NOU Norges offentlige utredninger 2015: 13

Digital sårbarhet – sikkert samfunn

Beskytte enkeltmennesker og samfunn i en digitalisert verden

Norges offentlige utredninger
2015

Seriens redaksjon:
Departementenes sikkerhets- og serviceorganisasjon
Informasjonsforvaltning

---

1. Produktivitet – grunnlag for vekst og velferd
   Finansdepartementet
2. Å høre til
   Kunnskapsdepartementet
3. Advokaten i samfunnet
   Justis- og beredskapsdepartementet
4. Tap av norsk statsborgerskap
   Barne-, likestillings- og inkluderingsdepartementet
5. Pensjonslovene og folketrygdreformen IV
   Finansdepartementet
6. Grunnlaget for inntektsoppgjørene 2015
   Arbeids- og sosialdepartementet
7. Assimilering og motstand
   Kommunal- og moderniseringsdepartementet
8. Fremtidens skole
   Kunnskapsdepartementet
9. Finanspolitikk i en oljeøkonomi
   Finansdepartementet
10. Lov om regnskapsplikt
    Finansdepartementet
11. Med åpne kort
    Helse- og omsorgsdepartementet
12. Ny lovgivning om tiltak mot hvitvasking og terrorfinansiering
    Finansdepartementet
13. Digital sårbarhet – sikkert samfunn
    Justis- og beredskapsdepartementet

Omslagsillustrasjon: Colourbox

NOU Norges offentlige utredninger 2015: 13

Digital sårbarhet – sikkert samfunn

Beskytte enkeltmennesker og samfunn i en digitalisert verden

Utredning fra et utvalg oppnevnt ved kongelig resolusjon 20. juni 2014.
Avgitt til Justis- og beredskapsdepartementet 30. november 2015.

Departementenes sikkerhets- og serviceorganisasjon
Informasjonsforvaltning

Oslo 2015

ISSN 0333-2306
ISBN 978-82-583-1249-6

07 Aurskog AS

Til Justis- og beredskapsdepartementet

Utvalget om digitale sårbarheter ble oppnevnt ved kongelig resolusjon 20. juni 2014. Utvalget gir med dette sin utredning.

Oslo 30. november 2015

Olav Lysne
Leder

Kristine Beitland

Janne Hagen

Åke Holmgren

Einar Lunde

Kristian Gjøsteen

Fredrik Manne

Eva Jarbekk

Sofie Nystrøm

Roger Kolbotn
Sekretariatsleder

Lene Bogen Kaland

Ingunn Moholt

Håkon Hermansson

André Nordbø

Ragnhild Castberg

Innhold

Del I **Innledning** ... 13

1 **Sammendrag** ... 15

2 **Mandat, utvalgets sammensetning og arbeid** ... 18
2.1 Mandat ... 18
2.2 Mandatforståelse ... 19
2.3 Sammensetning og utvalgets arbeid ... 20
2.4 Struktur og innhold ... 21

Del II **Situasjonsbeskrivelse** ... 23

3 **Rettsstatsprinsipper og grunnleggende samfunnsverdier** 25
3.1 Digital ivaretakelse av grunnleggende samfunnsverdier ... 26
3.2 Menneskerettigheter ... 26
3.2.1 Retten til liv ... 27
3.2.2 Retten til privatliv ... 27
3.2.3 Rett til vern om personlige opplysninger ... 27
3.2.4 Retten til frie ytringer ... 28
3.2.5 Forsamlingsfrihet ... 29
3.3 Menneskerettighetsbrudd ... 29

4 **Hva er digitale sårbarheter?** ... 31
4.1 Sårbarhetsbegrepet ... 31
4.2 Verdivurdering ... 31
4.3 Trussel og fare ... 32
4.4 Risikovurdering ... 32

5 **Sikring av IKT og digital informasjon** ... 34
5.1 Hva er IKT-sikkerhet? ... 34
5.2 Motsetninger mellom sikkerhetsmål ... 35
5.3 Sikkerhetsnivå og risikoaksept ... 35
5.4 Noen sentrale IKT-sikkerhetstiltak ... 36
5.4.1 Menneskelige og organisatoriske sikkerhetstiltak ... 36
5.4.2 Preventive tekniske sikkerhetstiltak ... 36
5.4.3 Overvåking ... 38
5.5 Utfordringer knyttet til programvareutvikling ... 39
5.6 Teknologiarven ... 40
5.7 Sikkerhet i prosesskontrollsystemer ... 41
5.8 Elektronisk identifisering ... 41

6 **Trender som påvirker sårbarhetsbildet** ... 43
6.1 Digitaliseringen av samfunnet og sårbarhetsbildet ... 43
6.2 Informasjonsteknikk og informasjonshåndtering ... 44
6.2.1 Økt regnekraft, store data og stordataanalyse ... 44
6.2.2 Tingenes Internett ... 46
6.2.3 Kroppsnær teknologi ... 47
6.3 Automatiseringen av hverdagen og arbeidslivet ... 47
6.3.1 Additiv produksjon – 3D-printere .. 48
6.3.2 Ubemannede luftfartøy – droner .. 48
6.4 Nye digitale tjenester og endringer i adferd ... 49
6.4.1 Skytjenester ... 49
6.4.2 Sosiale medier ... 49
6.4.3 Bruk av privateid datautstyr i jobbsammenheng ... 49
6.5 IKT-sikkerhet på den strategiske agendaen ... 50
6.6 Trender i sikkerhetsteknologien .. 50

7 **Utilsiktede og tilsiktede IKT-hendelser** ... 52
7.1 Utilsiktede IKT-hendelser ... 52
7.1.1 Naturhendelser ... 52
7.1.2 Svikt ... 53
7.2 Tilsiktede IKT-hendelser ... 54
7.2.1 IKT-kriminalitet ... 55
7.2.2 Sabotasje, spionasje og terror ... 57

8 **Organisering av roller og ansvar** ... 61
8.1 Overordnede mål og prinsipper for IKT-sikkerhetsarbeidet ... 61
8.2 Sentrale myndighetsaktører med særlig ansvar for oppfølging av IKT-sikkerhet ... 63
8.3 Øvrige aktører ... 66
8.4 Sentrale koordineringsarenaer for IKT-sikkerhet ... 67

9 **IKT-sikkerhetsarbeid i andre land** ... 69
9.1 Generelle betraktninger ... 69
9.2 Nasjonale myndigheters organisering og ansvar ... 70
9.3 Nasjonale strategier ... 71
9.4 Hendelseshåndtering ... 71

9.5 Informasjonsdeling og offentlig–privat samarbeid 72
9.6 Forskning og utvikling 73
9.7 Regulering 73
9.8 Personvern 74

10 Folkerett og internasjonalt samarbeid 75
10.1 Folkerettslige rammer for grenseoverskridende informasjonsinnhenting 75
10.2 Alminnelige folkerettslige skranker for grenseoverskridende informasjonsinnhenting 76
10.2.1 Wien-konvensjonen om diplomatisk samkvem 77
10.3 Menneskerettslige skranker for informasjonsinnhenting 77
10.3.1 Den europeiske menneskerettskonvensjonen art. 8 og FNs konvensjon om sivile og politiske rettigheter art. 17 77
10.3.2 I hvilken grad kommer menneskerettighetene til anvendelse ved grenseoverskridende overvåking og informasjonsinnhenting, jf. EMK art. 1 og SP art. 2 nr. 1? 80
10.3.3 FN-resolusjonene om retten til et privatliv i den digitale tidsalder 82
10.4 Europarådets personvernkonvensjon 83
10.5 Europarådets konvensjon nr. 185 om datakriminalitet 83
10.6 Norges forpliktelser som følger av EØS-avtalen og øvrige avtaler med EU 84
10.6.1 EUs regelverk for nettverks- og informasjonssikkerhet (NIS-direktivet) 84
10.6.2 Ekom 85
10.6.3 Personverndirektivet 86
10.6.4 Politisamarbeid 87
10.7 EUs strategier, programmer og fora 88
10.7.1 EUs strategi for sikkerhet i det digitale rom 88
10.7.2 ENISA 88
10.7.3 Digital agenda 88
10.7.4 EU-fora for personvern 89
10.8 IKT-arbeid i OECD 89
10.8.1 OECDs retningslinjer for «cybersecurity» 90
10.8.2 OECDs retningslinjer for personvern 91
10.9 FNs arbeid i fora knyttet til det digitale rom 91
10.10 NATO 93
10.11 Interpol 93
10.12 Andre multilaterale samarbeidsfora 93

Del III Sårbarheter i kritiske samfunnsfunksjoner 95

11 Elektronisk kommunikasjon ... 97
11.1 Ekominfrastruktur 97
11.1.1 Robusthet i infrastrukturen 99
11.1.2 Kjerne- og transportnett 99
11.1.3 Aksessnett 100
11.1.4 Mobilnett 100
11.1.5 Satellittkommunikasjon 100
11.1.6 Kommunikasjonsinfrastruktur på norsk sokkel 100
11.1.7 Nødnett 101
11.1.8 Internett 101
11.2 Roller og ansvar 102
11.3 Hjemmelsgrunnlag og tilsynsvirksomhet 103
11.4 Beredskap og hendelseshåndtering 105
11.4.1 Øvelsesfunn 105
11.5 Sårbarheter i ekominfrastruktur .. 106
11.5.1 Verdikjeder i ekom 106
11.5.2 Samfunnets avhengighet av ekominfrastruktur 107
11.5.3 Avhengigheten av kraftforsyning .. 110
11.5.4 Sårbarheter knyttet til drift og styring 111
11.5.5 Driftsmodeller under press fra den globale konkurransen 112
11.5.6 Nasjonal autonomi og personvernutfordringer 112
11.6 Fremtidige problemstillinger og trender 114
11.7 Vurderinger og tiltak 114
11.7.1 Redusere kritikaliteten av Telenors kjerneinfrastruktur 115
11.7.2 Sikre mangfold blant leverandørene til infrastrukturen .. 115
11.7.3 Opprette en CSIRT i ekomsektoren i regi av Nkom 115
11.7.4 Aktiv myndighetsutøvelse fra Samferdselsdepartementet og Nasjonal kommunikasjonsmyndighet 116
11.7.5 Etablere tiltak for å regulere utlevering av trafikkdata til politiet 116

12 Satellittbaserte tjenester 118
12.1 Romrelatert infrastruktur 118
12.2 Roller og ansvar 120
12.3 Hjemmelsgrunnlag og regulering 122
12.4 Sårbarheter i satellittbaserte tjenester 122
12.4.1 Trusler mot romrelatert infrastruktur 123
12.4.2 Samfunnets avhengighet av satellittbaserte tjenester 123
12.4.3 Romvær og romskrot 124
12.4.4 Menneskelig svikt 125
12.4.5 Restsårbarhet og redundans 125
12.4.6 Bevissthet rundt sårbarhet og risiko 126
12.4.7 Sårbarheter knyttet til verdikjeder 126
12.5 Vurderinger og tiltak 127
12.5.1 Tydeliggjøre myndighetsansvar for norsk romvirksomhet 127

13 Energiforsyning 129
13.1 Kraftsystemet 129
13.2 Roller og ansvar 130
13.3 Hjemmelsgrunnlag, konsesjoner og tilsynsvirksomhet 132
13.3.1 Konsesjoner 133
13.3.2 Tilsyn 133
13.4 Beredskap og hendelses-håndtering 134
13.5 Digitale sårbarheter i kraft-forsyningen 136
13.5.1 Verdikjeden i norsk kraftforsyning 136
13.5.2 Sårbarheter i driftskontroll-systemer 137
13.5.3 Sårbarheter i tilknytning til smarte nett 139
13.5.4 Avhengighet av ekom og satellitt-baserte tjenester 141
13.6 Fremtidige problemstillinger og trender 142
13.7 Vurderinger og tiltak 143
13.7.1 Styrke tilsyn og veiledning i IKT-sikkerhet 143
13.7.2 Stimulere til større og mer ressurssterke fagmiljøer innen IKT-sikkerhet 144
13.7.3 Bygge et sterkt operativt fagmiljø for IKT-hendelseshåndtering 144
13.7.4 Vurdere de sikkerhetsmessige forhold ved å behandle og lagre kraftsensitiv informasjon i utlandet 144
13.7.5 Gjennomføre risiko- og sårbarhetsanalyse for utvidet bruk av AMS 145
13.7.6 Utarbeide en oppdatert analyse av kraftforsyningens avhengighet av ekom 145

14 Olje og gass 146
14.1 Olje- og gassinfrastruktur 146
14.2 Roller og ansvar 146
14.3 Hjemmelsgrunnlag og tilsyns-virksomhet 148
14.4 Beredskap og hendelses-håndtering 148
14.5 Digitale sårbarheter i olje- og gassektoren 150
14.5.1 Verdikjede 150
14.5.2 Letevirksomhet 150
14.5.3 Feltutvikling 151
14.5.4 Produksjon 152
14.5.5 Transport 153
14.5.6 Avhengigheter av andre samfunnsfunksjoner 153
14.5.7 Kompetanse og sikkerhetskultur .. 155
14.6 Fremtidige problemstillinger og trender 156
14.7 Vurderinger og tiltak 156
14.7.1 Overføre sikkerhetstradisjonen innen HMS til det digitale området 157
14.7.2 Verdivurdere sektorens anlegg og IKT-systemer, og etablere regelverk for digitale sårbarheter .. 157
14.7.3 Tydeliggjøre rolle og kapasitet hos Petroleumstilsynet 157
14.7.4 Vurdere tilknytning til respons-miljø for IKT-hendelser 158

15 Vannforsyning 159
15.1 Vann- og avløpsinfrastruktur 159
15.2 Roller og ansvar 160
15.3 Hjemmelsgrunnlag og tilsyns-virksomhet 161
15.4 Beredskap og krisehåndtering 161
15.5 Digitale sårbarheter i vann-forsyningen 161
15.5.1 Bruk av driftskontrollsystemer innen vannforsyning 161
15.5.2 Vannforsyningens avhengighet av kraft og ekom 164
15.5.3 Organisatoriske forhold og kompetanse 164
15.6 Vurderinger og tiltak 166
15.6.1 Øke IKT-sikkerhetskompetansen i norske vannverk 166
15.6.2 Styrke tilsyn og veiledning i IKT-sikkerhet 166

