventet at gass vil utgjøre mer enn 50 prosent av den samlede produksjonen målt i Sm^3 oljeekvivalenter (se Olje- og energidepartementet, 2005). Utviklingen avhenger imidlertid av framtidig leteaktivitet og at det gjøres drivverdige funn.

Den fysiske petroleumsinfrastrukturen består av havbunnsinstallasjoner, faste og flytende installasjoner, rørledninger for transport av olje- og gass, prosesseringsanlegg, landterminaler og lagre. Eierskapet til installasjonene er fordelt mellom rettighetshaverne på de ulike feltene. Eierskapet til gasstransportsystemet er organisert i et interessentskap, Gassled, som har 10 oppstrømsaktører som eiere, hvorav Petoro er størst med 38,3 prosent etterfulgt av Statoil med 20,4 prosent.[17]

Det statlige eierskapet i sektoren består i ca. 71 prosent av aksjene i Statoil (pr. oktober 2005), 43,8 prosent av aksjene i Norsk Hydro (pr. oktober 2005) samt SDØE, som forvaltes av det helstatlige aksjeselskapet Petoro. I tillegg eier staten Gassco, som er systemoperatør for gassinfrastrukturen. Statoil, Hydro og Petoro er de tre største aktørene på sokkelen målt i antall utvinningstillatelser. Statoil og Hydro har også flest operatørskap. Totalt er det 24 norske og utenlandske aktører som har operatørskap og ytterligere 10 som har utvinningstillatelser (se Olje- og energidepartementet, 2005).

4.3 Samfunnsøkonomisk begrunnelse for organisering og eierskap

4.3.1 Bakgrunnen for omorganiseringen av petroleumssektoren

Statoil ble dannet i 1971, og har siden vært den sentrale offentlige aktøren i norsk petroleumsvirksomhet. Statoil eier både oljeinstallasjoner og deler av infrastrukturen for gasstransport. Selskapet har også vært operatør for store deler av gasstransportsystemet. Det overordnede målet med organiseringen og eierskapet var å sikre en samfunnsøkonomisk effektiv utbygging av de norske petroleumsressursene og sikre at en størst mulig andel av grunnrenten i sektoren tilfaller det norske samfunnet. I tillegg var det en rekke andre politiske mål knyttet til blant annet næringsutvikling og lokaliseringen av petroleumsvirksomheten på land. Statoil var et viktig instrument også i disse sammenhengene. I 1985 ble deler av Statoils portefølje skilt ut som Statens Direkte Økonomiske Engasjement, som var direkte eid av staten ved Olje- og energidepartementet. SDØE ble imidlertid fortsatt forvaltet av Statoil. Salget av gass fra sokkelen ble ivaretatt gjennom GFU (gassforhandlingsutvalget), som hadde monopol på salg av norsk gass.

Samfunnsøkonomisk ligner deler av petroleumsinfrastrukturen på andre infrastrukturer som elnettet. Det gjelder særlig infrastrukturen for transport av gass, som kan betegnes som et naturlig monopol.[18] Det har derfor ikke vært samfunnsøkonomisk ønskelig å etablere parallelle infrastrukturer for gasstransport. I motsetning til for eksempel kraftsektoren har imidlertid eierskapet til gassinfrastrukturen ligget hos oppstrømsaktørene (produsentene av gassen) separat. Den tradisjonelle modellen for driften av systemet var at en av eierne av hvert enkelt gassrørledningsnett

[16] I tillegg kommer utbytte fra Statoil, CO2-avgift og arealavgift.

[17] Etter planen skal Petoros andel øke til 47,8 prosent i 2011.

[18] Nese og Hagen (1998) inneholder en diskusjon av kostnadsstrukturen i gasstransportsystemet på den norske kontinentalsokkelen.

hadde operatøransvar. Behovet for koordinert drift og utvikling av infrastrukturen kunne i stedet ivaretas gjennom GFU-ordningen. I GFU ble det fattet beslutninger om hvilke gassfelter som skulle bidra til å oppfylle de forskjellige leveringsavtalene og hvilke transportløsninger som skulle velges.

De siste 5-10 årene har flere trender og drivkrefter gitt opphav til en omfattende debatt om organiseringen av den norske petroleumssektoren:

- Den norske kontinentalsokkelen er blitt en moden petroleumsprovins. Nivået på oljeproduksjonen er nær toppen, mens gassproduksjonen er ventet å vokse en del fortsatt. Ekspansjonsmulighetene for Statoil ligger derfor primært utenfor Norge.
- 1990-tallet var preget av en rekke store fusjoner og oppkjøp innen internasjonal petroleumsindustri. Helstatlig eierskap kunne være en hemsko for Statoil dersom selskapet skulle ønske å delta i den internasjonale omstruktureringen.
- EUs konkurranseregler og innføringen av gassdirektivet skapte press mot GFU-ordningen og dermed hele organiseringen av gasssalg og -transport fra sokkelen. En ordning med koordinert gassalg via et monopol som GFU var vanskelig å forene med EUs regelverk. EU-kommisjonen sendte i 2001 et klageskrift (Statement of Objections) til rettighetshavere på norsk sokkel der kommisjonene hevdet at GFU-ordningen var i strid med konkurransereglene.
- Kostnadsnivået på sokkelen ble vurdert som et problem for verdiskapingen. Blant annet ble det identifisert et behov for å endre eiersammensetningen i ulike felt for å stimulere til en mer kostnadseffektiv utnyttelse av ressursene.
- Økt mangfold i aktørbildet, særlig ved å legge til rette for at mindre aktører vant innpass, ble vurdert som positivt for å stimulere til økt leteaktivitet.
- Det var utviklet et omfattende virkemiddelapparat i form av skattesystemet, konsesjonssystemet og forskjellige lover, forskrifter og enkeltvedtak som kunne ivareta de samfunnsmessige målene med petroleumsvirksomheten. Statoil var blitt mindre viktig som politisk instrument.
- En betydelig del av statens inntekter stammer fra petroleumssektoren, slik at statens inntekter var svært eksponert for oljeprisrisiko.

Samtidig er det klart at de grunnleggende økonomiske kjennetegnene ved infrastrukturen i sektoren, som det naturlige monopolet innen gasstransport, ikke er endret. Her skiller petroleumssektoren seg fra telesektoren, hvor det naturlige monopolet langt på vei er erstattet av konkurranse mellom infrastrukturer.

4.3.2 Valg av organisering og eierskap

I perioden 2000-2005 har det skjedd en rekke endringer i organiseringen av den norske petroleumsvirksomheten:

- Statoil ble delprivatisert (gjennom emisjon og nedsalg) og børsnotert i 2001. I første omgang ble den statlige andelen redusert til 82 prosent. Etter ytterligere nedsalg er den statlige eierandelen redusert til 71 prosent. Ansvaret for SDØE-andelene ble overført til et nytt statlig selskap, Petoro AS, i 2001, og 21,5 prosent av SDØE-porteføljen er blitt solgt. (Se St.prp. nr. 36, 2000-2001, og Innst. S. nr. 198, 2000-2001).
- Eierskapet til gasstransportsystemet ble overført til et nytt interessentskap, Gassled, hvor de tidligere eierne av gassinfrastrukturen er representert som eiere (med enkelte unntak). Kapasiteten i Gassled disponeres av en uavhengig systemoperatør, det statseide Gassco, som ble etablert i 2001. Gassco tildeler kapasiteten i transportsystemet til skipere av gass i henhold til definerte regler, og opererer også et annenhåndsmarked for transportkapasitet.
- GFU ble nedlagt i 2002, og ansvaret for salget av statens gass er overført til selskapene som eier gassen.

Målene med delprivatiseringen av Statoil var flere:

- Gi Statoil like konkurransevilkår med andre oljeselskaper
- Klargjøre statens roller i petroleumsvirksomheten og understreke Statoils rolle som kommersiell aktør
- Legge til rette for løpende markedsvurdering av verdiskapingen i Statoils virksomhet og på den måten gi signaler om Statoils forretningsmessige disposisjoner

Det ble slått klart fast at Statoil ikke lenger var et sektorpolitisk instrument, men skulle styres etter forretningsmessige kriterier. Fullt statlig eierskap var verken nødvendig eller hensiktsmessig for å realisere hovedmålene med petroleumspolitikken. EØS-avtalen og EUs regelverk la dessuten begrensninger på mulighetene til å bruke gi Statoil særfordeler og bruke selskapet som et sektorpolitisk instrument.

Salget av SDØE-andeler og etableringen av Petoro var tilsvarende begrunnet i flere forhold (jf. St.prp. nr. 36, 2000-2001):

- Maksimere verdien av statens petroleumsvirksomhet gitt risikoen i sektoren
- Styrke de industrielle aktørene på sokkelen
- Øke effektiviteten på sokkelen gjennom en mer hensiktsmessig eierstruktur som styrker incentivene til å drive de ulike feltene effektivt

Petoro skal ivareta statens direkte eierandeler og være en aktiv partner i de ulike lisensene. I tillegg skal selskapet overvåke at Statoil utfører avsetningen av statens petroleum i samsvar med Statoils avsetningsinstruks. Avsetningsinstruksen innebærer at Statoil skal avsette statens petroleum sammen med sin egen for å maksimere verdien av statens samlede petroleumsinteresser (Statoil pluss SDØE).

Da koordineringen av gasstransporten gjennom GFU falt bort, var det nødvendig å innføre en institusjon med sentralt systemansvar etter mønster av kraftsektoren, hvor én aktør har ansvar for den løpende systemdriften og fordelingen av tilgjengelig kapasitet i systemet. Gassco overtok operatøransvaret for det samlede gasstransportsystemet fra Statoil og andre selskaper. I motsetning til Statnett, systemoperatøren i den norske kraftsektoren, eier imidlertid ikke systemoperatøren Gassco infrastrukturen selv.

I valget av organisasjonsmodell for gassinfrastrukturen la departementet vekt på at gasstransport utgjør et naturlig monopol som må reguleres. Videre ble det understreket at infrastrukturen for gass er et helhetlig transportsystem med en høy grad av fleksibilitet i koordineringen av leveranser fra forskjellige felt, samtidig som den høye graden av gjensidig avhengighet mellom de forskjellige delene av systemet gjorde driftskoordineringen til en kompleks oppgave som må styres fra et sentralt kontrollsenter (i tråd med organiseringen før opprettelsen av Gassco). Det overordnede hensynet til samfunnsøkonomisk effektiv forvaltning av gassressursene tilsa at det burde være én nøytral og uavhengig systemoperatør:

- Det var et uttrykt ønske fra myndighetene om at «den sentrale premissleverandøren skal være nøytral og uavhengig». Dersom systemansvaret ble ivaretatt av en aktør med eierinteresser på produksjonssiden, som Statoil, ville det gi aktøren mulighet å påvirke utviklingen av infrastrukturen ut fra egne interesser og ikke nødvendigvis ivareta samfunnsøkonomisk hensyn.
- Enkeltselskaper måtte ikke få informasjonsfordeler som kunne utnyttes forretningsmessig. Det beste virkemidlet mot dette var ifølge Olje- og energidepartementet en uavhengig og nøytral systemoperatør.
- Med et fullstendig selskapsmessig skille mellom gassproduksjon og systemansvar unngikk en incentiver til kryssubsidiering (i dette tilfellet i form av overveltning av kostnader fra den konkurranseutsatte oppstrømsvirksomheten til det naturlige monopolet).

Statlig eierskap i viktige gassfelt som Troll, Oseberg og Ormen Lange ble vurdert som viktig for å legge til rette for en optimal utnyttelse av samordningsgevinster mellom felt. De store feltene spiller en særlig viktig rolle i utnyttelsen av samordningsgevinster.

4.3.3 Utviklingen av virkemiddelapparatet

I takt med endringene i eierskapet er det skjedd en rekke endringer også i virkemiddelapparatet overfor petroleumssektoren.

Økonomi

Petroleumsinntektene til staten er blitt sikret gjennom et system med særbeskatning av olje- og gassvirksomheten på sokkelen (50 prosent av særskattepliktig inntekt), som gir en marginalskatt på 78 prosent for selskaper i full skatteposisjon. Det er de siste årene blitt gjennomført flere endringer i skattesystemet for å stimulere til økt leteaktivitet og lavere inngangsbarrierer for nye aktører, men endringene.

Leting og utbygging

Beslutninger om leting og utbygging er blitt håndtert gjennom et omfattende regelverk som ligner konsesjonsordningene for andre infrastrukturer. Siktemålet med regelverket er å sørge for en rasjonell utnyttelse av petroleumsressursene, herunder oppnå en hensiktsmessig samlet utbygging av petroleumsinfrastrukturen. Med utgangspunkt i petroleumsloven med tilhørende forskrifter gjennomføres blant annet konsesjonsrunder for tildeling av oppstrømsressursene, som inkluderer konsekvensutredninger, undersøkelsestillatelser, utvinningstillatelser, og krav om samarbeidsavtaler i lisenser. Samlede utbyggingsløsninger inklusive transportløsninger godkjennes av Olje- og energidepartementet og eventuelt Stortinget. Det skal leveres inn planer for utbygging og drift (PUD) og eventuelt for anlegg og drift (PAD).

Regelverket består i all hovedsak også med den nye organiseringen og endringene i eierskapet. Det er imidlertid innført noen nye tiltak innenfor

det etablerte rammeverket. I 2003 ble det innført en ordning med tildeling av utvinningstillatelser i forhåndsdefinerte områder (TFO) i modne deler av sokkelen (jf. St.meld. nr. 38, 2003-2004). Ordningen innebærer blant annet at store forhåndsdefinerte leteområder gjøres tilgjengelige for selskapene og faste årlige rutiner for gjennomføring av konsesjonsrundene. Myndighetene kan også beslutte at enkelte områder ikke skal åpnes for petroleumsvirksomhet (som har vært tilfelle for Nordland VI-området rundt Lofoten så langt). Det har i 2005 vært gjennomført en høring om endringer i arealavgiften for å stimulere til rask og effektiv utforsking og eventuelt produksjon.

Gasstransport

Som ledd i omorganiseringen av gasstransporten er det gjort en rekke endringer i lovverket:

- Operatørrollen er tatt inn som en egen paragraf i petroleumsloven (§4-9). Her heter det blant annet at «den helhetlige driften av oppstrøms gassrørledningsnett og tilknyttede anlegg skal skje i samsvar med forsvarlige tekniske og sunne økonomiske prinsipper. Den som har det særlige operatøransvar som nevnt i første ledd, skal opptre nøytralt og ikke-diskriminerende.» Videre heter det at operatøren «også skal treffe avgjørelser vedrørende adgang til oppstrøms gassrørledningnett, og at denne kan gi pålegg til eiere og brukere av oppstrøms gassrørledningsnett og tilknyttede anlegg og til rettighetshavere til utvinningstillatelser hvor det utvinnes petroleum, om å tilpasse sin virksomhet. Slikt pålegg skal kunne gis for å sikre en forsvarlig ressursforvaltning og effektiv drift av det aktuelle oppstrøms gassrørledningsnett.»
- Gassco, som har fått operatøransvaret, har fått et særskilt ansvar for utviklingen av systemet for gasstransport. Selskapet skal ikke gjøre egne investeringer eller eie infrastruktur, men skal samordne prosessene for videreutvikling av gasstransportsystemet og vurdere behovet for videreutvikling. Gassco har på denne måten fått tildelt en rolle som *systemarkitekt*. Et sentralt element i utøvelsen av arkitektrollen er utarbeidelsen av en rullerende 10-års transportplan basert på informasjon fra aktørene på sokkelen, som oppdateres årlig. Basert på transportplanen skal Gassco gi «forslag til forbedrende løsninger og videre utvikling av infrastrukturen» (se www.gassco.no).
- I samsvar med EUs gassdirektiv er det åpnet for tredjepartsadgang til gasstransportsystemet. Fra 2003 er prinsippene for fastsettelse av tariffene i Gassled nedfelt i en egen forskrift til petroleumsloven. Tariffene er basert på de faktiske kostnadene ved å transportere gassen, inklusive en tillatt kapitalavkastning på 7 prosent reelt før skatt. Transporttariffene har også tidligere vært gjenstand for offentlig regulering langs de samme linjene som nå er forskriftsfestet.

Beredskap og sikkerhet

Petroleumstilsynet har ansvar for sikkerhetsarbeidet i petroleumssektoren med vekt på HMS-regelverket. Regelverket er nedfelt i forskrifter med utgangspunkt i flere lover, blant annet petroleumsloven og arbeidsmiljøloven. Petroleumstilsynet ble opprettet i 2004, og er underlagt Arbeids- og sosialdepartementet (fra 1.1.2006 Arbeids- og inkluderingsdepartementet). Tilsynet har overtatt oppgaver som tidligere var underlagt Oljedirektoratet, Arbeidstilsynet og Direktoratet for samfunnssikkerhet og beredskap (se St.meld. nr. 17, 2002-2003).