15.6.3 Bedre systemer for hendelses-håndtering ... 167
15.6.4 Gjennomføre risiko- og sårbarhetsanalyser før en eventuell innføring av smarte vannmålere ... 167

16 Finansielle tjenester ... 168
16.1 Finansiell infrastruktur ... 168
16.2 Roller og ansvar ... 169
16.3 Hjemmelsgrunnlag og tilsyns-virksomhet ... 171
16.4 Beredskap og hendelses-håndtering ... 172
16.5 Digitale sårbarheter i finans-sektoren ... 174
16.5.1 Formidle kapital nasjonalt og internasjonalt ... 174
16.5.2 Sikre befolkningen tilgang til betalingsløsninger ... 175
16.5.3 Sikre betalinger og andre finansielle transaksjoner ... 176
16.5.4 Sikker og stabil drift av finansielle registre ... 177
16.5.5 Kommunisere med befolkningen om kritiske hendelser ... 178
16.5.6 Særskilte personvernutfordringer 179
16.5.7 Avhengighet av kraft og elektronisk kommunikasjon ... 180
16.6 Fremtidige problemstillinger og trender ... 180
16.7 Vurderinger og tiltak ... 182
16.7.1 Styrke innsatsen på vurdering av fremtidige betalingstjenester ... 182
16.7.2 Videreføre tverrfaglig samarbeid for god beredskapsevne og håndtering av alvorlige tilsiktede IKT-hendelser ... 182
16.7.3 Analysere sårbarhets-konsekvensene som følge av utkontraktering ut av landet ... 183
16.7.4 Videreføre og styrke engasjementet for å påvirke internasjonal regulering av IKT-sikkerhetsmekanismer ... 183
16.7.5 Styrke beredskapstiltak for utviklingen mot det kontantløse samfunnet ... 183

17 Helse og omsorg ... 185
17.1 Infrastruktur ... 185
17.2 Roller og ansvar ... 186
17.3 Hjemmelsgrunnlag og tilsyns-virksomhet ... 188
17.4 Beredskap og hendelses-håndtering ... 189
17.5 Digitale sårbarheter i helse-sektoren ... 191
17.5.1 Avhengighet av elektronisk kommunikasjon og øvrige infrastrukturer ... 192
17.5.2 Infrastruktur og tjenester ... 193
17.5.3 Styring og samhandling ... 194
17.5.4 Kompetanseutfordringer når det gjelder IKT-sikkerhet ... 195
17.5.5 Særskilte personvernutfordringer 195
17.6 Fremtidige problemstillinger og trender ... 198
17.7 Vurderinger og tiltak ... 199
17.7.1 Sterkere styring av IKT-sikkerhet fra Helse- og omsorgs-departementet ... 199
17.7.2 Mer forskning på IKT-sikkerhet innenfor ny helse- og velferds-teknologi ... 200
17.7.3 Etablere løsninger for å imøte-komme utviklingen innenfor helse- og velferdsteknologien ... 200
17.7.4 Gjennomføre flere IKT-øvelser der kritiske systemer er ute av funksjon ... 200

18 Transport ... 201
18.1 Veitrafikk ... 201
18.1.1 Sårbarhet i kjøretøy og digitale trafikkstyringssystemer ... 202
18.1.2 Trafikkstyringens avhengighet av elektronisk kommunikasjon og satellittbaserte tjenester ... 203
18.1.3 Særskilte personvernutfordringer innen veitrafikken ... 203
18.2 Jernbane ... 204
18.2.1 Sikkerhetsutfordringer i skinne-gående trafikk ... 204
18.2.2 Sårbarheter i systemer knyttet til togfremføring ... 205
18.2.3 Avhengighet av ekom ... 205
18.3 Luftfart ... 205
18.3.1 Internasjonale avhengigheter – globale premissgivere ... 206
18.3.2 Sårbarheter om bord i fly ... 207
18.3.3 Systemkompleksitet i operative systemer og på lufthavnene ... 208
18.3.4 Luftfartens avhengighet av ekom og satellittbaserte tjenester ... 208
18.4 Sjøtransport ... 209
18.4.1 Roller og ansvar ... 209
18.4.2 Hjemmelsgrunnlag og tilsyns-virksomhet ... 209

18.4.3 Beredskap og hendelses-håndtering ... 210
18.4.4 Digitale sårbarheter innen sjø-transport ... 210
18.4.5 Fremtidige problemstillinger og trender ... 215
18.5 Vurderinger og tiltak på tvers av transportsektoren ... 215
18.5.1 Styrke IKT-tilsyn og samarbeid mellom transportgrenene ... 216
18.5.2 Etablere en felles rapporterings-kanal for IKT-hendelser innen transportsektoren ... 216
18.5.3 Særskilte tiltak for sjøtransport ... 216

Del IV Tverrsektorielle forhold ... 219

19 Kompetanse ... 221
19.1 Sentrale dokumenter ... 221
19.2 Roller og ansvar ... 223
19.3 Kompetansesituasjonen i samfunnet ... 224
19.4 Utdanning ... 224
19.4.1 Offentlig grunnskole ... 224
19.4.2 Videregående opplæring ... 225
19.4.3 Høyere utdanning ... 226
19.4.4 Etterutdanning ... 228
19.5 Forskning og utvikling (FoU) ... 228
19.5.1 Norsk FoU-aktivitet innen IKT-sikkerhet ... 228
19.5.2 Kvaliteten på norsk IKT-sikkerhetsforskning ... 229
19.5.3 Forskningsrådets rolle ... 230
19.5.4 Internasjonal finansiering ... 230
19.5.5 Diskusjoner ... 230
19.6 Kunnskap og støtte til befolkningen ... 231
19.7 Tjenesteutsetting ... 232
19.8 Vurderinger og tiltak ... 233
19.8.1 Etablere en overordnet nasjonal kompetansestrategi innen IKT-sikkerhet ... 233
19.8.2 Prioriteringer i en overordnet strategi ... 233

20 Styring og kriseledelse ... 238
20.1 IKT-systemer for beredskap og krisehåndtering ... 238
20.1.1 Hva er en krise? ... 238
20.1.2 Sentral kriseledelse ... 239
20.1.3 Regionalt nivå ... 241
20.1.4 Lokalt nivå ... 242
20.1.5 Sivilt–militært samarbeid i kriser ... 242
20.1.6 Risiko- og krisekommunikasjon ... 242
20.2 Sårbarheter knyttet til styring og kriseledelse ... 244
20.2.1 Samhandlingsutfordringer og behov for informasjonsdeling ... 244
20.2.2 Avhengigheter på lokalt og regionalt nivå, og kompetanse-utfordringer ... 244
20.2.3 Risiko- og krisekommunikasjon ... 246
20.2.4 Meteorologiske tjenester ... 247
20.2.5 Kommunikasjonsløsninger for departementene ... 248
20.2.6 Målrettede IKT-angrep ... 249
20.3 Vurderinger og tiltak ... 250
20.3.1 Øke IKT-sikkerhetskompetansen på lokalt og regionalt nivå ... 250
20.3.2 Styrke beredskapen på regionalt og lokalt nivå ... 250
20.3.3 Etablere felles gradert IKT-infrastruktur ... 250
20.3.4 Vurdere virkemidler for kommunikasjon med befolkningen 251

21 Avdekke og håndtere digitale angrep ... 252
21.1 Sentrale begreper og føringer ... 252
21.1.1 Sentrale begreper ... 252
21.1.2 Nasjonale føringer, rapporter og viktige hendelser ... 253
21.2 Roller og ansvar ... 254
21.2.1 Nasjonal sikkerhetsmyndighet ... 254
21.2.2 Sektorvise responsmiljøer ... 254
21.2.3 Politiet, PST og påtale-myndigheten ... 255
21.2.4 Forsvaret ... 256
21.2.5 Andre aktørers ansvar ... 256
21.3 Håndteringskjeden ved tilsiktede hendelser ... 256
21.3.1 Forebygge og forberede ... 257
21.3.2 Avdekke ... 258
21.3.3 Håndtere ... 259
21.3.4 Etterforske ... 260
21.4 Hindre for effektivt samarbeid ... 261
21.4.1 Utfordringer knyttet til roller og ansvar ... 261
21.4.2 Mangel på et felles operativt situasjonsbilde ... 262
21.4.3 Utfordringer knyttet til utveksling av gradert og sensitiv ikke-gradert informasjon på tvers av sektorer ... 262
21.5 Utfordringer knyttet til avdekking av sårbarheter og deteksjon av IKT-hendelser ... 262
21.5.1 Utilstrekkelig evne til å oppdage IKT-hendelser ... 262

21.5.2 Varierende og tidvis motstridende krav til logging og sletting av samme informasjon 263
21.5.3 Mangelfullt grunnlag for et helhetlig IKT-trusselbilde 263
21.6 Kapasitets- og kompetanse-utfordringer knyttet til håndtering av digitale angrep 263
21.6.1 Kompetanse- og kapasitets-utfordringer ved håndtering av hendelser 263
21.6.2 Fragmentert analysekapasitet mellom offentlige og private aktører 264
21.6.3 Utfordringer knyttet til sektorvise responsmiljøer og skalerings-behov ved større hendelser 264
21.7 Kapasitet-, kompetanse- og prioriteringsutfordringer i politiet 264
21.7.1 Utfordringer knyttet til ramme-faktorer 265
21.7.2 Mangelfull kapasitet i politiet 265
21.7.3 Uklarheter knyttet til hvilken aktør som skal etterforske 266
21.7.4 Prioriteringsutfordringer 266
21.8 Manglende evne til videre-utvikling av og investering i politiets IKT-systemer 267
21.9 Sårbarheter som påvirker private virksomheter og enkeltindividets evne til å håndtere hendelser 267
21.9.1 Utilstrekkelig støtte for inn-byggerne og SMB 267
21.9.2 Manglende operative krav i anskaffelser og styring av drifts- og tjenesteleverandører 267
21.10 Aktuelle dilemmaer i forbindelse med utvidede metoder for å avdekke, håndtere og etterforske digitale angrep 268
21.10.1 Behovet for nye etterretnings- og etterforskningsmetoder 268
21.10.2 Endring i maktbalansen mellom stat og borger 269
21.10.3 Masseinnsamling av person-opplysninger til uavklarte formål .. 269
21.10.4 Balansen mellom effektivitet og sikkerhet 270
21.10.5 Balansen mellom kriminalitets-bekjempelse og personvern 271
21.11 Vurderinger og tiltak 272
21.11.1 Etablere og øve et helhetlig rammeverk for digital hendelses-håndtering 272
21.11.2 Forbedre den nasjonale operative evnen gjennom samlokalisering ... 273
21.11.3 Øke deteksjonsevnen og sammen-stille et felles situasjonsbilde 275
21.11.4 Styrke kapasitet og kompetanse knyttet til håndtering av digitale angrep 276
21.11.5 Etablere et nasjonalt «Cyber Crime Center» 277
21.11.6 Sikre sterke fagmiljøer for IKT-kriminalitet i politidistriktene 277
21.11.7 Sikre en IKT-infrastruktur til støtte for politiets kriminalitets-bekjempelse 278
21.11.8 Sikre balansen mellom person-vern og et sikrere samfunn 278

22 Felleskomponenter 280
22.1 Utvalg av felleskomponenter 280
22.2 Roller og ansvar 281
22.3 Hjemmelsgrunnlag og tilsyns-virksomhet 281
22.4 Beskrivelse av felleskomponenter 282
22.4.1 Kartverket 282
22.4.2 Brønnøysundregistrene 282
22.4.3 Skatteetaten 282
22.5 Identifisering av sårbarhet 283
22.5.1 Generelt om sikkerhetsarbeidet ... 283
22.5.2 Sårbarhetsbeskrivelser 284
22.5.3 Andre observasjoner 284
22.6 Vurderinger og tiltak 285
22.6.1 Følge utviklingen av IKT-utsetting for felleskomponenter 285
22.6.2 Utvikle felles beskyttelsestiltak mot sofistikerte IKT-angripere 285
22.6.3 Regulere elektronisk identitet 285

23 Tverrsektorielle sårbarhets-reduserende tiltak 288
23.1 Etablere et nasjonalt rammeverk for å ivareta en helhetsvurdering av verdikjeder 288
23.2 Tydeliggjøre krav til virksomhets-styringssystemer 290
23.2.1 Bevisst bruk av standarder 291
23.3 Styrke Justis- og beredskaps-departementet på IKT-sikkerhetsområdet 291
23.3.1 Tydeliggjøre Justis- og beredskapsdepartementets rolle og ansvarsområde 292
23.3.2 Styrke Justis- og beredskaps-departementets virkemidler 292

23.3.3 Øke kapasiteten innen IKT-sikkerhet i Justis- og beredskapsdepartementet ... 293
23.4 Tilpasse tilsynsvirksomheten til å omfatte IKT-sikkerhet ... 293
23.4.1 Vurdere funksjonsbasert regelverk ... 293
23.4.2 Øke IKT-sikkerhetskompetanse og kapasitet hos tilsynene ... 295
23.5 Redegjørelse for IKT-sikkerhet bør inngå i årsmeldinger ... 295
23.6 Næringsutvikling og IKT-sikkerhet ... 296
23.6.1 Behov for balanse mellom verdiskaping og IKT-sikkerhet ... 296
23.6.2 Økt veiledning for særlig sårbare grupper i næringslivet ... 297
23.6.3 Tillit bør være en forutsetning for digitaliseringen ... 297
23.6.4 IKT-sikkerhet som hinder for verdiskaping? ... 298
23.7 Utkontraktering og skytjenester ... 299
23.7.1 Hva er utkontraktering – internasjonale forhold ... 299
23.7.2 Hva er skytjenester? ... 300
23.7.3 Juridiske forhold ved skytjenester 302
23.7.4 Observasjoner og funn ... 305
23.7.5 Vurderinger og tiltak ... 306
23.8 Regulering av kryptografi ... 307

Del V Økonomiske og administrative konsekvenser ... 309

24 Økonomiske og administrative konsekvenser ... 311

Del VI Vedlegg ... 313

25 Vedlegg ... 315
25.1 Datagrunnlag ... 315
25.2 Ansvarsfordeling mellom departementene for samfunnssikkerhetsarbeidet ... 318
25.3 Oppsummering av sentrale utvalg 320

Referanser ... 324

Del I
Innledning

Kapittel 1
Sammendrag

De siste tiårene har digitaliseringen ført til gjennomgripende samfunnsmessige endringer. Den har effektivisert arbeidshverdagen for de fleste av oss, slik at det samme arbeidet nå kan utføres av langt færre hender. Den har forandret måten vi styrer prosesser på, slik at komplekse operasjoner og infrastrukturer nå kan kontrolleres fra ett eller noen få sentrale steder. Den har gitt befolkningen en lang rekke nye tjenester, som kontantløs handel og finansielle tjenester på mobil, elektronisk samhandling med det offentlige og sanntids trafikkinformasjon som lar oss finne den mest hensiktsmessige reiseveien mellom to steder. Videre har den revolusjonert måten vi kommuniserer på, ved at mobiltelefoner, sosiale medier og samarbeidsstøtteverktøy er blitt dagligdags. Norge ligger i verdenstoppen når det gjelder bruk av IKT. Dette gjør norsk næringsliv mer konkurransedyktig, og øker samfunnets totale produktivitet og innovasjonsevne. En videreføring av denne situasjonen forutsetter at samfunnet har tillit til at teknologien er trygg å ta i bruk.