Olje- og energidepartementet har som overordnet sektormyndighet ansvar for andre deler av sikkerhets- og beredskapsarbeidet. Petroleumsloven med tilhørende forskrifter er det sentrale styringsverktøyet. For eksempel inneholder petroleumsloven bestemmelser om levering til nasjonalt behov og levering i tilfelle krig, krigsfare eller andre ekstraordinære situasjoner. Den norske staten kan med hjemmel i disse bestemmelsene pålegge rettighetshavere å levere petroleum til utvalgte mottakere innenlands til dekning av nasjonalt behov (mot vederlag beregnet etter bestemte regler). I tilfelle krig og lignende situasjoner kan rettighetshavere pålegges å stille petroleum til disposisjon for norske myndigheter.

Olje- og energidepartementet vurderte i Ot.prp. nr. 46 (2002-2003) at fleksibiliteten med hensyn til alternative transportveier har økt, noe som igjen har ført til en reduksjon i sårbarheten i infrastrukturen på sokkelen og økt leveringssikkerhet. Det var likevel behov etter departementets vurdering behov for å styrke beredskapen ytterligere. Et konkret tiltak var å innføre en ny paragraf (§9-3) i petroleumsloven som pålegger rettighetshavere på sokkelen visse plikter for å opprettholde nødvendige sikrings- og beredskapstiltak mot bevisste anslag i fredstid. Loven omfatter følgende forpliktelser:

- Plikt til å iverksette og opprettholde sikringstiltak
- Plikt til å ha beredskapsplaner vedrørende bevisste anslag

– Plikt til å stille innretninger til disposisjon i forbindelse med øvelser og til å delta i slike øvelser

Lovens § 9-2 inneholder fra før lignende bestemmelser vedrørende beredskap mot fare- og ulykkessituasjoner som skyldes menneskelig svikt, tekniske forhold og lignende. Fra før finnes det også en bestemmelse (§9-4 i gjeldende lov) om *sikkerhetssoner*. Rettighetshavere har etter denne bestemmelsen en plikt til å opprette sikkerhetssoner rundt og over visse innretninger på sokkelen.

4.4 Oppnåelse av sikkerhetsmål

4.4.1 Erfaringer

Petroleumstilsynet publiserer en årlig rapport om risikonivået på norsk sokkel med vekt på personrisiko. Petroleumstilsynet konkluderer i sin rapport for 2004 med at det ikke er noen klare utviklingstrekk for totalindikatoren for risikonivået, selv om enkelte hendelser som karakteriseres som meget alvorlige trekker opp i 2004 (se Petroleumstilsynet, 2004).[19] For 2004 konkluderer derfor Petroleumstilsynet med at risikoen for tap av liv på norsk sokkel har økt sammenlignet med gjennomsnittsnivået 1996-2003. Tilsynet har gitt flere pålegg og kritikk av operatørene i forbindelse med hendelsene som følge av brudd på HMS-regelverket. Samtidig viser de fleste storulykkesindikatorene som benyttes av tilsynet nedgang eller stabilt nivå for 2004. Antall alvorlige personskader økte i siste halvdel av 1990-tallet, men er siden redusert.[20]

Det har inntruffet flere hendelser som følge av ulykker eller menneskelig svikt som har medført stans eller reduksjon i produksjonen i enkelte installasjoner over kortere eller lengre perioder.[21] Generelt er imidlertid petroleumsvirksomheten på den norske kontinentalsokkelen preget av høy tilgjengelighet og leveringssikkerhet.

Investeringsnivået i petroleumsvirksomheten drives i stor grad av leteaktiviteten og utbygging av konkrete funn, og det er vanskelig å lese noen trender med hensyn til sikkerhet ut av makrotallene for investeringene i sektoren. Olje- og energidepartementet konkluderte i Ot.prp. nr. 46 (2002-2003) som nevnt med at sårbarheten i infrastrukturen på sokkelen var redusert som følge av økt fleksibilitet med hensyn til alternative transportveier.

4.4.2 Økonomiske incentiver til å ivareta beredskap og sikkerhet og rollen til andre virkemidler

Det kan i prinsippet være en konflikt mellom sikkerhetshensyn og ønsket om lavest mulige kostnader og maksimalt overskudd fra petroleumsvirksomheten. Petroleumstilsynet har likevel argumentert for at HMS-regelverket for flyttbare boreinnretninger, som har vært viet særlig oppmerksomhet, ikke er fordyrende sammenlignet med regelverket i andre land (se Petroleumstilsynet, 2005). I et bedriftsøkonomisk perspektiv er det også klare incentiver til å gjennomføre sikkerhetstiltak, som reduserer eller fjerner den mulige konflikten mellom sikkerhet og lønnsomhet. Manglende ivaretakelse av sikkerhetshensyn skaper en risiko for stans i produksjonen, som i sin tur kan gi betydelige inntektstap. Det samme gjelder manglende beredskap mot bevisste anslag. På sikt kan manglende ivaretakelse av sikkerheten fra en aktørs side føre til tap av troverdighet og reduserte muligheter til å investere i nye prosjekter på norsk sokkel.

Kostnadene ved sikkerhetstiltak må imidlertid også avveies mot nytten av tiltakene, som igjen henger sammen med oppfatningen av risikoen. Det gjelder både i et samfunnsøkonomisk og et bedriftsøkonomisk perspektiv. I den grad samfunnets oppfatning av risikoen avviker fra den bedriftsøkonomiske, kan sikkerhetstiltakene bli utilstrekkelige sett fra et samfunnsøkonomisk perspektiv.

Offentlig eierskap er uansett ikke et særlig egnet virkemiddel til å løse denne typen målkonflikter. En betydelig del av petroleumsvirksomheten på den norske kontinentalsokkelen skjer i regi av aktører med privat og/eller utenlandsk eierskap. Det er derfor uansett behov for et effektivt sikkerhetsregelverk med tilstrekkelige sanksjonsmuligheter. En rekke slike virkemidler er tilgjengelige i dagens lovverk og forskrifter. Offentlig eierskap er i beste fall et partielt virkemiddel for å ivareta sikkerhetshensyn, og vil være overflødig som virkemiddel dersom det generelle sikkerhetsregelverket og håndhevingen av det fungerer godt nok.

Når det gjelder investeringer i transportsystemet for gass, er bildet sammensatt. Dersom inves-

[19] De aktuelle hendelsene omfatter den undersjøiske gassutblåsingen på Statoils Snorre A-innretning i november, brudd på en gassrørledning fra Jotun A i august og tap av ankerkjettinger fra den flyttbare boreinnretningen Ocean Vanguard i desember.

[20] Foreløpige tall for første halvår 2005 viser en økning i antall alvorlige personskader, mens flere andre indikatorer går ned. Se Petroleumstilsynet (2005b). Tilsynet understreker at tallene ikke er ferdiganalysert og at de kan bli gjenstand for endringer.

[21] Jf. Snorre A-utblåsingen.

teringene i transportsystemet primært skjer for å frakte gass fra ett punkt til et annet, kan infrastrukturinvesteringene i stor grad integreres med investeringene i oppstrømsanlegg uten samfunnsøkonomiske tap. Mange av gassprosjektene på norsk sokkel har dessuten vært av en slik fysisk og økonomisk størrelse at de har kunnet finansiere sine egne infrastrukturinvesteringer.

Det er imidlertid sannsynlig at de fleste nye gassfunn vil være av en begrenset størrelse, noe som kan medføre at investeringer i økt transportkapasitet blir ulønnsomt når utbygginger vurderes enkeltvis (jf. St. meld. nr. 38, 2003-2004, og Kon-Kraft, 2003). Da blir det også behov for å koordinere utbyggingen av ny infrastruktur mellom flere uavhengige aktører (i den grad en ikke kan ta i bruk ledig kapasitet i eksisterende infrastruktur etter hvert som andre felt reduserer produksjonen). Det reiser kompliserte økonomiske problemstillinger, og det er et åpent spørsmål hvordan dagens organisering vil fungere på sikt.[22]

Ofte er det også ønskelig å gjøre investeringer for å etablere alternative transportveier, ringforbindelser og lignende, som reduserer sårbarheten og styrker leveringssikkerheten. Integrerte investeringer i maskede nett, der nytten kan tilfalle mange aktører, kan være vanskelige å gjennomføre innenfor en ramme der infrastrukturinvesteringene besluttes og gjennomføres av uavhengige aktører. Dels skyldes det at sikkerheten i det samlede systemet har karakter av å være et kollektivt gode i noen grad (jf. diskusjonen av leveringssikkerhet i kraft- og telesektorene). Det kan også være incentiver til å agere strategisk for å dra nytte av investeringer i det felles transportsystemet uten å måtte betale kostnadene (gratispassasjerproblemer). Videre kan ulike oppstrømsaktører ha forskjellige interesser med hensyn til hvilke felt som skal bygges ut og hvilke markeder gassen skal selges til.