De store teknologiske endringene gir oss noen utfordringer. Vi ser at sentrale tjenester for samfunnet, som for eksempel betaling og telefoni, utfordres av internasjonale aktører som leverer tjenester i Norge uten at norske myndigheter har rettslig kontrollmulighet over dem. Dessuten er vår evne til å holde informasjon konfidensiell utfordret, og dermed også personvernet. I tillegg utsettes mange virksomheter for reelle trusler knyttet til at det utstyret de bruker kan angripes, og som et resultat bli delvis styrt av uvedkommende. Det foreligger således et betydelig teknologisk press som kan utfordre sentrale samfunnsverdier.

En spesielt viktig observasjon er at kritiske samfunnsfunksjoner er blitt avhengige av lange og uoversiktlige digitale verdikjeder, som gjerne spenner over mange sektorer og flere land. Slik vil sårbarheten til for eksempel en betalingstjeneste på mobil avgjøres av lovhjemler og tilsynsregimer i kraftsektoren, i ekomsektoren, i finanssektoren og innenfor næringsregulering. En underleverandør som har utkontraktert sentrale deler av virksomheten til et annet land, vil kunne arve sårbarheter fra de tilsvarende sektorene i vedkommende land.

Slike sammensatte, sektorovergripende verdikjeder finner vi i alle de kritiske samfunnsfunksjonene denne rapporten omhandler. Dette har betydning for hvordan vi bør forholde oss til både tilsiktede og utilsiktede hendelser. Konsekvensene av en digital hendelse kan ligge i en annen sektor enn hendelsen selv, og vissheten om at en angriper ikke forholder seg til sektorgrensene utfordrer vår evne til å håndtere skarpe situasjoner på en effektiv og hensiktsmessig måte.

En effekt av den digitale utviklingen er en kraftig endring i samfunnets risiko- og sårbarhetsbilde. Vi opplever nye trusler, som for eksempel at maskiner og infrastruktur i Norge kan angripes av anonyme aktører som befinner seg i andre land. Vi har fått nye sårbarheter å forholde oss til, som at programmeringsfeil i én komponent kan få effekter som slår ut store deler av mobilnettet. Samfunnsfunksjonene våre er – gjennom digitale verdikjeder – utsatt for hendelser på nye og tidligere ukjente måter. For eksempel kan svikt i telekommunikasjonsnettene føre til at veitunneler må stenges og at leger ikke får tilgang til pasientjournaler.

På samme måte som digitaliseringen har endret sårbarhetsbildet i samfunnet, vil måten vi håndterer disse sårbarhetene på, ha betydning for hvilket samfunn vi skaper for fremtiden. I et overordnet samfunnsperspektiv vil en forsvarlig ivaretakelse av sårbarhetsutfordringene være avgjørende for å opprettholde rettsstatens og demokratiets grunnleggende verdier. På samme tid kan nettopp disse samme verdiene komme under press i møte med andre og utfordrende digitale muligheter, for eksempel overvåking av enkeltindividet eller av befolkningen som sådan.

Norge regnes som et av de mest digitaliserte landene i verden. Dette har gitt oss store effektiviserings- og moderniseringsgevinster, men det har også ført til at vi er et av de landene der endringen

i risiko- og sårbarhetsbildet har kommet lengst. En av utfordringene ved å ha kommet så langt, er at det ofte mangler tydelige eksempler fra andre land å se hen til. Denne endringen krever at vi som samfunn videreutvikler og endrer måten vi forholder oss til sårbarheter på. Likevel er det klart at mange av de utfordringene vi nå står overfor, bare kan løses i en internasjonal kontekst. For et lite land som Norge vil det være svært viktig å delta aktivt på de internasjonale arenaene der relevante problemer diskuteres.

I denne utredningen gir vi en fremstilling av hvilke grep vi mener det norske samfunnet bør ta. Under følger de viktigste anbefalingene våre.

- *Redusere kritikaliteten av Telenors kjerneinfrastruktur.* Telenors kjerneinfrastruktur inngår som en komponent i nær sagt alle digitale verdikjeder. Et utfall i denne får derfor alvorlige og samtidige konsekvenser på de aller fleste samfunnsområder, og for alle de kritiske samfunnsfunksjonene som er omtalt i denne rapporten. Telenors kjerneinfrastruktur er godt utbygd, den er profesjonelt operert, og den har historisk sett meget høy stabilitet. Likevel vil den kunne settes ut av spill ved menneskelige feil, rutinesvikt, sabotasje, terror eller utro tjenere. Det er utvalgets syn at den totale summen av samfunnsverdier dette nettet bærer, er uakseptabelt høy. Utvalget vil derfor anbefale at det arbeides mot et målbilde der minst én tilleggsaktør har et landsdekkende kjernenett som er på samme nivå som Telenors med hensyn til dekning, kapasitet, fremføringsdiversitet, redundans og uavhengighet.
- *Sikre balansen mellom personvern og et sikrere samfunn gjennom utredninger og offentlig debatt.* Utvalget har merket seg at hensynet til samfunnets sikkerhet fører med seg forslag om innføring av nye og inngripende overvåkingsmetoder. Eksempler på dette er forslag om innføring av digital grenseovervåking og PSTs ønsker om å registrere ytringer på sosiale medier og analysere informasjon fra åpne kanaler. Utvalget erkjenner det etterretningsfaglige og politifaglige behovet som ligger bak slike forslag, men mener at forslagene er av en så inngripende natur at de ikke bør innføres uten en forutgående offentlig debatt. En slik debatt bør forberedes gjennom en offentlig utredning som diskuterer denne typen virkemidler i sin fulle bredde. Hensyn til etterretningsbehov, teknologisk kompetanse og personvern må ivaretas, og det må sikres en grundig redegjørelse for de teknologiske, rettslige og samfunnsmessige spørsmålene sakene reiser.
- *Bruk av kryptografi bør ikke reguleres.* Det foregår en debatt internasjonalt om hvorvidt bruken av sterk kryptografi bør reguleres. Det er svært vanskelig – kanskje umulig – å lage systemer som samtidig ivaretar legitime behov for beskyttelse og et legitimt behov for avlytting. Det er rimelig å tro at begrensninger på lovlig bruk av kryptografi vil ramme norske borgere, virksomheter og myndigheter. Slike begrensninger vil imidlertid ikke i vesentlig grad hindre uærlige aktørers bruk av kryptografi og dermed heller ikke løse politiets og etterretningstjenestenes problem. Det er derfor utvalgets oppfatning at bruk av kryptografi ikke bør reguleres eller forbys i Norge, at norske myndigheter bør arbeide aktivt mot regulering eller forbud internasjonalt, og at det må utvikles nye etterforskningsmetoder for å sikre et effektivt politi- og etterretningsarbeid.
- *Styrke Justis- og beredskapsdepartementets tverrsektorielle virkemidler på IKT-sikkerhetsområdet.* Ingen sektor kan kontrollere sin egen digitale sårbarhet alene. Verdikjedene gjør at alle arver sårbarheter fra andre sektorer, og angripere forholder seg ikke til sektorgrensene. Samtidig observerer utvalget at sektorene tidvis har vansker med å enes om en gjennomføring av sektorovergripende tiltak. Utvalget er enig i at de ulike sektorene i mange tilfeller er svært forskjellige og kan ha behov for spesifikke tilpasninger. Dette står imidlertid ikke i motsetning til sektorovergripende løsninger dersom disse angir en nedre grense, slik at sektorene står fritt til å definere strengere krav. Utvalget vurderer det slik at utvikling av sektorovergripende mekanismer vil være nødvendig over tid, og at et effektivt sektorovergripende virkemiddelapparat vil være nødvendig for å håndtere samfunnets IKT-sårbarheter. Justis- og beredskapsdepartementet bør derfor settes bedre i stand til å gjennomføre sektorovergripende tiltak.
- *Etablere et helhetlig rammeverk for digital hendelseshåndtering.* Utvalget har merket seg at offentlige og private virksomheter som blir utsatt for alvorlige dataangrep, opplever usikkerhet og utilstrekkelig koordinering mellom myndighetsaktører som har ansvar for å bekjempe digitale angrep. Utvalget mener derfor at Justis- og beredskapsdepartementet må ta initiativ til å etablere et helhetlig rammeverk for å avklare og tydeliggjøre innsatsen mellom relevante aktører innen hendelseshåndtering

og straffeforfølgning. Rammeverket bør etableres og øves i tett samarbeid med Forsvarsdepartementet.

- *Styrke politiets evne til å bekjempe IKT-kriminalitet.* Utvalget observerer at det blant virksomheter og hos enkeltindivider er lave forventninger til hvilken bistand politiet kan gi når man blir utsatt for IKT-kriminalitet. Dette fører blant annet til at IKT-kriminalitet i liten grad blir anmeldt. Utvalget vil derfor støtte forslaget til opprettelsen av et nytt nasjonalt senter for å forebygge og etterforske kompleks og grenseoverskridende IKT-kriminalitet. Senteret bør organiseres under Kripos, og det bør ha et nasjonalt fagansvar for forebygging og etterforskning av alvorlig og kompleks IKT-kriminalitet. Videre bør det ha en særskilt bistandsfunksjon for å støtte politidistriktene både polititaktisk og påtalefaglig.
- *Tydeliggjøre et myndighetsansvar for norsk romvirksomhet.* De fleste samfunnsområder er gjennom digitale verdikjeder mer eller mindre avhengige av digitale satellittbaserte tjenester. Disse tjenestene kan være posisjon, navigasjon, presis tidsangivelse, kommunikasjon, jordobservasjon med mer. Myndighetsbildet knyttet til området er komplekst. Regulering av romvirksomheten er hjemlet i mange ulike lover og forskrifter, og ansvaret for oppfølging av romsektoren er desentralisert. Behovet for tydeliggjøring av myndighetsansvaret for norsk romvirksomhet omhandler å øke bevisstheten rundt de ulike samfunnsområdenes sårbarheter, identifisere avhengigheter og stille krav til og føre tilsyn med romvirksomheten.
- *Styrke IKT-sikkerhetskompetansen i flere sektortilsyn.* Utvalget ser en økende digitaliseringstakt innenfor de fleste sektorer, og tilsynsmyndighetene vil møte mange mer eller mindre nye og komplekse problemstillinger. Det vil derfor i økende grad være behov for å styrke IKT-sikkerhetskompetansen innenfor flere sektortilsyn. På kort sikt vil det være viktig med felles ressurser, slik at ulike sektortilsyn kan tilføres kompetanse fra for eksempel Nasjonal sikkerhetsmyndighet i enkelttilfeller. På lengre sikt tilsier teknologiutviklingen at sektorer og tilsynsvirksomheter må etablere en egen IKT-sikkerhetskompetanse. Mange av problemstillingene knyttet til IKT-sikkerhet vil være felles for de fleste sektorer, og det vil være hensiktsmessig å etablere fellesarenaer for erfaringsutveksling og dialog mellom sektortilsyn og tverrsektorielle tilsyn. I forbindelse med at det stilles krav til IKT-sikkerhet, bør funksjonsbasert regelverk og tilsyn vurderes – dette for å kunne følge med på raske teknologiske endringer og legge til rette for sikkerhetstiltak som er tilpasset den enkelte virksomhet.
- *Etablere en overordnet nasjonal kompetansestrategi innen IKT-sikkerhet.* Utvalget har sett at det eksisterer en utfordrende kompetansesituasjon innen IKT-sikkerhet på de fleste nivåer i samfunnet. Læreplanene for grunnskolen og den videregående skolen har målformuleringer knyttet til temaet, men det er uklart om det reelle læringsutbyttet dekker den kunnskapen om IKT-sikkerhet som hver enkelt av oss må ha for å kunne håndtere en digitalisert hverdag på en trygg måte. Utvalget mener at en overordnet strategi bør ha et mål om at et minimum av IKT-sikkerhet må inngå i alle IKT-bachelorgrader. Det må etableres en kapasitet på mastergradsutdanning i IKT-sikkerhet som står i forhold til det kompetansebehovet som finnes i offentlig og privat sektor, og det bør utvikles en langsiktig plan for oppbygging og vedlikehold av norsk forskningskapasitet på området.

I tillegg til forslagene til tiltak vi har fremhevet her, fremmer vi forslag om tiltak innenfor hvert av temaene elektronisk kommunikasjon, satellittbaserte tjenester, energiforsyning, olje og gass, vannforsyning, finansielle tjenester, helse og omsorg, transport, kompetanse, styring og kriseledelse, avdekking og håndtering av digitale angrep, felleskomponenter og tverrsektorielle problemstillinger. Hvert av disse temaene er behandlet i de separate kapitlene 11–23.

Kapittel 2
Mandat, utvalgets sammensetning og arbeid

Lysneutvalget er satt ned av Regjeringen for å kartlegge samfunnets digitale sårbarhet. Utvalget skal foreslå konkrete tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet.

2.1 Mandat

Internett og nye IKT-anvendelser har endret vår hverdag radikalt de siste 15–20 årene. IKT er i alt – i telefonen, bilen, panelovnen, postkassen og hvitevarene. Teknologien er i alle hjem, på de aller fleste arbeidsplasser, i operasjonsstuen på sykehuset, på kraftstasjonen og i politibilen. Enheter, maskiner og brukere kobles sammen på stadig nye måter, og bruken av internett som infrastruktur fortsetter å vokse. De fleste kritiske infrastrukturer og samfunnsviktige funksjoner er i dag digitalisert. Vår avhengighet av IKT i samfunnsmessige, næringsmessige og private sammenhenger er stor og økende.

Dette medfører nye sårbarheter i samfunnet. Med økende avhengighet mellom kritiske komponenter kan flere viktige samfunnsfunksjoner bli skadet eller lammet i utilsiktede hendelser som for eksempel en ulykke eller ekstremvær. Samtidig har det digitale rom åpnet for nye tilsiktede og alvorlige trusler fra både statlige og ikke-statlige aktører. Kriminalitet, mellomstatlige kriser og konflikter har i stadig større grad digitale elementer i seg. Det digitale rom og de digitale tjenestene er koblet sammen på tvers av sektorer og på tvers av landegrenser. Det kan være ulike aktører som eier, har tilsyn med og driver de ulike infrastrukturene, og ansvarslinjene mellom dem oppleves ikke alltid som like klare.

Dette medfører en rekke utfordringer blant annet knyttet til personvern, rettssikkerhet, samfunnssikkerhet og kriminalitetsbekjempelse. Denne utviklingen har også stor betydning for myndighetenes informasjonsinnhenting og -bearbeiding og forebyggende virksomhet.

Det er på denne bakgrunn behov for en gjennomgang som kartlegger samfunnets digitale sårbarheter slik at vi kan få et solid faglig grunnlag for ytterligere å styrke og samordne vår beredskap. Gjennomgangen skal gi et grunnlag for å vurdere tiltak som støtter opp om overordnede mål som å trygge liv og helse, økonomisk vekst og sosial utvikling, rettigheter og eiendom, sikre ivaretagelse av lov og orden, nasjonale sikkerhetsinteresser, rettsstatlige prinsipper, personvern og demokratisk styresett.

Utvalgsarbeidet skal basere seg på eksisterende kunnskapsgrunnlag om dagens og fremtidens utfordringer. Utvalget kan be om særskilte utredninger fra eksperter/ekspertgrupper på enkeltområder.

Utvalget skal ikke vurdere nasjonale regler for datalagring vedtatt ved lov 11. april 2011 nr. 11 eller konsekvensene for norsk rett av EU-domstolens avgjørelse i saken om datalagringsdirektivet.

Utvalget skal utrede følgende:

1. Utvalget skal beskrive de digitale sårbarheter som Norge står overfor i dag og i nærmeste fremtid. Sårbarheter innen kritiske samfunnsfunksjoner og kritisk infrastruktur, blant annet elektronisk kommunikasjon, kraftforsyning og bank- og finansielle tjenester, og de gjensidige avhengigheter mellom disse, skal spesielt analyseres nærmere. Utvalget skal vurdere hvilke konsekvenser denne sårbarheten kan få for enkeltmennesker, næringsliv og samfunnssikkerheten. I denne forbindelse skal utvalget også se på sivilt-militært samarbeid og samarbeid mellom offentlige og private aktører.
2. Utvalget skal beskrive aktuelle problemstillinger knyttet til sikring av informasjon, derunder eventuell manglende kontroll i egen virksomhet med leverandører. Utvalget skal redegjøre for tiltak som bør settes i verk for å hindre at informasjon blir behandlet rettsstridig eller på annen måte blir kompromittert.
3. Utvalget skal beskrive de sentrale folkerettslige rammer for grenseoverskridende informasjonsinnhenting. Videre skal utvalget identifi-

sere de internasjonale arenaer hvor folkerettslige problemstillinger i det digitale rom diskuteres, og som er av særlig relevans for Norge og norske interesser.

4. Utvalget skal vurdere de digitale sikkerhetsutfordringene ved IKT-kriminalitet, spionasje, sabotasje og terror. Utvalget skal beskrive behovet for å kunne avdekke, håndtere og etterforske digitale angrep. Utvalget skal beskrive de dilemmaer som må tas hensyn til i denne sammenheng, særlig knyttet til næringsutvikling, demokratisk deltakelse og forholdet mellom personvern og informasjonsinnhenting.
5. Utvalget skal foreta en prinsipiell vurdering av hvordan samfunnet bør forholde seg til håndtering av digital sårbarhet. Utvalget skal vurdere effekt sett opp mot kostnader og ulemper ved risikoreduserende tiltak (proporsjonalitet), balansen mellom forebyggende tiltak og evne til skadereduksjon ved faktiske hendelser, samt hvilken grad av sårbarhet samfunnet bør være beredt til å leve med.
6. Utvalget skal beskrive hvordan relevante allierte og andre sammenlignbare land arbeider med å redusere denne sårbarheten, med særlig vekt på virkemidler som har overføringsverdi til norske forhold.
7. På denne bakgrunn skal utvalget komme med forslag til tiltak som kan bidra til å redusere sårbarheten. De anbefalte tiltakene kan være av regulatorisk, strukturell, organisatorisk, teknologisk eller kompetansemessig karakter.
8. Utvalget skal utrede administrative, økonomiske og andre vesentlige konsekvenser av sine anbefalinger. Minst ett forslag skal baseres på uendret ressursbruk.
9. Dersom det er behov for å gjøre mindre endringer i mandatet så skal utvalget ta dette opp med Justis- og beredskapsdepartementet som kan beslutte disse.
10. Utvalget skal levere sin utredning i form av en NOU til Justis- og beredskapsdepartementet innen utgangen av september 2015. Innstillingen skal utarbeides i en form som egner seg til å bli sendt på en offentlig høring. De delene av utvalgets arbeid som vil omfatte gradert informasjon, vil måtte behandles av en begrenset del av utvalgets medlemmer. Disse må ha nødvendig sikkerhetsklarering. Materiale som er gradert utarbeides i separate vedlegg.

2.2 Mandatforståelse

Mandatet favner vidt og byr derfor på både muligheter og begrensninger innenfor det tidsrommet utvalget disponerer. Mulighetsrommet ligger i å se sårbarhet i et helhetlig samfunnsperspektiv. Begrensningene innebærer at det ikke har vært mulig med en omfattende analyse av hvert enkelt område. Det vil derfor være digitale sårbarheter i samfunnet vårt som ikke er omhandlet i tilstrekkelig grad i denne utredningen.

Rammeverket for kritisk infrastruktur og kritiske samfunnsfunksjoner (KIKS-rammeverket) er lagt til grunn for utvelgelsen av områdene utvalget har vurdert.[1] Kritiske samfunnsfunksjoner er de funksjoner som dekker samfunets og befolkningens grunnleggende behov. Kritisk infrastruktur er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner. Vårt arbeid med å se på digitale sårbarheter har omfattet å vurdere sårbarheter på flere *nivåer* av systemer – både på et overordnet samfunnsnivå og i tekniske infrastrukturer og systemer.

Forslag til tiltak for å redusere sårbarheten og styrke samfunnssikkerheten må vurderes med tanke på om de griper inn i og forrykker de konstitusjonelle og menneskerettslige grensene for statens maktutøvelse overfor befolkningen. Både risiko for svikt i IKT-systemer og reduksjon av risiko kan få konsekvenser både for samfunnet som helhet og for det enkelte individ. På overordnet nivå omtaler vi derfor våre grunnleggende samfunnsverdier og forpliktelser som sentrale premisser for det videre arbeidet med de problemstillingene vi presenterer. I tråd med mandatet vil derfor utvalget i så stor grad som mulig vise til områder der vi ser at det er utfordrende å opprettholde en god balanse mellom forsvarlig håndtering av digital sårbarhet og de grunnleggende samfunnsverdiene.

Utvalget har sett på sårbarheter i det sivile samfunnet og i noen grad beskrevet sivilt–militært samarbeid. I den sammenheng er det sivile samfunnets avhengighet av Forsvaret til dels omhandlet. Forsvarets avhengighet av sivil sektor og sårbarheter i Forsvarets egne IKT-systemer er ikke omhandlet. Utvalget er imidlertid klar over at Forsvaret i økende grad er avhengig av sivil infra-

[1] DSB (2012): *Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring.* KIKS-prosjektet – 1. delrapport. Revidert KIKS-rammeverk er planlagt utgitt i løpet av høsten 2015.

struktur for å utføre sitt samfunnsoppdrag, spesielt knyttet til elektronisk kommunikasjon.

Problemstillinger og tiltak knyttet til sikring av informasjon er først beskrevet teoretisk i innledende kapitler. Tiltakene er omtalt i kapittelet om felleskomponenter, der utvalget har valgt å se nærmere på sentraliserte funksjoner som offentlige registre og portaler, herunder anbefalinger knyttet til elektronisk identitet. Svært mye informasjon kan være sensitiv og samfunnsviktig selv i ugraderte systemer. Traavik-utvalget[2] er bedt om å komme med tiltak for å harmonisere relevant lovregulering, og utvalget har valgt å avgrense mot denne problemstillingen.

I kapittelet om å avdekke og håndtere digitale angrep omtales sårbarheter som vil påvirke evnen til å håndtere digitale angrep med konsekvenser for i hovedsak samfunnssikkerheten og næringslivet. Utvalget drøfter ikke PSTs eller Etterretningstjenestens mandat og oppgaveløsning utover å foreslå fremgangsmåte ved innføring av nye, personverninngripende metoder.

Utvalgets vurdering av IKT-kriminalitet avgrenses mot tradisjonell organisert kriminalitet der IKT-systemer benyttes som verktøy for å begå straffbare handlinger. Politiets arbeid med elektroniske spor er bare drøftet i relasjon til saker som gjelder de alvorligste formene for IKT-kriminalitet. I henhold til mandatet begrenser utvalget sin omtale av straffesakskjeden til å gjelde den delen som er knyttet til politiets og påtalemyndighetens arbeid.

EOS-utvalget[3] fører en ekstern og uavhengig kontroll av om de hemmelige tjenestene – EOS-tjenestene – holder seg innenfor regelverket, spesielt for å hindre at enkeltpersoner blir utsatt for ulovlig overvåking. Utvalget har ikke vurdert EOS-utvalgets kapasitet og kompetanse til å utføre denne kontrollen, da det pågår en parallell evaluering som skal avsluttes i mars 2016.

Utvalget er bedt om å vurdere hvordan samfunnet bør forholde seg til håndtering av digital sårbarhet. For hvert enkelt tiltak har utvalget diskutert kostnader og ulemper sett opp mot ønsket effekt. Ut fra sårbarhetsbeskrivelsene er det vurdert både forebyggende og konsekvensreduserende tiltak. Utvalget er av den oppfatning at det på det nåværende tidspunkt er lite hensiktsmessig å formulere en grad av sårbarhet som samfunnet bør være beredt til å leve med. Grunnen til det er at det ikke finnes noe metodisk grunnlag for å fastslå hvilken sårbarhet som foreligger. Det er utvalgets syn at et slikt grunnlag må bygges først. Vårt viktigste tiltak i den retning er å etablere et rammeverk for helhetsvurdering av digitale verdikjeder. Det vil skape en bevisstgjøring og en synliggjøring av sårbarheter som igjen kan danne grunnlag for hensiktsmessige forebyggende tiltak.

2.3 Sammensetning og utvalgets arbeid

Utvalget har hatt ni medlemmer:
- Leder: Olav Lysne, Bærum, professor (Simula Research Laboratory)
- Janne Hagen, Ski, forsker (Forsvarets forskningsinstitutt)
- Fredrik Manne, Fjell (Hordaland), professor (Universitetet i Bergen)
- Åke Holmgren, Stockholm (Sverige), senior strategisk rådgiver (Myndigheten för samhällsskydd och beredskap)
- Eva Jarbekk, Oslo, advokat og partner (Advokatfirmaet Føyen Torkildsen)
- Einar Lunde, Mandal, avdelingsdirektør (Nasjonal kommunikasjonsmyndighet)
- Kristian Gjøsteen, Trondheim, professor (Norges teknisk-naturvitenskapelige universitet)
- Sofie Nystrøm, Oslo, direktør (Center for Cyber and Information Security)
- Kristine Beitland, Oslo, direktør myndighetskontakt (Microsoft)

Utvalget har hatt et fast sekretariat som har bestått av:
- Sekretariatsleder: Roger Kolbotn, seniorrådgiver (Justis- og beredskapsdepartementet)
- Ingunn Moholt, utredningsleder (Direktoratet for samfunnssikkerhet og beredskap)
- Lene Bogen Kaland, seniorrådgiver (Nasjonal sikkerhetsmyndighet)
- Ragnhild Castberg, seniorrådgiver (Datatilsynet), fra 1. november 2014
- Håkon Hermansson, seniorrådgiver (Nasjonal sikkerhetsmyndighet), til 20. mars 2015
- André Nordbø, rådgiver (Politidirektoratet), fra 10. april 2015

Utvalgets arbeid er basert på ulike metoder og datagrunnlag:
- eksisterende utredninger og analyser
- skriftlige innspill og møter med en rekke departementer, direktorater og tilsyn, forsk-

[2] Regjeringen.no. *Pressemelding 27.03.2015 Regjeringen oppnevner sikkerhetsutvalg.*

[3] Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste.

nings- og undervisningsinstitusjoner, interesseorganisasjoner og konsulentselskaper (se vedlegg 25.1)
- analyser og utredninger som er gjennomført av offentlige og private virksomheter på oppdrag av utvalget og benyttet som innspill til tekst og beskrivelser, uten at alt er tatt videre av utvalget til NOU-en (se vedlegg 25.1)

Utvalget har i tillegg hatt fortløpende dialog med en rekke personer og virksomheter i utvalgsperioden, spesielt med tanke på å få utdypet problemstillinger og kvalitetssikret informasjon.

Utvalget har hatt 16 møter, enkelte over to dager, og har i tillegg gjennomført studiebesøk til Brussel og Berlin. I Brussel møtte utvalget den norske EU-delegasjonen, representanter fra noen av EUs generaldirektorater og NATO, samt private aktører. I Berlin besøkte utvalget BMI (Bundesministerium des Innern) og BSI (Bundesamt für Sicherheit in der Informationstechnik).