Det er altså flere utfordringer knyttet til videreutviklingen av gasstransportsystemet. Disse utfordringene har åpenbare implikasjoner for verdiskapingen på sokkelen, men kan også påvirke leveringssikkerheten og robustheten i systemet. I prinsippet kan Gassco som systemarkitekt definere og anbefale investeringer som styrker leveringssikkerheten og på den måten bidra til å redusere koordineringsproblemer mellom aktørene. Staten har på den måten tilgang til et viktig virkemiddel for å påvirke investeringene i ønsket retning. Det er imidlertid ikke gitt at Gassco har alle de nødvendige virkemidlene for at de riktige investeringene i ny infrastruktur skal realiseres.

Enkelte (blant annet Kon-Krafts aktivitetsprosjekt, jf. Kon-Kraft, 2003) har foreslått at staten gjennom SDØE bør bidra med større andeler i infrastruktur for å sikre tilstrekkelige investeringer. Olje- og energidepartementet vurderer likevel i St.meld. nr. 38 (2003-2004) at det er formålstjenlig at gassinfrastrukturen utvikles av selskaper med oppstrømskompetanse og eget transportbehov. Departementet konkluderer med at «i utgangspunktet bør statens andel i infrastruktur derfor reflektere statens andel i de ressursene som forventes å benytte denne infrastrukturen». I St.meld. nr. 38 (2003-2004) konkluderer regjeringen med at de vil «spesielt følge opp studien Gassco utfører i samarbeid med berørte parter for å utvikle gasstransportkapasitet fra Halten/Nordland, og foreta en vurdering om dagens ordning for etablering av ny gassinfrastruktur er hensiktsmessig i etterkant av denne prosessen».[23]

4.5 Oppsummering

Endringene i eierskapet i Statoil, forvaltningen av SDØE og organiseringen av gasstransporten fra norsk sokkel har sitt utspring i både nasjonale og internasjonale utviklingstrekk. Dels er det bygd opp et omfattende regelverk som ivaretar ulike sektorpolitiske mål slik at eierskapet i Statoil og andre oljeselskaper ikke lenger er noe egnet instrument utover hva som følger av bedriftsøkonomiske mål. Dels har EUs gassdirektiv og konkurranseregler endret handlingsrommet for organiseringen av gassalget og gasstransporten. Det har også vært vurdert som ønskelig å stimulere til strukturendringer og økt kostnadseffektivitet på sokkelen for å øke verdiskapingen. Endringer i eierskap og organisering er viktige virkemidler i det henseende.

Sikkerhets- og beredskapshensyn ivaretas av flere myndighetsorganer, men Petroleumstilsynet og Olje- og energidepartementet har særlig viktige roller. I tillegg til påbud og andre reguleringer gjennom lover og forskrifter vil rettighetshavere i den norske petroleumssektoren ha bedriftsøkonomiske incentiver til å ivareta beredskap og sikkerhet. Manglende ivaretakelse av sikkerhetshensyn

[22] Kon-Kraft (2003) og St.meld. nr. 38 (2003-2004) inneholder diskusjoner av disse spørsmålene.

[23] Bjørndalen og Nese (2003) inneholder en diskusjon av organiseringen av transportsystemet for naturgass, med vekt på incentivene til optimal utnyttelse av den eksisterende kapasiteten. Mye av diskusjonen er imidlertid også relevant i et investeringsperspektiv. Blant annet peker de på incentivvirkningene av at flere aktører både er skipere av gass og eiere av Gassled.

vil føre til inntektstap ved at produksjon går tapt. Det kan likevel være grunn til å spørre om de bedriftsøkonomiske incentivene vil være sterke nok til at samfunnets mål for sikkerheten og beredskapen nås. Offentlig eierskap vil imidlertid ikke være tilstrekkelig til at samfunnets sikkerhetsbehov med hensyn til petroleumsvirksomheten vil ivaretas. Det skyldes at en betydelig del av petroleumsressursene og installasjonene er eid av ikke-offentlige aktører. Det er derfor behov for et effektivt regelverk for sikkerhet og beredskap uansett.

Når det gjelder investeringer som gjør petroleumsinfrastrukturen mer fleksibel og robust, er det usikkert om dagens organisering vil gi de rette investeringene over tid. Dette er særlig viktig for gasstransportsystemet. Gjennom systemoperatøren Gassco har imidlertid staten et viktig verktøy for å påvirke investeringsbeslutningene i gassinfrastruktur.

5 Oppsummering og konklusjoner

Vi har i dette notatet sett nærmere på bakgrunnen for omorganiseringen av tre norske infrastruktursektorer: Kraft, tele og petroleum. Drivkreftene for endringene har vært svært forskjellige, og henger sammen med teknologiske forhold, utvikling av nasjonale og internasjonale regulatoriske rammebetingelser og behovet for å tilpasse de kommersielle strategiene til offentlig eide selskaper i de tre sektorene. Det grunnleggende spørsmålet vi har stilt, er om hel- eller delprivatiserte infrastrukturbedrifter har bedriftsøkonomiske incentiver til å ivareta samfunnets behov for sikkerhet og beredskap. Offentlig eierskap kan utgjøre et virkemiddel for å ivareta sikkerhetshensyn ved at myndighetene bruker sin residuale styringsrett som eiere og instruerer bedriftene. Samfunnsøkonomisk er det imidlertid ingen grunn til å bruke sterkere virkemidler for å ivareta sikkerhetshensyn enn det som er nødvendig.

I alle de tre sektorene vi har sett på, er det mulig å gi incentiver gjennom påbud og andre typer krav med hensyn til sikkerhet og beredskap. I stor grad finnes slike regler i dag gjennom et omfattende sett av lover og forskrifter.

I alle de tre sektorene finnes det incentiver til å utvide kapasiteten i infrastrukturen som også øker leveringssikkerheten. For eksempel vil knapphet på produksjonskapasitet i kraftsystemet reflekteres i høyere priser, som igjen kan gjøre det lønnsomt å investere i ny produksjon. I markedene for elektronisk kommunikasjon vil kvalitet og sikkerhet være en konkurranseparameter på linje med pris. Det kan imidlertid være avvik mellom samfunnets verdsetting av sikkerhetstiltak og investeringer i sikkerhetstiltak og ny kapasitet. Slike avvik kan i mange tilfeller fjernes gjennom særskilte tiltak (for eksempel ved at myndighetene kjøper inn nærmere definerte sikkerhetstjenester).

I elnettet (særlig sentralnettet) og gassinfrastrukturen på sokkelen er leveringssikkerheten i betydelig grad et kollektivt gode. Investeringene er preget av høy gjensidig avhengighet mellom prosjekter, vanskelig målbare nytteeffekter og mange involverte aktører med delvis motstridende interesser. Det er utfordrende å definere gode økonomiske og juridiske virkemidler som sikrer at de samfunnsøkonomisk riktige investeringene gjennomføres. Det taler for at offentlig eierskap kan være et viktig supplement til andre regulatoriske virkemidler. Norske myndigheter besitter på denne måten viktige virkemidler i form av eierskapet i Statnett og Gassco.

I telesektoren er denne typen sentralt eierskap mindre viktig. Det skyldes at de underliggende økonomiske og tekniske forholdene legger til rette for konkurranse mellom ulike infrastrukturer. Offentlig eierskap vil bare være et partielt virkemiddel som påvirker sikkerheten til de brukerne som er tilknyttet nett eid av offentlige aktører og trafikk hos andre infrastruktureiere som går via deler av Telenors nett. Det er derfor uansett behov for et velfungerende sikkerhetsregelverk som gjelder samtlige tilbydere av elektronisk kommunikasjon. Da blir eierskap mindre egnet som virkemiddel, også overfor offentlige aktører. For brukere med særlige behov er det mulig å etablere egne infrastrukturløsninger som i stor grad er uavhengige av andre nett for elektronisk kommunikasjon (jf. Forsvarets digitale nødnett).