2.4 Struktur og innhold

Utredningen er delt inn i fem deler.

Del I består av sammendrag, mandat og en beskrivelse av mandatforståelsen, sammensetningen av utvalget og en oversikt over hvordan rapporten er strukturert.

Del II gir et bakteppe for diskusjonen om digitale sårbarheter i samfunnet vårt. Det pekes på sentrale avveininger mellom ulike samfunnshensyn og verdier, sett i lys av digitaliseringen av samfunnet og digitale sårbarheter.

Videre gir vi en beskrivelse av hva som legges i begrepet *digitale sårbarheter*, utfordringer ved sikring av IKT og digital informasjon, digitale trender som påvirker sårbarhetsbildet, og tilsiktede og utilsiktede IKT-hendelser.

Vi gir også en oversikt over organisering av roller og ansvar og sentrale tverrsektorielle virksomheter på IKT-sikkerhetsområdet, samt de overordnede målene og prinsippene som gjelder for IKT-sikkerhetsarbeidet i Norge. IKT-sikkerhetsutfordringer er grenseoverskridende, og i kapittelet om andre lands arbeidsformer gir vi en oversikt over IKT-sikkerhetsarbeid som kan ha overføringsverdi til Norge.

Avslutningsvis i denne delen beskrives folkerettslige rammer for grenseoverskridende informasjonsinnhenting og internasjonalt samarbeid.

Del III gir en oversikt over det digitale sårbarhetsbildet for en rekke samfunnsfunksjoner: elektronisk kommunikasjon, satellittbaserte tjenester, energiforsyning, finansielle tjenester, olje og gass, vannforsyning, transport og helse og omsorg. Utvalget foreslår tiltak for å redusere sårbarhetene som er identifisert.

En særlig problemstilling i utvalgets arbeid er tverrsektorielle forhold. Del IV omtaler sårbarheter og tiltak innenfor områdene kompetanse, styring og kriseledelse, avdekking og håndtering av digitale angrep, og felleskomponenter.

Avslutningsvis i denne delen gir vi en oversikt over noen sentrale tverrsektorielle sårbarhetsreduserende tiltak, i hovedsak basert på summen av sårbarheter som er identifisert i utredningen.

Del V gir en omtale av økonomiske og administrative tiltak. Vedlegg følger i del VI.

Del II
Situasjonsbeskrivelse

Kapittel 3
Rettsstatsprinsipper og grunnleggende samfunnsverdier

I Sårbarhetsutvalgets utredning fra 2000 slås det fast at IKT-systemene er blitt en av samfunnets bærebjelker, og at samfunnet er blitt mer sårbart for svikt i disse systemene.[1] Denne utredningen fikk bred omtale og oppfølging. Utredningen ble i 2006 fulgt opp av Infrastrukturutvalget, som kartla landets kritiske infrastruktur og kritiske samfunnsfunksjoner.[2] Først ut i rekken med sårbarhetsutredninger knyttet til bruk av IKT var imidlertid Seip-utvalget i 1986 med *Datateknikk og samfunnets sårbarhet.*[3] I utredningen uttrykkes det:

> «Datateknikk og telekommunikasjon har skapt store forandringer i næringsliv og offentlig forvaltning. I løpet av drøye 20 år er EDB tatt i bruk i større eller mindre grad på de aller fleste områder, skritt for skritt innen den enkelte bedrift/institusjon, uten at man samtidig har tilstrebet noen samlet oversikt over EDB-avhengighet og samfunnsmessige konsekvenser. Dette har ført til nye og uoversiktlige strukturer og avhengighetsforhold innen næringsliv og forvaltning.»

Siden den gang er Internett og IKT-systemer blitt stadig mer integrert i alle deler av samfunnet, herunder i kritiske samfunnsfunksjoner. Utviklingen har ført til økt avhengighet av IKT, en avhengighet som også gjør samfunnet mer sårbart for svikt og angrep på grunn av utilstrekkelig IKT-sikkerhet. Se vedlegg 25.3 «Oppsummering av sentrale utvalg».

I et overordnet samfunnsperspektiv vil en forsvarlig ivaretakelse av utfordringer på sårbarhets- og sikkerhetsområdet være avgjørende for å opprettholde rettsstatens og demokratiets grunnleggende verdier. På samme tid kan nettopp disse samme verdiene komme under press i møte med andre utfordrende digitale muligheter, for eksempel overvåking av enkeltindividet eller befolkningen som sådan. Det er et mål å kunne håndtere sårbarhet på en slik måte at det ikke forrykker balansen mellom borgerne og myndighetene.

Forslag til tiltak for å redusere sårbarheten og styrke samfunnssikkerheten må derfor belyse hvilke konsekvenser de kan ha både for hver enkelt av de verdiene vi legger til grunn for et sunt og velfungerende samfunn, og for summen av dem. I tråd med mandatet vil derfor utvalget i så stor grad som mulig vise til områder der vi ser at det er utfordrende å opprettholde en god balanse mellom forsvarlig håndtering av digital sårbarhet og de grunnleggende samfunnsverdiene.

Våre grunnleggende samfunnsverdier kommer til utrykk både i nasjonal og i internasjonal rett. Grunnloven og rettssystemet vårt bygger på rettsstatsprinsipper som legalitetsprinsippet, rettssikkerhetshensyn, demokratihensyn og menneskerettigheter, herunder personvern, ytringsfrihet og forsamlingsfrihet. Det er disse verdiene som er fundamentet for reguleringen av det innbyrdes forholdet mellom statsmaktene ved maktfordelingsprinsippet og forholdet mellom staten og befolkningen.

Grunnloven og menneskerettighetskonvensjonene vi har forpliktet oss til å overholde, har avgjørende betydning for forholdet mellom stat og individ på mange områder. Dette gjelder også for samfunnets håndtering av digital sårbarhet. Disse samfunnsverdiene kan ses på som «dørvoktere» for statens adgang til å gripe inn i befolkningens og enkeltindividets rettigheter og friheter.

De siste endringene i Grunnloven, fra 2014, styrker vernet om flere grunnleggende menneskerettigheter, herunder retten til privatliv, personvern, ytringsfrihet og krav på rettssikkerhet. Endringen av Grunnloven § 102 utvider vernet om enkeltindividet eksplisitt ved at enkeltindividets kommunikasjon også omfattes, og ved at «statens myndigheter skal sikre et vern om den enkeltes

---

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

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

3 NOU 1986: 12 *Datateknikk og samfunnets sårbarhet.*

integritet». Fordi bare noen få menneskerettigheter er tatt inn i Grunnloven, er det viktig at Grunnloven viser til menneskerettsloven[4], som slår fast at visse menneskerettighetskonvensjoner gjelder som norsk lov, og at disse reglene går foran annen norsk lov ved eventuell motstrid. Det finnes i tillegg flere lignende reguleringer i andre deler av lovgivningen, for eksempel innen straff, prosess, utdanning, diskriminering og barns rettigheter.

3.1 Digital ivaretakelse av grunnleggende samfunnsverdier

Den digitale utviklingen har skapt nye og bedre forutsetninger for å ivareta mange av de grunnleggende samfunnsverdiene. Digitaliseringen har gitt nye muligheter for samspill og informasjonsutveksling mellom befolkningen og offentlige myndigheter. I dag er det en helt annen grad av åpenhet i offentlig forvaltning, noe som bidrar til at den enkelte kan foreta informerte valg fordi det er enklere å få innsyn i viktige beslutninger og arbeidsprosesser i forvaltningen.

Det er også grunn til å anta at etableringen av nettbaserte rettslige informasjonssystemer, som for eksempel Lovdata, har sikret en større grad av likebehandling og dermed gitt bedre rettssikkerhet gjennom tilgangen til lovforarbeider, oppdaterte rettsregler, sentrale forvaltningsavgjørelser og dommer.

Internett-tilgang og nettpublisering har ikke minst endret forutsetningene for enkeltindividets adgang til å benytte retten til å ytre seg. Mulighetene for frie ytringer er tilnærmet uendelige gjennom et mangfold av ulike nettfora som når frem til ulike deler av befolkningen, noe som ikke var mulig i «førdigital tid». Ikke minst har Internett gitt tilgang til kunnskap som tidligere var lite tilgjengelig, og som både forutsatte kjennskap til hva man skulle lete etter, og som likevel var tidkrevende å finne frem til.

Digitalisering har ført til langt mer effektiv kommunikasjon og tilgang til informasjon, både for befolkningen, det private næringslivet og offentlig forvaltning. Effektivisering har derfor vært et sentralt argument for videreutviklingen av digitale tjenester og oppgaver i både privat og offentlig sektor.

Utviklingen har foregått i et ekstremt raskt tempo. Den digitale utviklingstakten synes å ligge konstant i forkant av tilstrekkelig kunnskap hos mange aktører som har tatt de teknologiske mulighetene i bruk. Negative konsekvenser av bruken har i liten grad vært overskuelige på det tidspunktet mange IKT-systemer ble etablert. Risiko og sårbarhet har ofte blitt kjent etter at IKT-systemene ble tatt i bruk, og er som regel blitt forsøkt utbedret i etterkant. Denne sårbarheten eksponeres ytterligere når stadig nye programvarer kobles til gamle systemer i kombinasjon med bruk av Internett som infrastruktur. Mange IKT-systemer representerer en vesentlig grad av usikkerhet og sårbarhet på grunn av dette. I et sårbarhetsperspektiv kan man spørre seg om det har vært en utilsiktet aksept av risiko i både privat og offentlig sektor.

3.2 Menneskerettigheter

De internasjonale menneskerettighetene ble utviklet i kjølvannet av andre verdenskrig. Bakteppet var de massive krenkelsene av individets integritet og verdighet særlig under nazistenes styre i Tyskland og okkuperte land. Siden har andre overgrep og annen urett preget utviklingen av rettighetene. Normene er i dag like relevante for velfungerende demokratier som for stater med grove og systematiske brudd på rettighetene.

Menneskerettighetene tar utgangspunkt i at hvert enkelt menneske har et sett av grunnleggende rettigheter og friheter. Disse rettighetene og frihetene skal være med på å utvikle frie, selvstendige individer som bidrar positivt i samfunnet. En underliggende tanke er at dette igjen skal hindre at nye kriger og samfunnskollapser oppstår.

Ansvarsfordelingen på menneskerettighetsfeltet er enkel: Individene er rettighetshavere, mens forpliktelsene påhviler staten. Forpliktelsene innebærer at staten både skal avstå fra krenkelser av den enkelte borger og bidra til at rettighetene oppfylles. Retten til liv kan tjene som eksempel: Staten skal ikke ta liv, og den skal samtidig etablere politi, rettsvesen og grunnleggende helsetilbud som bidrar til at liv ikke berøves.

Menneskerettigheter har relevans for håndtering av digital sårbarhet i ulike sammenhenger, både langs en negativ og langs en positiv akse. Om myndighetenes intensjoner er aldri så gode, kan krenkelser oppstå. Det er derfor viktig at de ulike tiltakene som blir foreslått, vurderes opp mot menneskerettighetene og i samsvar med kravene i Utredningsinstruksen kapittel 2.3.2.[5] Det er

[4] LOV-1999-05-21-30 *Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven)*.

[5] Instruksen ble fastsatt ved kongelig resolusjon 18. februar 2000 og revidert ved kongelig resolusjon 24. juni 2005.

laget en veileder til Utredningsinstruksen som stiller krav til «vurdering av personvernkonsekvenser». Dette kravet er særlig aktuelt i forbindelse med den økte digitale innsamlingen og bruken av personopplysninger. Det sentrale vurderingstemaet er om rettigheter krenkes eller ikke i de konkrete enkeltsakene, ikke om det er formelle ordninger på plass.

Selv om koblingene er mange og viktige, er det ikke opplagt at menneskerettighetsspørsmål blir behandlet grundig når sårbarhet drøftes. Eksempelvis er ordet *menneskerettighet* bare benyttet én gang i 22. juli-kommisjonens rapport (NOU 2014: 14). Dette betyr ikke nødvendigvis at tilsvarende eller lignende vurderinger ikke er gjort, men det er vesentlig at slike vurderinger forankres i de internasjonale normene, og at vurderingene synliggjøres. Dette vil sikre grundigere faglige analyser, og både vurderingene og konklusjonene kan lettere være gjenstand for rettslig og/eller demokratisk kontroll.

I det følgende skal vi se på noen sentrale menneskerettigheter og hvilken betydning håndteringen av digital sårbarhet kan ha for disse.

3.2.1 Retten til liv

Retten til liv kan kobles med digital sårbarhet på ulike vis. I ekstreme situasjoner vil manglende sikring av personopplysninger kunne ramme den enkeltes rett til liv, slik de norske registrene over jøder under andre verdenskrig åpnet for uttransportering til dødsleirer i Tyskland. Svikt i digitale systemer kan også resultere i unødvendige dødsfall, for eksempel der styringssystemer for flytrafikk svikter, eller når en situasjon som togulykken ved Åsta oppstår. Det kan også vurderes om mangelfull eller svak overvåking i saker om terror og massiv kriminalitet kan krenke retten til liv, som ved Breiviks angrep i Oslo og på Utøya eller Nokas-ranet i Stavanger, jf. for eksempel NOU 2014: 14. Gjørv-kommisjonen trekker frem denne problemstillingen og et eventuelt behov for at PST må «få tilgang til effektive metoder også innenfor IKT-basert informasjonsinnhenting, knyttet til de konkrete sakene hvor det foreligger et reelt behov for å undersøke om noen er i ferd med å planlegge et terrorangrep».

Retten til liv kan også pålegge myndighetene å bruke digitale løsninger på en bedre måte. Et eksempel er pasientinformasjon, der problemstillingen like gjerne er beskyttelse av personsensitiv informasjon som en mulig plikt for myndighetene til å iverksette bedre og raskere informasjonsflyt, for eksempel om blodtype eller medisinbruk for skadde i trafikkulykker. Utviklingen går fort, og når det for eksempel finnes løsninger utviklet av bilprodusenter for automatisk varsling av bilulykker, kan også staten bli ansvarlig.

3.2.2 Retten til privatliv

Retten til respekt for privatlivet, inkludert familie, hjem og korrespondanse, er en menneskerettighet som favner vidt. Menneskerettighetenes definisjon av privatliv omfatter også personvern, jf. neste avsnitt. Dermed er det mange koblinger til digital sårbarhet og samfunnets håndtering av dette. For eksempel vil det være aktuelt og nødvendig å vurdere ulike typer digital overvåking opp mot menneskerettighetene. Eksempler kan være manipulering av nettbaserte kameraer, alarmsystemer, mobile enheter og smart-TV. Tilsvarende avveininger må foretas for bruk av digitale løsninger til kontroll av kommunikasjon, som e-postprogrammer og bildedelingstjenester jf. også NOU 2014: 14, side 390 og videre.

En annen type problemstilling kan være behov for varsling av befolkningen og retten til privatliv. Ved behov for varsling av befolkningen, for eksempel ved spesielt risikoutsatte områder, er det etablert og vurderes etablert varsling av befolkningen via SMS. Slike tiltak fra offentlige myndigheters side kan anses som et tiltak for å beskytte innbyggernes liv, helse og hjem, som alle er godt etablerte menneskerettigheter. Men en effektiv SMS-varsling innebærer også avveininger og problemstillinger, som for eksempel individuell sporingsmulighet.

3.2.3 Rett til vern om personlige opplysninger

I den europeiske menneskerettighetskonvensjonen (EMK) artikkel 8 understrekes enkeltindividets krav på å ha en beskyttet privatsfære, og dette er fundamentet for EUs regulering av personopplysninger i direktiv 95/46 EF. Direktivet ligger til grunn for den norske personopplysningsloven, og det er tilnærmet likelydende lovgivning i de øvrige europeiske landene innenfor EU- og EØS-samarbeidet. Personvern er i menneskerettslig forstand en del av retten til respekt for privatlivet. Personvern er ikke et helt presist begrep, men i digital sammenheng siktes det til den enkeltes rett til og reelle mulighet til både å ha kunnskap om og rådighet over bruken av egne personopplysninger. I personopplysningsloven er personopplysninger definert som «opplysninger og vurderinger som kan knyttes til en enkeltperson».

Personopplysningsloven regulerer enhver bruk av personopplysninger, det være seg innsamling, lagring, prosessering, videreformidling, salg m.fl.

Mange personopplysninger er i seg selv alminnelige og lite sensitive, men kan likevel gi omfattende informasjon om den enkelte dersom de kobles sammen. Andre personopplysninger, som for eksempel om DNA, er i seg selv både omfattende og sensitive. Det er åpenbart at både den enkelte og samfunnet vil ha nytte av at mange personopplysninger er lett tilgjengelige, for eksempel ligningsopplysninger, blodtyper og allergier, men denne nytten må veies opp mot faktorer som enkeltindividets råderett, fare for misbruk, regulering av overskuddsinformasjon, og så videre.

Koblingene mellom personvern og digital sårbarhet er mange. Her skal det nevnes at to fundamentalt ulike perspektiver ofte preger denne debatten: Det ene er at retten til selv å råde over sine personopplysninger er nær sagt ukrenkelig, det andre at myndighetene bør få tilgang til flest mulige personopplysninger for å beskytte samfunnet og enkeltindividene. I en menneskerettslig kontekst kan det første synspunktet sies å bygge på retten til privatliv, mens det andre bygger på retten til liv og helbred. Snowden-saken illustrerer dette spennet. Hans avsløringer av den massive overvåkingen fra amerikanske myndigheters side, særlig etter 11. september, oppfattes av mange som et helt uforholdsmessig og massivt inngrep i personvernet, og mange gir ham sin støtte. Andre mener at avsløringene bidrar til å hindre at myndighetene kan sikre liv og helse i USA.

EUs datalagringsdirektiv er et lignende eksempel. Direktivet ble vedtatt med henvisning til behovet for å styrke innsatsen mot terrorisme og organisert kriminalitet, men ble siden opphevet av EU-domstolen. Domstolen slo fast at direktivet på en særlig alvorlig måte åpnet for inngrep i privatlivet og beskyttelse av private data. Selv om direktivet fremmet visse samfunnsbehov, var det ikke tilstrekkelig proporsjonalitet mellom inngrepene og de målene som skulle fremmes. Domstolen fremhevet at inngrepene gikk utover det som var strengt nødvendig for å nå formålene. Ett av momentene i avgjørelsen var at det ikke var etablert tilstrekkelig beskyttelse mot misbruk.

3.2.4 Retten til frie ytringer

En viktig forutsetning for reell ytringsfrihet er tilgang til effektive kommunikasjonskanaler. Retten til å ytre seg og til å motta informasjon er i stor grad knyttet til digitale løsninger. Trykte aviser erstattes mer og mer av Internett-baserte aviser, og trykte bøker erstattes av e-bøker. Film og musikk «strømmes» via Internett og erstatter fysiske medier. En parallell og viktig utvikling er at ytringsfrihet flyttes fra etablerte mediehus med profesjonelle journalister og redaktører over til enkeltpersoner som benytter kommunikasjonskanalene direkte, uten mellomledd. Vanlige blogger, men også øyevitneobservasjoner og bildeopptak fra ulykker eller demonstrasjoner, er eksempler på det.

Når ytringsfriheten gjøres avhengig av digitale løsninger, har myndighetene et ansvar for å sikre at de digitale tjenestetilbudene er innrettet slik at rettighetene kan realiseres. Tilbudene må ha tilstrekkelig kapasitet og driftssikkerhet, slik at de ikke kollapser ved viktige samfunnshendelser, og de må være trygge nok til å hindre manipulering fra eksterne, slik at for eksempel journalister kan legge til grunn at den offentlige informasjonen er gyldig. Gitt at digital kommunikasjon er viktig for samfunnet og demokratiet, kreves det at myndighetene må regulere og styre markedet, slik at det ikke er private tilbyderes posisjon som avgjør hvor grensene for ytringsfrihet går, ved bruk av sensur og styring av sosiale medier. Befolkningen, individer og organisasjoner må ha berettiget tillit til tjenestene de bruker for sine ytringer. I motsatt fall vil vi se en nedkjølingseffekt som begrenser ytringsfriheten ved for eksempel lagring og videre analyse av informasjon på Google, ved at andre lands myndigheter kan overvåke befolkningen, jf. Snowden-saken, eller ved at journalister frykter at overvåkingstjenester får tilgang til kildene deres. Den digitale sårbarheten innenfor ytringsfrihetsfeltet favner altså vidt.

Ytringsfrihetskommisjonens NOU 1999: 27[6] oppsummerte politisk og personlig frihet til å omfatte tre elementer: sannhetsprinsippet om at bedre innsikt bare kan nås gjennom meningsutveksling der fremsatte påstander kan korrigeres i konfrontasjon med andre meninger, autonomiprinsippet om at vi fritt kan teste ut våre tanker, utdype og drøfte dem med andre uten kontrollører, og demokratiprinsippet om offentlig meningsutveksling. Realiseringen av disse tre prinsippene og ytringsfrihet forutsetter et skille mellom ytringer i det offentlige rom og ytringer i det private rom. Kommisjonen skrev også:

> «Man kan bare utvikles som menneske ved at man har et rom der man kan føle seg fri fra å måtte stå til ansvar for hva man sier eller gjør overfor ytre, ukjente kontrollører. Den offent-

[6] NOU 1999: 27 *Ytringsfrihed bør finde Sted*.

lige samtale i et fritt samfunn har sitt utgangspunkt i slike fri og utvungne prosesser, den springer frem fra den beskyttede privatsfære.»

3.2.5 Forsamlingsfrihet

Forsamlingsfriheten er en sentral rettighet for å sikre og videreutvikle demokratiet. De siste års utvikling av IKT har påvirket denne rettigheten særlig i to henseender: det ene er at informasjon om grupperinger og organisasjoner spres via Internett, det andre at IKT-plattformer benyttes som forsamlingsarenaer, for eksempel som erstatning for møter og demonstrasjoner på offentlige torg, i parker og i gater.

Sikkerhetstiltak som har som formål å redusere digital sårbarhet, kan ha betydning for forsamlingsfriheten i ulike sammenhenger. Det ene og åpenbare er systematisk individuell overvåking eller masseovervåking som IKT-løsninger åpner for, slik at myndigheter og andre kan skaffe seg informasjon om hvem som har deltatt i forsamlingene, og når. Men det er også muligheter for manipulering av invitasjoner, utestenging av aktører fra IKT-nettverk, tjenestenekt med mer. Mye av dette er kjente eksempler fra forsamlingsarbeid under og etter den arabiske våren.

Myndighetenes ansvar kan være relatert til at de selv gjør inngrep, eller til at de ikke i stor nok grad sikrer beskyttelse og realisering av rettigheten ved for eksempel å tillate private tjenestemonopolordninger, eller ved at de ikke stiller strenge nok krav til stabil infrastruktur, at det ikke er etablert hindre for diskriminering eller utestenging av tjenester, og så videre.

3.3 Menneskerettighetsbrudd

Håndtering av digital sårbarhet henger sammen med menneskerettigheter, men ikke alle situasjoner omfattes av menneskerettighetsvernet. Før man kan ta stilling til om en situasjon reguleres av en rettighet eller ikke, kreves det ofte omfattende juridiske vurderinger. De ulike rettighetene utgjør også en helhet, slik at ett enkelt forhold kan omfatte ulike rettigheter. Det blir dermed ofte en avveining av rettighetene mot hverandre, der vekten av de ulike interessene og argumentene avgjør utfallet.

Selv i situasjoner der det er klart at myndighetene gjør inngrep i rettighetene, kan dette ofte forsvares gjennom den såkalte inngrepshjemmelen. Eksempelvis vil individer måtte tåle inngrep i sitt privatliv dersom myndighetene har behov for å overvåke dem for å hindre omfattende samfunnsskade. Slike inngrep er lovlige bare dersom de tre følgende vilkårene er oppfylt: (1) at det finnes hjemmel/rettsgrunnlag, (2) at inngrepet søker å nå visse oppsatte formål, og (3) at det er nødvendig i et demokratisk samfunn.

Det er særlig vilkåret om at inngrepet skal være nødvendig i et demokratisk samfunn, som kan være vanskelig å oppfylle. Dette kravet er i noen grad presisert gjennom en lang rekke dommer avsagt av Den europeiske menneskerettighetsdomstolen.[7] Ett delkrav knytter seg til proporsjonalitet mellom mål og middel. Proporsjonalitetskravet, eller forholdsmessighetskravet, som det også kalles, åpner for en helt konkret balansering av nødvendigheten av hensyn som taler for inngrep og hensyn som taler for å sikre den enkeltes rettigheter.

Domstolene vil her kreve at det er utredet alternative løsninger, og at det minst inngripende tiltaket velges der det finnes reelle valgmuligheter. Det er bare inngrep som kommer av et presserende samfunnsbehov, som blir akseptert. Det holder dermed ikke å forsvare inngrep med at de er effektive, lønnsomme, enkle å iverksette eller lignende. Domstolene vil også kreve at myndighetenes begrunnelse for inngrepet er relevant og tilstrekkelig. Relevansen går tilbake til interesseavveiningen: De argumentene som benyttes, må ha reell betydning i den beslutningskjeden som leder frem til at inngrepet iverksettes. Tilsvarende er det med kravet om at argumentene skal være tilstrekkelige: Det holder ikke at de angir en ønsket retning, og de må ikke være fremstilt ufullstendig. Her stilles det strenge krav til lovgiveren, men ikke minst til forvaltningen: Det er ikke tilstrekkelig å si at en konkret løsning har «de beste grunner» eller at «man etter en totalvurdering konkluderer med» denne løsningen. Det er dermed ikke bare en prøving av resultatet, men også av argumentasjonskjeden, som har ledet frem til resultatet.

Det spiller også inn hvilke kontroll- og sikringsmekanismer som er iverksatt. Disse mekanismene prøves helt konkret mot det konkrete inngrepet og effekten det har for den enkelte. Videre har det betydning hvor bredt tiltakene rammer, for eksempel målt opp mot antall personer og hva slags situasjoner som dekkes, eller hvor lenge tiltakene er ment å vare. Jo mer avgrenset og presist inngrepet er, jo enklere er det for myndighetene å forsvare det. Særlig innen

[7] Se punkt 10.3 «Menneskerettslige skranker for informasjonsinnhenting» som viser til rettspraksis fra EMD.

IKT-reguleringer er dette siste argumentet viktig, slik det også ble vist i EU-domstolens behandling av saken om datalagringsdirektivet.

Myndighetene har en viss skjønnsmargin i sin forvaltning, men i siste instans er det domstolene som avgjør hvor langt denne går. Skjønnsmarginen vil variere over tid og med de interessene og rettighetene som prøves. Domstolene vil typisk gå dypere inn i saker som er typisk rettslige (som kvaliteten på lovhjemmelen og sikrings- og kontrollmekanismer), enn saker som har mer med politikk og etikk å gjøre. Den nasjonale skjønnsmarginen farges også av situasjonen i sammenlignbare land. Eksempelvis vil Den europeiske menneskerettighetsdomstolen se hen til andre lands praksis, og de henter ofte inn komparative analyser i sine avgjørelser. I flere saker om inngrep i privatliv og ytringsfrihet har Den europeiske menneskerettighetsdomstolen lagt til grunn at statene har en mer begrenset skjønnsmargin når det gjelder disse rettighetene.

I særlige tilfeller kan statene gjennom derogasjon[8] gjøre generelle inngrep i menneskerettslige forpliktelser utover det som følger av den individuelle inngrepshjemmelen. Vilkårene etter for eksempel EMK artikkel 15 er svært strenge – artikkelen kan kun påberopes under «krig eller annen offentlig nødstilstand som truer nasjonens sikkerhet» – men bestemmelsen vil kunne være aktuell i flere av de situasjonene som denne meldingen omhandler. Det skal også sies at enkelte rettigheter har et absolutt vern mot inngrep/derogasjon.

Inngrepshjemmel og derogasjon sier noe om hvordan myndighetene kan beskjære menneskerettighetene for å fremme andre interesser. Vel så viktig er det å ha det perspektivet at myndighetene også har en positiv plikt til å bidra til å realisere menneskerettigheter. Her vil det ofte være spørsmål om tilgang til ressurser som slår inn: Har man råd til å etablere så trygge løsninger som ønskelig for å sikre gjennomføring av visse rettigheter? Evalueringene etter Åsta-ulykken, Nokasranet og 22. juli viser at det også er et annet spørsmål som kommer inn, og som kan være avgjørende: Er det tilstrekkelig bevissthet, årvåkenhet og planleggingsevne i samfunnet og hos myndighetene om disse spørsmålene?