I tabell 12.1 nedenfor oppsummerer vi noen av hovedtrekkene ved de tre sektorene.

Tabell 12.1 Økonomiske kjennetegn, drivkrefter og offentlig eierskap i kritisk infrastruktur

	Kraft	Tele	Petroleum
Økonomiske kjennetegn ved infrastrukturen	Elnettet et naturlig monopol	Stadig mindre innslag av naturlig monopol - mulig med konkurranse mellom infrastrukturer	Naturlig monopol i gasstransportsystemet
Drivkrefter for endringer	Mer effektiv ressursutnyttelse Mulig med konkurranse i produksjon og omsetning	Teknologiutvikling Framvekst av nye aktører Internasjonal konkurranse	Moden sokkel Utvikling av virkemidler som kan erstatte eierskap Press mot GFU fra EU
Offentlig eierskap (statlig eierandel)	Statnett SF (100%), Statkraft AS (100%), kommunale selskaper*	Telenor (54%), BaneTele (100%), nødnett (100%)	Statoil (71%), Petoro (100%), Gassco (100%), Norsk Hydro (43,8%)
Incentiver til å ivareta sikkerhet og beredskap	Incentiver til å unngå inntektstap ved bortfall av produksjon - knapphet på kapasitet reflekteres i markedet Utfordrende å lage gode mekanismer for å stimulere til riktige nettinvesteringer Omfattende sikkerhetsregelverk	Effektiv konkurranse mellom infrastrukturer - manglende sikkerhet kan gi inntektstap Også mulig å etablere egne nett for brukere med spesielle behov Omfattende sikkerhetsregelverk	Manglende sikkerhet kan gi betydelige inntektstap ved bortfall av produksjon Komplekse beslutninger om investeringer i gasstransportsystemet - behov for å koordinere mellom mange aktører Omfattende sikkerhetsregelverk
Rolle for offentlig eierskap	Ønskelig med offentlig eierskap til systemoperatør/sentralnett -mindre viktig på lavere nettnivåer og i produksjon Mulig å etablere virkemidler for å stimulere til høy leveringssikkerhet	Sikkerhet i offentlig eide nett påvirker bare de brukerne som er tilknyttet de offentlige nettene samt trafikk i andre nett som går via offentlige nett Nødvendig med sikkerhetsregelverk overfor ikke-offentlige aktører	Ønskelig med et offentlig engasjement i investeringer i gassinfrastruktur - dagens organisering med statseid systemoperatør gir et slikt virkemiddel Nødvendig med sikkerhetsregelverk overfor ikke-offentlige aktører

Kilde: *Statkraft eier andeler i flere kommunale kraftselskaper. Totalt er ca. 88 prosent av kraftproduksjonen i offentlig eie, ca. 85 prosent av det samlede elnettet.

Referanser

Bjørndalen, J. og G. Nese (2003): *Transportsystemet for naturgass.* SNF-arbeidsnotat nr. 66/03, Samfunns- og næringslivsforskning AS.

Bråten, J. (2001): *Det økonomiske samspillet mellom nett og kraftmarked. Sammendragsrapport.* Forskningsrapport 92/01, ECON Senter for økonomisk analyse.

Doorman, G., G. Kjølle, K. Uhlen, E.S. Huse og N. Flatabø (2004): *Vulnerability of the Nordic Power System. Main Report. Report to the Nordic Council of Ministers. T*R A5962, SINTEF Energiforskning.

DSB (2003): *Strømbrudd i Europa og Nord-Amerika august-september 2003.* DSB-rapport 2003-10-14. Direktoratet for samfunnssikkerhet og beredskap.

ECgroup (2004): *Evaluering av gjeldende KILE-ordning.* Prosjektrapport, august 2004.

ECON (2005): *Konsekvenser av langvarige strømutfall og høye kraftpriser i flere måneder.* Rapport 2005-014, ECON Analyse.

ECON og Oeconomica (2003): *Effektiv og bærekraftig konkurranse i tele- og mediemarkedene - hva skal til.* Rapport 2003-84, ECON Analyse og Oeconomica.

Fridheim, H., J. Hagen og S. Henriksen (2001): *En sårbar kraftforsyning - Sluttrapport etter BAS3.* FFI/Rapport-2001/02381. Forsvarets forskningsinstitutt.

Hagen, K.P. (2003): *Telepolitikk.* Notat, Samfunns- og næringslivsforskning AS.

Hagen, K.P. og O.D. Nafstad (2003): *Telepolitikk i Europa.* Rapport 27/03, Samfunns- og næringslivsforskning AS og ECON Analyse.

Innst. S. nr. 198 (2000-2001): *Innstilling fra energi- og miljøkomiteen om eierskap i Statoil og fremtidig forvaltning av SDØE.*

Innst. S. nr. 28 (1991-1992): *Innstilling fra energi- og industrikomiteen om omorganisering av Statkraft.*

Joskow, P. og J. Tirole (2005) "Merchant transmission investments», blir publisert i *Journal of Industrial Economics.*

Kon-Kraft (2003): *Aktivitetsprosjektet. Sluttrapport.* August 2003.

Laffont J og Tirole J. (1993): *A Theory of Incentives in Procurement and Regulation.* Cambridge, Massachusetts: MIT Press.

Nese, G. og K.P. Hagen (1998): *Pricing of natural gas transportation.* SNF-rapport nr. 64/98.

Nordel (2004): *Årsrapport.*

NOU 1985:9: *Energilovgivningen.* Olje- og energidepartementet.

NOU 1996:9: *Grønne skatter - en politikk for bedre miljø og høy sysselsetting.* Finansdepartementet.

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

NVE (2005a): *Aldersfordeling for komponenter i kraftsystemet. Levetid og behov for reinvesteringer.* Rapport nr. 8-2005, Norges vassdrags- og energidirektorat.

NVE (2005b): *Den økonomiske reguleringen av nettvirksomheten. Forslag til endring av forskrift om økonomisk og teknisk rapportering, m.v. Høringsdokument 1. juli 2005.* Dokument nr. 9 2005 Norges vassdrags- og energidirektorat.

Olje- og energidepartementet (2005): *Fakta 2005. Norsk petroleumsverksemd.*

Ot.prp. nr. 46 (2002-2003): *Om lov om endringer i lov 29. november 1996 nr. 72 om petroleumsvirksomhet.* Olje- og energidepartementet.

Ot.prp. nr. 58 (2002-2003): *Om lov om elektronisk kommunikasjon (ekomloven).* Samferdselsdepartementet.

Petroleumstilsynet (2004): *Årsberetning.*

Petroleumstilsynet (2005a): *Risikonivå på norsk sokkel 2004. Sammendragsrapport. Fase 5.*

Petroleumstilsynet (2005b): *Utvikling i risikonivå – norsk sokkel. Hendelsesdata for 1. halvår 2005.*

Post- og teletilsynet (2004): *Årsrapport.*

Post- og teletilsynet (2005): *Det norske telemarkedet 2004.*

Samdal, K., G. Kjølle, O. Kvitastein og B. Singh (2002): *Anbefaling til nye KILE-satser.* SINTEF Energiforskning og Samfunns- og næringlivsforskning (SNF).

Schweppe, Fred C., Caramanis, Michael C., Tabors, Richard D. og Bohn, Roger E. (1988): *Spot pricing of electricity.* Boston/Dordrecht/London: Kluwer Academic Publishers.

SINTEF (2003): *Etterspørsel etter nettinvesteringer - virkelighetsbeskrivelse.* AN 03.12.62, SINTEF Energiforskning.

St.meld. nr. 17 (2002-2003): *Om statlige tilsyn.* Arbeids- og administrasjonsdepartementet.

St.meld. nr. 38 (2003-2004): *Om petroleumsvirksomheten.* Olje- og energidepartementet.

St.meld. nr. 47 (2000-2001): *Telesikkerhet og beredskap i et telemarked med fri konkurranse.* Samferdselsdepartementet.

St.prp. nr. 1 (2001-2002): *For budsjetterminen 2002.* Olje- og energidepartementets fagproposisjon. Kapittel 6: Gjennomgang av Statnett SFs -organisering og oppgaver.

St.meld. nr. 1 (2005-2006): *Nasjonalbudsjettet 2006.* Finansdepartementet.

St.prp. nr. 100 (1990-1991): *Omorganisering av Statkraft.* Olje- og energidepartementet.

St.prp. nr. 36 (2000-2001): *Eierskap i Statoil og fremtidig forvaltning av SDØE.* Olje- og energidepartementet.

St.prp. nr. 58 (1998-1999): *Om sammenslåing av Telenor AS og Telia AB.* Samferdselsdepartementet.

St.prp. nr. 66 (1999-2000): *Om Telenor.* Samferdselsdepartementet.

Statnett (2005): *Nettutviklingsplan for sentralnettet 2005-2020.* Juni 2005, Statnett SF.

Tabell over ytre etater (direktorater og tilsyn) som har ansvar for sikkerhet som en del av sin virksomhet

Tabell 13.1 Tabell over ytre etater (direktorater og tilsyn) som har ansvar for sikkerhet som en del av sin virksomhet

Tilsyn	Hovedformål	Etatens egen målformulering	Lovhjemmel
Arbeidstilsynet	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser	Et fullt forsvarlig arbeidsmiljø for alle, med trygge tilsettingsforhold og meningsfylt arbeid for den enkelte	1947-04-26 nr 01 Lov om 1. og 17. mai som høgtidsdager 1973-03-09 nr 14 Lov om vern mot tobakkskader (T) 1973-12-14 nr 61 Lov om statsgaranti for lønnskrav ved konkurs m.v. 1977-02-04 nr 4 Lov om arbeidervern og arbeidsmiljø m.v. (T) 1988-04-29 nr 21 Lov om ferie 1988-05-06 nr 22 Lov om lønnsplikt under permittering
Bergvesenet	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser	Bærekraftig drift av mineralske ressurser, ivareta allmennhetens behov for sikkerhet, ivareta estetiske hensyn ved driften	1914-03-06 nr 5 Lov om erverv av kalksteinsforekomster (T) 1949-17-06 nr 3 Lov om erverv av kvartsforekomster (T) 1972-30-06 nr 70 Bergverksloven (T) 1974-31-05 nr 19 Konsesjonsloven (T)
Datatilsynet	Integritetsvern og ideelle verdier	Å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger (lovformålet)	1999-07-16 nr 66 Lov om Schengen informasjonssystem (SIS) (T) 2000-04-14 nr 31 Lov om behandling av personopplysninger (personopplysningsloven) (T) 2001-05-18 nr 24 Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) (T)
Direktoratet for naturforvaltning	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser	Bevare det biologiske mangfoldet (opprettholde naturlig produksjonsevne), og styrke allemannsretten (bruk av naturen til friluftsliv, opplæring og høsting)	1957-06-28 nr 16 Lov om friluftslivet (T) 1970-06-19 nr 63 Lov om naturvern (T) 1975-06-06 nr 31 Lov om utnytting av rettar og lunnende m.m. i statsallmenningane (fjellova) 1977-06-10 nr 82 Lov om motorferdsel i utmark og vassdrag (T) 1978-06-09 nr 50 Lov om kulturminner (T) 1981-04-13 nr 38 Lov om viltet (T) 1985-06-14 nr 77 Plan- og bygningsloven 1992-03-13 nr 6 Lov om vern mot forurensninger og om avfall (T) 1992-05-15 nr 47 Lov om laksefisk og innlandsfisk m.v. (T) 1993-04-02 nr 38 Lov om framstilling og bruk av genmodifiserte organismer (Genteknologiloven) (T) 1996-06-21 nr 38 Lov om statlig naturoppsyn (T)

Tabell 13.1 Tabell over ytre etater (direktorater og tilsyn) som har ansvar for sikkerhet som en del av sin virksomhet

Tilsyn	Hovedformål	Etatens egen målformulering	Lovhjemmel
Fiskeridirektoratet	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser. Fungerende markeder	å skape en bærekraftig og lønnsom fiskeri- og havbruksnæring og gjennom dette bevare hovedtrekkene i bosettingsmønsteret, sikre folk trygge og gode arbeidsplasser og øke næringens lønnsevne.	1920-02-09 nr 00 Traktat mellem Norge, Amerikas Forente Stater, Danmark, Frankrike, Italia, Japan, Nederlandene, Storbritannia og Irland og de britiske oversjøiske besiddelser og Sverige angående Spitsbergen (T) 1932-06-17 nr 23 Lov om kvalitetskontroll av landbruksvarer (T) 1959-05-28 nr 12 Lov om kvalitetskontroll med fisk og fiskevarer o.a. (T) 1962-06-08 nr 4 Lov om tiltak mot dyresjukdommer (T) 1966-06-17 nr 19 Lov om Norges fiskerigrense og om forbud mot at utlendinger driver fiske m.v. innenfor fiskerigrensen (T) 1973-03-23 nr 18 Lov om tilsyn med fôrvarer (T) 1976-12-17 nr 91 Lov om Norges økonomiske sone (T) 1983-06-03 nr 40 Lov om saltvannsfiske m.v. (T) 1985-06-14 nr 68 Lov om oppdrett av fisk, skalldyr m.v. (T) 1993-05-19 nr 3 Lov om tilsyn med næringsmidler (T) 1994-06-24-nr 34 Lov om registrering som kjøper i første hånd av råfisk m.v. (T) 1997-02-28 nr 19 Lov om Folketrygd 1997-06-13 nr 42 Lov om Kystvakten (kystvaktloven) (T) 1997-06-13 nr 54 Lov om tiltak mot sykdom hos fisk og andre akvatiske dyr (T) 1999-03-26 nr 15 Lov om retten til å delta i fiske og fangst (Deltakerloven) (T) 2000-12-21 nr 118 Lov om havbeite (T)

Tabell 13.1 Tabell over ytre etater (direktorater og tilsyn) som har ansvar for sikkerhet som en del av sin virksomhet

Tilsyn	Hovedformål	Etatens egen målformulering	Lovhjemmel
Kredittilsynet	Fungerende markeder	Betryggende soliditet, risikobevissthet, styring og kontroll i institusjonene under tilsyn. Å avdekke forhold som truer stabiliteten i det finansielle system og ha beredskap for håndtering av problemer i finanssektoren. Gode etiske normer og ordnede forhold blant aktørene i finansmarkedet. Rammebetingelser som gir velfungerende markeder både for tilsynsenhetene og deres brukere.	1953-07-03 nr 2 Lov om sjøtrygdelag (T) 1956-07-12 nr 1 Lov om tilsynet for kredittinstitusjoner, forsikringsselskaper og verdipapirhandel m.v. (Kredittilsynsloven) (T) 1961-05-24 nr 1 Lov om sparebanker (T) 1961-05-24 nr 2 Lov om forretningsbanker (T) 1981-06-12 nr 52 Lov om verdipapirfond (T) 1985-06-14 nr 62 Lov om verdipapirsentral (T) 1988-05-13 nr 26 Lov om inkassovirksomhet og annen inndriving av forfalte pengekrav (inkassoloven) (T) 1988-06-10 nr 39 Lov om forsikringsvirksomhet (T) 1988-06-10 nr 40 Lov om finansieringsvirksomhet og finansinstitusjoner (T) 1989-06-16 nr 53 Lov om eiendomsmegling (T) 1989-06-16 nr 69 Lov om forsikringsavtaler (T) 1993-06-18 nr 109 Lov om autorisasjon av regnskapsførere (T) 1996-12-06 nr 75 Lov om sikringsordninger for banker og offentlig administrasjon m.v. av finansinstitusjoner (T) 1997-06-19 nr 79 Lov om verdipapirhandel (T) 1998-07-17 nr 56 Lov om årsregnskap m.v. (regnskapsloven) (T) 1999-01-15 nr 2 Lov om revisjon og revisorer (revisorloven) (T) 1999-06-25 nr 46 Lov om finansavtaler og finansoppdrag (finansavtaleloven) 1999-12-17 nr 95 Lov om betalingssystemer m.v. (T) 2000-03-24 nr 16 Lov om foretakspensjon (T) 2000-11-17 nr 80 Lov om børsvirksomhet m.m. (børsloven) (T) 2000-11-24 nr 81 Lov om innskuddspensjon (T)
Kystdirektoratet	Infrastruktur (inklusive sikkerhet og i noen utstrekning tredjepersons adferd i den sammenheng)	Etat for kystforvaltning og samferdsel. Ivaretar noen sikkerhetsregler (tilsyn) overfor brukere av de aktuelle farvann.	1984-06-08 nr 51 Lov om havner og farvann mv (T) 1989-06-15 nr 59 Lov om lostjenesten m.v. (T) 1985-06-14 nr 77 Plan og bygningsloven
Luftfartstilsynet	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser	Bidra til økt sikkerhet i luftfarten	1903-06-09 nr 7 Lov om statskontroll med skibes sjødyktighet (bistand) 1977-02-04 nr 4 Lov om arbeidervern og arbeidsmiljø (T) 1993-06-11 nr 101 Lov om luftfart (T) 1999-11-29 nr 72 Lov om petroleumsvirksomhet (bistand)
Nasjonal sikkerhetsmyndighet	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser	Å motvirke trusler mot rikets selvstendighet og sikkerhet	1998-03-20 nr 10 Lov om forebyggende sikkerhetstjeneste (T)