---

8 «Derogasjon» betyr: adgang til å fravike de rettslige forpliktelsene, utover konvensjonens egne regler om unntak fra forpliktelsene.

Kapittel 4
Hva er digitale sårbarheter?

4.1 Sårbarhetsbegrepet

Sårbarhetsbegrepet står sentralt i denne utredningen. Sårbarhetsutvalget definerte sårbarhet som

> «et 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».[1]

Å gjenoppta sin virksomhet handler om at systemet igjen kan ivareta sine oppgaver, men ikke nødvendigvis på nøyaktig samme måte som før. Det er et mål at gjenopprettingen skjer på en måte som gjør systemet mer robust, slik at lignende hendelser kan tåles i fremtiden. Robusthet er et uttrykk for den motstandskraft et system har mot en uønsket hendelse, samt den evne systemet har til å gjenoppta sin virksomhet etter at hendelsen har inntruffet.

Uønskede hendelser kan være både tilsiktede og utilsiktede. En tilsiktet hendelse er forårsaket av en aktør som gjennom målrettede handlinger utløser den uønskede hendelsen. En utilsiktet hendelse kan skyldes værfenomener, jordskjelv og systemsvikt, eller den kan være forårsaket av uhell, uforsiktighet eller uvitenhet.

Lysneutvalgets arbeid har omfattet å se på digitale sårbarheter på flere nivåer av systemer:

1. Sårbarheter som knyttes direkte til IKT-systemer, både logiske og fysiske feil. Slike sårbarheter kjennetegnes ved svakheter, feildesign eller feilimplementering.
2. Sårbarheter i selve samfunnsfunksjonene som er forårsaket av svikt i IKT-systemer, og ved at svakheter arves av feil i IKT-systemer.

Den sårbarheten som samfunnet står overfor til enhver tid, faller i én av to kategorier:

1. Sårbarheter som er kjent og akseptert fordi det blir vurdert at kostnadene ved de aktuelle tiltakene ikke står i forhold til skadepotensialet, trusselen eller verdien.
2. Sårbarheter som ikke blir gjenstand for tiltak fordi sårbarheten enten er ukjent, feilvurdert, ikke forstått eller mangelfullt kommunisert.

Restsårbarhet er et begrep som beskriver den sårbarheten man sitter igjen med etter at sårbarhetsreduserende tiltak er gjennomført. Utvalget mener det er de sårbarhetene som ikke er erkjent, som utfordrer oss både som samfunn og som enkeltmennesker. Utvalget er av den oppfatning at ukjente, feilvurderte, ikke forståtte eller mangelfullt kommuniserte sårbarheter er et spesielt omfattende problem innenfor de digitale sårbarhetene.

Denne utredningen omhandler digitale sårbarheter som ligger i grenseflatene mellom digital informasjonsbehandling, digital kommunikasjon og digital styring. Eksempler på digital styring er kontroll av adgang, lys, varme og ventilasjon i bygg, førerstøtte i transportmidler, regulering av trafikk og kontroll med infrastruktur som strøm- og vannforsyning.

Dagens IKT-systemer er fremdeles umodne, og risikoen for at uvedkommende får innsyn i sensitiv informasjon, har økt i takt med digitaliseringen. Det er fremdeles mangelfulle mekanismer for å bekrefte identitet over digitale kommunikasjonskanaler, og teknologiens interaksjon med fysiske prosesser blir allerede misbrukt for å utføre sabotasje, for eksempel ved tilsiktet overbelastning som medfører fysisk skade.

4.2 Verdivurdering

Verdivurdering handler om å etablere en oversikt over de verdiene som finnes.[2] I verdivurderinger identifiseres verdier, og man forsøker å estimere

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

[2] NSM (2015): *Sikkerhetsfaglig råd 2015.*

skade som uønskede hendelser kan få for verdiene. Utfordringene knyttet til verdivurderinger blir tydelige når informasjon i og avhengigheten av IKT-utstyret skal vurderes.

Verdibegrepet, slik det er benyttet i denne utredningen, bidrar til å identifisere hvilke kritiske samfunnsfunksjoner det er viktigst å opprettholde.

Bortfall av IKT-tjenester kan i løpet av kort tid føre til store tap i produktivitet og inntjening. Det kan være svært kostbart å gjenskape informasjon dersom den går tapt. Informasjon som kommer i gale hender, kan gi utslag i negativt omdømme, i tillegg til store skader for kunder dersom det er snakk om sensitive personopplysninger.

Å verdivurdere det som er eksponert for sårbarheter, viser seg i mange tilfeller å være svært komplisert. Internasjonal litteratur indikerer at digitale trusler er spesielt vanskelig å kvantifisere, i særlig grad gjelder dette trusselen fra tilsiktede handlinger.[3] [4] [5] Verdikjeder med komplekse avhengigheter på tvers av sektorer og virksomheter gjør det vanskelig å kartlegge omfanget av verdier som er eksponert for sårbarheter. NSM har utgitt veiledning i verdivurdering.[6]

4.3 Trussel og fare

Trussel kan defineres som «en mulig årsak til en uønsket hendelse».[7] Begrepet brukes både om kapasitet og intensjon til å gjennomføre skadelige handlinger og til å beskrive faren ved konsekvensene av utilsiktede hendelser.[8] I norsk straffelov brukes trusselbegrepet om aggressive ord eller handlinger. NSM beskriver begrepet trussel som en tilsiktet uønsket handling.[9]

Fare er i norske standarder definert som «handling eller forhold som kan føre til en uønsket hendelse».[10] NSM beskriver fare som en utilsiktet uønsket hendelse.

4.4 Risikovurdering

Formålet med risikovurderinger er å prioritere begrensede ressurser i arbeidet med å oppnå ønsket sikkerhetsnivå. Iverksatte tiltak kan være forebyggende, det vil si at de reduserer sannsynligheten for at en uønsket hendelse skal skje. Tiltak kan også være konsekvensreduserende, noe som innebærer at de minimerer konsekvensene i etterkant av en uønsket hendelse. Tilnærmingen til risikobegrepet avhenger av hvilket fagmiljø man kommer fra, og formålet med risikovurderingen.

Risiko kan uttrykkes som en kombinasjon av sannsynligheten for og konsekvensen av en uønsket hendelse.[11] Metoden har god forankring i bruksområder rettet mot utilsiktede hendelser. Risiko kan også uttrykkes som forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen.[12] Trusselen blir estimert basert på vurderinger av trusselaktørens kapasitet, evne og vilje til å påføre skade. Denne fremgangsmåten benyttes mot tilsiktede uønskede handlinger der man må forholde seg til en strategisk og kalkulerende trusselaktør som er i stand til å tilpasse seg sikringstiltak og endrede rammebetingelser.

FFI har utgitt en rapport der de sammenligner disse to standardene for risikovurdering.[13] FFI konkluderer i sin rapport med at tilnærmingene har mange likhetstrekk, og at forskjellen hovedsakelig ligger i hvorvidt sannsynlighetsvurderingen er eksplisitt eller implisitt. I rapporten skriver de at begge modellene har svakheter knyttet til hvordan de kommuniserer usikkerheten knyttet til risikoen, og at det verken nasjonalt eller internasjonalt eksisterer en beste fremgangsmåte for å vurdere tilsiktede uønskede hendelser.

---

3 Biener, Christian; Martin, Eling og Jan Hendrik Wirfs (2015): *«Insurability of Cyber Risk: An Empirical Analysis». The Geneva Papers on Risk and Insurance-Issues and Practice* 40.1 s. 131–158.

4 ENISA (2012): *Incentives and barriers for the cyber insurance market in Europe.* I rapporten blir det dokumentert at usikkerhet knyttet til vurderingen av hvilke verdier som skal forsikres, er et av de største hindrene for utvikling av et velfungerende forsikringsmarked.

5 World Economic Forum (2015): *Partnering for Cyber Resilience, Towards the Quantification of Cyber Threats.* En hovedobservasjon i denne rapporten er at det internasjonale samfunnet mangler en felles metodikk for å kvantifisere cybertrusler og tilhørende verdier.

6 NSM (2009): *Veiledning i verdivurdering.*

7 NS-ISO 22300:2012 *«Samfunnssikkerhet – terminologi». Oversatt fra «Potential cause of an unwanted incident, which can result in harm to individuals, a system or organization, the environment or the community».*

8 NOU 2006: 6 *Når sikkerheten er viktigst — Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*, s. 36.

9 NSM (2015): *Helhetlig IKT-risikobilde 2015.*

10 NS 5814:2008.

11 Ibid.

12 NS 5832:2014.

13 Forsvarets forskningsinstitutt (2015): FFI-rapport 2015/00923 *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger. Om Forsvarsbyggs operasjonalisering av NS 5814:2008 og NS 5832:2014.*

Disse begrepene eller nært beslektede begreper finner man igjen i standarder og mønsterpraksisdokumenter fra ENISA[14] og World Economic Forum.[15] [16] I ISO 27005 defineres risiko som «potensialet for at en gitt trussel vil utnytte sårbarhetene til et sett av verdier og derigjennom å forårsake skade».

[14] ENISA (2012): *ENISA Threat landscape 2012.* Begrepene benyttes også i Threat landscape-rapportene fra 2013 og 2014, men de defineres i rapporten fra 2012.

[15] World Economic Forum (2012): *Risk and responsibility in a Hyperconnected world – pathways to global cyber resilience.*

[16] World Economic Forum (2015): *Partnering for Cyber Resilience – Towards the quantification of cyber threats.*

Kapittel 5
Sikring av IKT og digital informasjon

5.1 Hva er IKT-sikkerhet?

Ulike begreper blir brukt om det digitale sikkerhetsarbeidet, blant annet *informasjonssikkerhet*, *IKT-sikkerhet* og *cybersikkerhet*. I Norge er begrepene brukt om hverandre de siste årene. I den nasjonale strategien på området utgitt i 2012[1] brukes begrepet *informasjonssikkerhet*. Informasjonssikkerhetsbegrepet handler om sikring av informasjon, uavhengig av om den er digital eller analog. I kongelig resolusjon av 2013[2] er begrepet *IKT-sikkerhet* brukt. I Forsvarsdepartementets cyberretningslinjer fra 2014 benyttes begrepet *cybersikkerhet*. Internasjonalt brukes også ofte begrepet *cybersikkerhet*, der *cyber* henviser til alt cyberdomenet består av – datasystemer og kommunikasjonsinfrastruktur, i tillegg til informasjonen som lagres og overføres. Cybersikkerhet handler derfor om å beskytte «alt» som er sårbart fordi det er koblet til, eller på annen måte er avhengig av informasjon- og kommunikasjonsteknologi.

En svensk offentlig utredning fra 2015 tillegger *cybersikkerhet* en mer internasjonal strategisk betydning, mens *informasjonssikkerhet* henviser til teknisk beskyttelse og standardisering:

> «Cybersäkerhetsbegreppet är mer strategiskt och fokuserar mer på nationella och internationella nätverk. Därmed har cybersäkerhet en större internationell räckvidd med t.ex. folkrättsliga frågeställningar och normer på cyberområdet än det mer tekniska informationssäkerhetsbegreppet. Det senare har en större tyngdpunkt mot hård- och mjukvara samt standardisering.»[3]

Utvalget benytter i denne NOU-en begrepet *IKT-sikkerhet*, og legger til grunn hele spekteret av digitale sårbarheter (se punkt 4.1 «Sårbarhetsbegrepet»). Videre legger utvalget til grunn at IKT-sikkerhet er synonymt med cybersikkerhet.

Sikkerhet innebærer beskyttelse mot farer og trusler som kan forårsake uønskede hendelser. Høy grad av sikkerhet gir en trygghetsfølelse, og i noen situasjoner kan følelsen av trygghet være vel så avgjørende som det objektive sikkerhetsnivået, selv om disse ikke nødvendigvis er sterkt korrelert med hverandre.

IKT-sikkerhet handler om å beskytte IKT og informasjonen i informasjonssystemer mot uønskede hendelser. Spørsmålet er så hvilke målsettinger – sikkerhetsmål – vi har når vi sikrer oss. De tre mest kjente er konfidensialitet, tilgjengelighet og integritet. Utvalget legger til grunn en vid forståelse av de tre begrepene, men understreker at disse ikke gir et komplett bilde.

Konfidensialitet innebærer beskyttelse mot at informasjon blir kjent for uvedkommende, og dermed at bare de vi gir lov til å se informasjonen, faktisk får se den. Det er verdt å merke seg at konfidensialitetsbrudd i praksis er uopprettelige i det digitale domenet. Et eksempel på konfidensialitetsbrudd er hackingen av SnapSave, som førte til at private bilder og videoer ble spredt på diverse fildelingsnettverk i 2014.

Tilgjengelighet innebærer at informasjon og tjenester er tilgjengelige når de trengs. For noen år siden, da Norge startet med digitale selvangivelser, var det mange som frustrert ble møtt med at tjenesten ikke var tilgjengelig rett etter at selvangivelsen ble sluppet. Tjeneren hadde ikke ressurser til å håndtere tilstrekkelig antall samtidige oppkoblinger, og dermed klarte den ikke å levere tjenesten til alle. Dette er et eksempel på utilsiktet tjenestenekt. Et annet eksempel er sanntidsoverføring av lyd og bilde, som IP-telefon og videokon-

---

1 Fornyings- og administrasjonsdepartementet, Samferdselsdepartementet, Justis- og beredskapsdepartementet og Forsvarsdepartementet (2012): *Nasjonal strategi for informasjonssikkerhet.*

2 Statsministerens kontor (2013): *Overføring av samordningsansvaret for forebyggende IKT-sikkerhet fra Fornyings-, administrasjons- og kirkedepartementet til Justis- og beredskapsdepartementet.* Kgl. res. 22.03.2013.

3 SOU 2015: 23 *Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten,* punkt 2.4 «klargörande av begrepp».

feranser. Det ligger i designet til Internett at datatrafikk mellom to punkter kan forsvinne underveis dersom det er stor belastning på nettet. Dette opplever vi som uklar lyd og hakkete bilde.