Tabell 13.1 Tabell over ytre etater (direktorater og tilsyn) som har ansvar for sikkerhet som en del av sin virksomhet

Tilsyn	Hovedformål	Etatens egen målformulering	Lovhjemmel
Norges vassdrags- og energidirektorat	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser Fungerende infrastruktur (energi) Fungerende markeder (energiomsetning)	Fremme verdiskaping, miljø og sikkerhet gjennom en helhetlig forvaltning av vann- og energiressurser. Herunder: ivareta miljø- og brukerinteresser, forebygge vassdragsulykker, ivareta sikkerhet og beredskap i kraftforsyningen, fremme effektiv og miljømessig akseptabel energiproduksjon, fremme effektiv og sikker overføring og omsetning av energi og effektiv energibruk.	1917-14-12 nr 16 Lov om erverv av vannfall, bergverk og annen fast eiendom m.v. (T) 1917-12-14 nr 17 Lov om vassdragsreguleringer (T) 1959-10-23 nr 3 Lov om oreigning av fast eigedom 1976-06-11 nr 79 Lov om kontroll med produkter og forbrukertjenester (produktkontrolloven) 1981-12-18 nr 90 Lov om merking av forbruksvarer m.v. 1985-06-14 nr 77 Plan- og bygningslov 1993-11-06 nr 98 Lov om produksjon, omforming, overføring, omsetning og fordeling av energi m.m. (Energiloven) (T) 2000-11-24 nr 82 Lov om vassdrag og grunnvann (vannressursloven) (T)
Næringslivets sikkerhetsorganisasjon	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser	organiserer og kontrollerer egenbeskyttelsen (industrivern) ved virksomheter som omfattes av «industrivernplikt» Råd om hvordan man beskytter virksomheten mot kriminelle handlinger	1953-07-17 nr 9 Lov om sivilforsvaret (T)
Oljedirektoratet*	Bidra til å skape størst mulig verdier for samfunnet fra olje- og gassvirksomheten gjennom en forsvarlig ressursforvaltning med forankring i sikkerhet, beredskap og ytre miljø.	Bidra til kostnadseffektiv leting Bidra til kostnadseffektivt uttak av petroleum, utnyttelse av infrastruktur og samordning på tvers av utvinningstillatelser Se til at næringen minimerer utslipp som belaster det ytre miljøet Nasjonalt ansvar for at data og informasjon fra petroleumsvirksomheten er tilgjengelig OD skal til enhver tid ha oversikt over petroleumsressursene på norsk sokkel. Beredskapsmessig ansvar for leveringssikkerhet Innkreving av CO2-avgift og andre avgifter Måleteknisk tilsyn OD har myndighet til å fastsette forskrifter om ressursforvaltning.	1996-11-29 nr 72 Lov om petroleumsvirksomhet. 1963-06-21 nr 12 Lov om vitenskapelig utforskning og undersøkelser etter og utnyttelse av andre undersjøiske naturforekomster enn petroleumsforekomster. 1990-12-21 nr 72 Lov om avgift på utslipp av CO2 i petroleumsvlrksomhet på kontinentalsokkelen.

Tabell 13.1 Tabell over ytre etater (direktorater og tilsyn) som har ansvar for sikkerhet som en del av sin virksomhet

Tilsyn	Hovedformål	Etatens egen målformulering	Lovhjemmel
Petroleumstilsynet	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser	Petroleumstilsynet skal legge premisser for og følge opp at aktørene i petroleumsvirksomheten holder et høyt nivå for helse, miljø, sikkerhet og beredskap og gjennom dette også bidra til å skape størst mulig verdier for samfunnet. *	1996-11-29 nr 72 Lov om petroleumsvirksomhet 2005-06-17 nr 62 Lov om arbeidsmiljø, arbeidstid og stillingsvern mv (arbeidsmiljøloven) 1929-05-24 nr 4 Lov om tilsyn med elektriske anlegg og elektrisk utstyr 2002-06-14 nr 20 Lov om vern mot brann, eksplosjon og ulykker med farlig stoff og om brannvesenets redningsoppgaver 1973-03-09 nr 14 Lov om vern mot tobakkskader 1925-07-17 nr 11 Lov om Svalbard
Park- og tivolitilsynet (Det Norske Veritas)	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser	Skal arbeide for at innretninger som omfattes av Tivoliloven oppføres, drives og vedlikeholdes på en måte som ivaretar sikkerheten for passasjerer, driftspersonell og tredjeperson	1991-06-07 nr 24 Lov om godkjenning og drift av innretninger til bruk i tivoli og fornøyelsesparker (T)
Post- og teletilsynet	Fungerende samferdsel, kommunikasjon og energiforsyning Fungerende markeder	Bidra til å sikre alle tilgang til post- og teletjenester av høy kvalitet til lavest mulig pris	1995-06-23 nr 39 Lov om telekommunikasjon (teleloven) (T) 1996-11-29 nr 73 Lov om formidling av landsdekkende postsendinger (postloven) (T) 1999-06-25 nr 50 Lov om standarder ved overføring av fjernsynssignaler (T) 2001-06-15 nr 81 Lov om elektronisk signatur (T)
Sjøfartsdirektoratet	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser	Oppnå høy sikkerhet for liv, helse, fartøy og miljø i en effektiv og velrennomert maritim virksomhet	1903-06-09 nr 7 Lov om Statskontrol med Skibes Sjødygtighed m.v. (T) 1964-06-19 nr 20 Lov om måling av fartøyer (T) 1966-06-17 nr 2 Lov om luftputefartøyer (T) 1971-06-18 nr 90 Lov om mønstring av arbeidstakere på skip m.v. (T) 1975-05-30 nr 18 Lov om sjømenn (T) 1977-06-03 nr 50 Lov om arbeidstiden og hviletiden på skip (T) 1979-06-11 nr 79 Lov om kontroll med produkter og forbrukertjenester (produktkontrolloven) (T) 1981-06-05 nr 42 Lov om sertifikatpliktige stillinger på norske skip, borefartøy og andre flyttbare innretninger i sjøen (Sertifiseringsloven) (T) 1982-12-17 nr 84 Lov om sikre containere 1987-06-12 nr 48 Lov om norsk internasjonalt skipsregister (T) 1994-06-24 nr 39 Lov om sjøfarten (sjøloven) (T) 1998-06-26 nr 47 Lov om fritids- og småbåter (T)
Statens bygningstekniske etat	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser	Sentral myndighet for bygningsteknisk regelverk. Driver en frivillig ordning for sentral godkjenning av foretak etter plan- og bygningsloven. Tilsynsmyndighet for regler om dokumentasjon av byggevarers egenskaper	1985-06-14 nr 77 Plan- og bygningslov (T) 1991-06-07 nr 24 Lov om godkjenning og drift av innretninger til bruk i tivoli og fornøyelsesparker (T)

Tabell 13.1 Tabell over ytre etater (direktorater og tilsyn) som har ansvar for sikkerhet som en del av sin virksomhet

Tilsyn	Hovedformål	Etatens egen målformulering	Lovhjemmel
Statens forurensnings-tilsyn	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser	At forurensning, skadelige produkter og avfall ikke skal føre til helseskade, gå ut over trivselen eller skade naturens evne til produksjon og fornyelse	1974-05-31-17 Lov om kommunale vass- og kloakkavgifter 1976-11-6 nr 79 Lov om kontroll med produkter og forbrukertjenester (produktkontrolloven) (T) 1981-13-6 nr 6 Lov om vern mot forurensninger og om avfall (forurensningsloven) (T) 2001-06-15 nr 79 Lov om miljøvern på Svalbard (Svalbardmiljøloven) (T)

Tabell 13.1 Tabell over ytre etater (direktorater og tilsyn) som har ansvar for sikkerhet som en del av sin virksomhet

Tilsyn	Hovedformål	Etatens egen målformulering	Lovhjemmel
Statens helsetilsyn	Trygge helsetjenester av tilstrekkelig omfang for hele befolkningen	Bidra til at befolkningens behov for helsetjenester blir ivaretatt, at helsetjenestene drives på en faglig forsvarlig måte og slik at svikt i tjenesteytingen forebygges samt at helsetjenesteressursene brukes på en forsvarlig og effektiv måte.	1936-06-19 nr 9 Lov om innskrenkning i adgangen for den som ikke er norsk læge eller tannlæge, til å ta syke i kur (kvaksalverloven) (T) 1973-02-09 nr 6 Lov om transplantasjon, sykehusobduksjon og avgivelse av lik m.m. (transplantasjonsloven) (T) 1975-06-13 nr 50 Lov om svangerskapsavbrudd (abortloven) (T) 1977-06-03 nr 57 Lov om sterilisering (steriliseringsloven) (T) 1982-11-19 nr 66 Lov om helsetjenesten i kommunene (kommunehelsetjenesteloven) (T) 1982-11-19 nr 68 Lov om planlegging av helse- og sosialtjenesten i kommunene (T) 1983-06-03 nr 54 Lov om tannhelsetjenesten (tannhelsetjenesteloven) (T) 1984-03-30 nr 15 Lov om statlig tilsyn med helsetjenesten (T) 1988-06-10 nr 48 Midlertidig lov om avvikling av institusjoner og kontrakter om privatpleie under det fylkeskommunale helsevern for psykisk utviklingshemmede (T) 1991-12-13 nr 81 Lov om sosiale tjenester m.v. (sosialtjenesteloven) (T) 1992-12-04 nr 132 Lov om legemidler m.v. (legemiddelloven) (T) 1994-08-05 nr 55 Lov om vern mot smittsomme sykdommer (smittevernloven) (T) 1994-08-05 nr 56 Lov om medisinsk bruk av bioteknologi (bioteknologiloven) (T) 1995-01-12 nr 6 Lov om medisinsk utstyr (T) 1995-12-15 nr 74 Lov om forbud mot kjønnslemlestelse (T) 1996-11-29 nr 72 Lov om petroleumsvirksomhet (petroleumsloven) (T) 1999-07-02 nr 61 Lov om spesialisthelsetjenesten m.m. (spesialisthelsetjenesteloven) (T) 1999-07-02 nr 62 Lov om etablering og gjennomføring av psykisk helsevern (psykisk helsevernloven) (T) 1999-07-02 nr 63 Lov om pasientrettigheter (pasientrettighetsloven) (T) 1999-07-02 nr 64 Lov om helsepersonell m.v. (helsepersonelloven) (T) 2000-06-02 nr 39 Lov om apotek (apotekloven) (T) 2000.06.23 nr 56 Lov om helsemessig og sosial beredskap (T) 2001.05.18 nr 24 Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) (T) 2001.06.15 nr 93 Lov om helseforetak (helseforetaksloven) (T)

Tabell 13.1 Tabell over ytre etater (direktorater og tilsyn) som har ansvar for sikkerhet som en del av sin virksomhet

Tilsyn	Hovedformål	Etatens egen målformulering	Lovhjemmel
Statens jernbanetilsyn	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser	Statens jernbanetilsyn skal bidra til at sikkerheten ved transport med tog og bane kontinuerlig forbedres. Sikkerheten ved jernbane i Norge skal minst være på nivå med andre europeiske land	1993-06-11 nr 100 Lov om anlegg og drift av jernbane, herunder sporvei, tunnelbane og forstadsbane m.m. (jernbaneloven) (T)
Statens legemiddelverk	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser	Bidra til å sikre befolkningen tilgang til nødvendige legemidler uavhengig av bosted, til lavest mulig pris, og ved langvarig behandling; uavhengig av betalingsevne. Bidra til riktig legemiddelbruk	1992-12-04 nr 132 Lov om legemidler m.v. (legemiddelloven) (T) 2000-06-02 nr 39 Lov om apotek (apotekloven) (T)
Statens strålevern	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser	Godt strålevern for samfunnet, den enkelte og miljøet Forsvarlig strålebruk og atomsikkerhet God beredskap Tilsyn med all bruk av strålekilder i medisin, industri og forskning samt atomanlegg Overvåking av radioaktivitetens vandring i biosfæren frem til mennesket Ivareta atomulykkesberedskap Begrense eksponeringen fra naturlige og kunstige strålekilder i miljøet	1972-12-05 nr 28 Lov om atomenergivirksomhet (T) 2000-05-12 nr 36 Lov om strålevern og bruk av stråling (T)
Statens vegvesen	Fungerende infrastruktur, men også sikkerhet for liv, helse, ytre miljø og materielle verdier/ressurser	Ansvar for planlegging, bygging, drift og vedlikehold av riks- og fylkesvegnettet og ansvar for riksvegferjetilbudet. Tilsyn med kjøretøy og trafikanter. Utarbeider bestemmelser for vegutforming, vegtrafikk, trafikantopplæring og kjøretøy. Godkjenningsmyndighet for førerrett etter vegtrafikklovgivningen.	1961-02-03 Lov om ansvar for skade som motorvogner gjer 1963-06-21 nr 23 Vegloven 1965-06-18 nr 4 Lov om vegtrafikk (T) 1973-02-23 nr 11 Lov om godkjenning av køyretøyverkstader (T)
Taubanetilsynet (Det Norske Veritas)	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser	Sikre at taubaner, kabelbaner, skitrekk, etc. bygges og drives på en slik måte at de ivaretar hensynet til tilfredsstillende trafikksikkerhet for passasjerer, driftspersonell og tredjeperson	1912-06-14 nr 1 Lov om anlæg av taugbaner og løipestrenger (T) 1993-11-06 nr 100 Lov om anlegg og drift av jernbane, herunder sporvei, tunnelbane og forstadsbane m.m. (jernbaneloven) (T)
Direktorat for beredskap og samfunnssikkerhet*	Sikkerhet for liv, helse, ytre miljø og materielle verdier/ ressurser	Skal ha oversikt over risiko og sårbarhet i samfunnet. Skal være pådriver i arbeidet med å forebygge ulykker, kriser og andre uønskede hendelser. Skal sørge for god beredskap og effektiv ulykkes- og krisehåndtering. *	Lov om vern mot brann, eksplosjon og ulykker med farlig stoff og om brannvesenets redningsoppgaver (brann- og eksplosjonsvernloven) Lov om kontroll med produkter og forbrukertjenester (produktkontrolloven) Lov om tilsyn med elektriske anlegg og elektrisk utstyr Lov om sivilforsvaret *

Tabell 13.1 Tabell over ytre etater (direktorater og tilsyn) som har ansvar for sikkerhet som en del av sin virksomhet

Tilsyn	Hovedformål	Etatens egen målformulering	Lovhjemmel
Mattilsynet*	En matforvaltning som bidrar til å sikre god mattrygghet og en god dyre- og plantehelse, og som fremmer redelig frambud og kvalitet på matvarer	Mattilsynet skal arbeide for å oppnå: Helsemessig trygg mat Friske planter, fisk og dyr Etisk forsvarlig hold av fisk og dyr Miljøvennlig produksjon God kvalitet samt redelig produksjon og omsetning Verdiskaping på matområdet En framtidsrettet og effektiv organisasjon*	Lov om tilsyn med kosmetikk og kroppspleieprodukter mv. 21.12.2005 nr. 126 Lov om matproduksjon og mattrygghet mv. (matloven). 19.12.2003 nr. 124 Lov om veterinærer og annet dyrehelsepersonell 15.06.2001 nr. 75 Lov om planteforedlerrett 12.03.1993 nr. 32 Lov om husdyravl 04.12.1992 nr. 130 Lov om dyrevern 20.12.1974 nr. 73 *

* Informasjon er hentet fra etatens hjemmeside eller ved direkte kontakt med etaten.

Kilde: St.meld. nr. 17 (2002-2003) *Om statlige tilsyn*. Vedlegg. Tilsynsorganer i Norge – faktabeskrivelser. Informasjon som er hentet fra andre steder er merket med*. Denne informasjonen er i hovedsak hentet fra hjemmesider og ved direkte kontakt med direktorat/tilsyn. Stortingsmelding 17 (2002-2003) finnes på odin.dep.no/fad/norsk/dok/regpubl/stmeld/002001-040025/ved001-bu.html