Integritet innebærer at informasjon er til å stole på, og at systemer og tjenester fungerer slik det er tenkt. Informasjonen skal være korrekt og gyldig. Bare de som har lov til å endre informasjonen, får endret den. Relatert til integritet har vi *autentisitet*, som handler om å sikre opphavet til informasjonen, for eksempel bekrefte identiteten til en sendt melding. Nært relatert har vi også *ikke-fornekting* (non-repudiation), som handler om at en digital handling ikke skal kunne benektes i etterkant. Innen digital kontraktsinngåelse ønsker man for eksempel ikke en situasjon der motparten kan fornekte en signert kontrakt i ettertid. Det er mange eksempler på områder der vi er avhengige av at informasjonen er korrekt, blant annet transaksjoner og kontobalanser i finansnæringen, samt overvåkings- og styringssystemer for industriprosesser og regulering av luftfart. Et eksempel på integritetsbrudd er fra 2013, da utpressingsskadevaren CryptoLocker ble brukt for å presse ofre til å betale for å få tilgang til filene sine igjen. Rent teknisk var dette en ikke-ønsket – såkalt uautorisert – endring av informasjon som medfører at informasjonen ikke lenger er tilgjengelig. Uansett hvor store ressurser samfunnet legger i beskyttelsestiltak, må vi akseptere at vi ikke alltid vil være i stand til å oppfylle sikkerhetsmålene. Ved brudd på sikkerhetsmålene, eller ved sterk mistanke om brudd, sier vi at systemet har blitt *kompromittert*. Siden vi ikke kan beskytte oss fullstendig mot kompromittering, må vi ha mekanismer som lar oss rydde opp i ettertid og dermed minimere konsekvensene. For mange virksomheter innebærer slik gjenoppretting å reinstallere programvare i påvente av sikkerhetsoppdateringer fra eksterne leverandører. I andre situasjoner kan det være behov langt mer komplekse verifikasjons- og tilbakerullingsprosedyrer, samt endringer i konfigurasjon og rutiner.

Vi kan her trekke frem et fjerde sikkerhetsmål, kalt *sporbarhet*. Sporbarhet handler om å kunne finne ut hva som har skjedd, i etterkant, for eksempel hvem som har håndtert informasjonen, og hvor den har vært kommunisert. Typiske eksempler er tilgangslogger, endringslogger og andre typer hendelseslogger. Kompromittering av sporbarheten innebærer at det blir vanskelig eller umulig å etterforske i ettertid.

5.2 Motsetninger mellom sikkerhetsmål

Noen ganger er det også motsetninger mellom forskjellige sikkerhetsmål. Sensitiv informasjon kan «låses ned», deles med færrest mulig. På den måten oppnås høy grad av konfidensialitet. Ulempen er at tilgjengeligheten og dermed effektiviteten blir mindre. For eksempel vil det å jobbe i et høygradert IKT-system frakoblet Internett redusere angrepsflaten for dataspionasje, men samtidig gjøre det vanskeligere å kommunisere med omverdenen. Motsatt vil høy grad av tilgjengelighet øke sjansen for at informasjon kommer på avveie eller blir endret på en ukontrollert måte.

Informasjonssikkerhetsfeltet har tradisjonelt vært sterkt fokusert på konfidensialitet, det vil si hemmelighold av informasjon, men ofte kan integritet eller tilgjengelighet være viktigere. For eksempel er mye informasjon i samfunnet offentlig og kravene om konfidensialitet dermed små eller ikke-eksisterende. Det kan likevel ha store konsekvenser dersom informasjonen er feil eller utilgjengelig.

Uttrykket «need to know» handler om at bare de som virkelig trenger informasjonen, bør få tilgang til den. Som et motstykke har begrepet «need to share» oppstått. Tanken bak det er at skadepotensialet ved at allierte mangler kritisk informasjon, kan være større enn om uvedkommende får kjennskap til informasjonen. I militært internasjonalt samarbeid er det eksempler på at liv har gått tapt fordi avgjørende informasjon ikke har kunnet deles. En relatert situasjon har vi ved håndtering av IKT-hendelser der deling av klausulert etterretningsinformasjon potensielt kunne ha avverget nye IKT-innbrudd, men der strategiske hensyn har veid tyngst.

5.3 Sikkerhetsnivå og risikoaksept

Et spørsmål som ofte blir stilt, er om et system er sikkert. Sikkerhet handler om at vi vil oppnå sikkerhetsmål, som blant annet konfidensialitet, integritet, tilgjengelighet og sporbarhet.

Men sikkerhet handler også om hva og hvem vi ønsker å beskytte oss mot. Vi må ta stilling til hva og hvem vi ønsker å beskytte oss mot. Er det tilfeldige feil og svikt? Er det nysgjerrige naboer og teknologisk kyndige tenåringer? Eller er det utro tjenere, organiserte kriminelle og fremmede stater?

Hvilket sikkerhetsnivå som er nødvendig for det aktuelle systemet eller tjenesten, kan vi først

avgjøre etter å ha gjennomført en risikovurdering. For å kunne vurdere hvilket sikkerhetsnivå en tjeneste eller et system har behov for, må vi se på helheten, og ikke bare tekniske forhold, men også miljøet systemet eksisterer i, og hvilke trusler og farer vi ønsker å beskytte oss mot.[4]

For å eksemplifisere kan vi vise til anonymiseringsnettverket The Onion Router (TOR). Formålet med TOR er å skjule egen identitet ved kommunikasjon via Internett. Sammen med noen forholdsvis enkle tiltak gir TOR beskyttelse mot en del trusler, som at Internett-tilbyderen din avlytter deg. Dersom du prøver å beskytte deg mot aktører som har kontroll over store deler av Internettinfrastrukturen, slik enkelte nasjonstater har, finnes det flere måter å bryte anonymitetsbeskyttelsen TOR gir.

Etter å ha foretatt en risikovurdering og definert et sikkerhetsnivå vil det alltid kunne være en restrisiko. En målsetting kan være å ha en oversikt over den konkrete restrisikoen, slik at prioriteringen mellom tiltak blir så hensiktsmessig som mulig. Kriterier for risikoaksept er verbale eller tallfestede uttrykk som setter grenser for hvilken risiko som er akseptabel eller ønskelig. Uakseptabel risiko krever tiltak. Å ha kriterier for risikoaksept betyr ikke at en aksepterer at en ulykkeshendelse inntreffer, men innebærer en erkjennelse av at en ikke kan fjerne all risiko, og at en må prioritere mellom ulike gode risikoreduserende tiltak. Å kunne gjøre gode prioriteringer mellom tiltak kan imidlertid være en ambisiøs målsetting, ikke minst fordi det vil være mange ukjente og usikre størrelser i en slik vurdering. Usikkerheten i nytte–kostnads-vurderinger vil være ekstra stor fordi det også vil være usikkerhet knyttet til sannsynligheten for at den hendelsen man ønsker å forebygge eller ha beredskap mot, faktisk inntreffer, eller ville ha inntruffet dersom tiltakene ikke ble gjennomført. En annen side ved dette er at samfunnets aksept av risiko kan være ulik fra område til område.

5.4 Noen sentrale IKT-sikkerhetstiltak

For å sikre IKT-systemer og digital informasjon har vi bygd opp en «verktøykasse» for å beskytte oss mot både utilsiktede og tilsiktede hendelser. Her gir vi en beskrivelse av de mest essensielle verktøyene vi har.

5.4.1 Menneskelige og organisatoriske sikkerhetstiltak

IKT-politikk, ledelse og rutiner handler om å regulere ønsket bruk av IKT-systemer og informasjonen i dem. Kjente mekanismer er utarbeidelse av strategier og risikovurderinger, lover og retningslinjer, god sikkerhetskultur, verdivurderinger, sikkerhetsgradering av informasjon, personellklarering, autorisasjon, godkjenning av systemer, avtalevilkår, brukerveiledninger og konfigurasjonskontroll. Rutiner rettet mot brukere kan håndteres både med og uten tekniske hjelpemidler. Merk at rutiner er skjøre sikkerhetstiltak når personalet kan omgå eller ignorere dem.

5.4.2 Preventive tekniske sikkerhetstiltak

Sikkerhetskopier og redundans. Sikkerhetskopier av data er kanskje det mest kjente sikkerhetstiltaket mot systemsvikt. Det finnes mange løsninger for sikkerhetskopiering på eksterne lagringsmedium, både lokalt og eksternt, for eksempel i skybaserte tjenester. Sikkerhetskopiløsninger kan være svært sårbare for tilsiktede hendelser. Det er flere eksempler på virus som sletter, krypterer eller endrer dokumenter, også på tilkoblede lagringsmedia. Løsninger som baserer seg på å speile data, vil da stå i fare for å erstatte sikkerhetskopier med infiserte versjoner. Sikkerhetskopier av data er en av flere former for redundans. Andre eksempler er alternative dataoverføringslinjer, reservedeler og ekstra strømforsyningsmuligheter. Det essensielle er at alternativene er uavhengige av hverandre.

Antivirus er en samlebetegnelse på dedikerte programmer som leter etter og forsøker å fjerne skadevare. Virus er en type skadevare, og navnet har sitt opphav i måten det biologiske viruset sprer seg på. Antivirus er ofte en form for svartelisting som innebærer at man oppretter en stor katalog med kjennetegn som skal blokkeres. En annen fremgangsmåte for å løse problemet kalles hvitlisting og innebærer å lage lister over hvilke programmer som skal få lov til å kjøre, mens alt annet blokkeres. Kontroll med hva som får kjøre på maskinvaren, håndheves ved hjelp av digitale signaturer.

Sikkerhetsoppdateringer («patching») består i å bytte ut gammel, sårbar programkode med ny programkode. Vi kan grovt skille mellom utvidelse av funksjonalitet og reparasjon av feil. Ny funksjonalitet er som regel det vi forbrukere spør etter, mens det sistnevnte – ofte kalt sikkerhetsoppdateringer – er det som gjør systemene sik-

[4] Direktoratet for forvaltning og IKT (2010): *Risikovurdering – en veiledning til Rammeverket for autentisering og uavvislighet i elektronisk kommunikasjon med og i offentlig sektor.*

rere. Det tar ofte lang tid fra sårbar programvare blir oppdaget, til en sikkerhetsoppdatering blir utviklet.[5] Dette kommer blant annet av kompleksitet i programvare, som gjør at nødvendige endringer kan få konsekvenser for annen funksjonalitet. Systemer der operative behov står sterkt, blir derfor ikke oppdatert uten at oppdateringene er forsvarlig testet. Manglende oppdateringer kan også skyldes uvitenhet og «latskap». Leverandører av programvare har derfor gradvis gått fra manuelle til helautomatiske oppdateringer, særlig for operativsystemer og nettlesere.

Ofte blir nye sårbarheter oppdaget ved at de benyttes i et angrep. Da eksisterer det naturligvis heller ingen «patch» (reparasjon) for sårbarheten. Vi kaller disse sårbarhetene for «zero-day» sårbarheter.

Programvare har ofte mange muligheter for konfigurasjon og innstillinger, og utgjør et potensial for sårbarheter som sikkerhetsoppdateringer sjelden retter. En særlig problemstilling her er standardinnstillingene til leverandøren, fordi disse normalt forblir uendret. Se boks 5.1.

Brannmur. En brannmur har som oppgave å blokkere uønsket nettverkstrafikk. Skallsikring er en tradisjonell sikkerhetstankegang og går ut på at man forsøker å plassere alt innenfor beskyttelsen av brannmurer. Skallsikring utfordres av alle måtene vi kobler ting sammen på, ved at det er blitt svært krevende å «holde skallet».[6] Alternative strategier er å dele nettverk inn i soner med egen skallsikring, transaksjonskontroll og ulike former for filtrering, samt å bygge moduler der hver enhet er ansvarlig for sin egen sikkerhet.

Boks 5.1 Slik stopper du 90 prosent av alle angrep[1]

1. Oppgrader program- og maskinvare.
2. Vær rask med installasjon av sikkerhetsoppdateringer, gjør det automatisk hvis mulig.
3. Ikke tildel sluttbrukere administratorrettigheter.
4. Blokker kjøring av ikke-autoriserte programmer.

[1] Nasjonal sikkerhetsmyndighet (2014): *Fire effektive tiltak mot dataangrep*.

I Internetts barndom var personlige brannmurer programvare vi på lik linje med antivirus måtte kjøpe separat. I dag har de mest kjente operativsystemene innebygd brannmur. Nettlesere og e-post utgjør i dag to sentrale punkter for introduksjon av skadevare. Når nettlesere laster inn nettsider, henter de også små programsekvenser fra mange steder på Internett, og disse kan være infisert. Det samme gjelder vedlegg og aktivt innhold i e-postmeldinger. Det finnes derfor mer spesialiserte former for blokkering, som for eksempel «script-blokkere» for nettlesere, og løsninger som ser etter virus i e-post under overføringen, før e-posten når frem til mottakeren.

Kryptografi. Det typiske kryptografiske problemet er to personer som ønsker å snakke sammen, men som også ønsker å beskytte seg mot avlytting. Tradisjonelt har kryptografi vært forbeholdt diplomatiet og militæret, men i løpet av de siste 50 årene har kryptografi blitt tatt i bruk av alle.

I klassisk bruk av kryptografi utveksler man først en hemmelig nøkkel. For å beskytte informasjonen man vil sende, brukes nøkkelen til å kryptere informasjonen. Resultatet er en chiffertekst som man sender til mottakeren. Mottakeren bruker nøkkelen til å dekryptere chifferteksten og kan så lese informasjonen. Uten nøkkelen er det i praksis umulig å trenge gjennom krypteringen for å lese den beskyttede informasjonen. Denne formen for kryptografi kalles ofte symmetrisk kryptografi, der ordet symmetrisk henspeiler på at det er symmetri i hvilke hemmelige nøkler man kjenner.

Det finnes nå en annen form for kryptografi, der de som skal kommunisere, ikke lenger trenger å forhåndsutveksle hemmelig informasjon. I stedet trenger man bare en sikker måte å utveksle offentlig kjent informasjon på. Dette kalles asymmetrisk kryptografi, siden de som skal kommunisere, ikke lenger kjenner de samme hemmelige nøklene.

Det mest kjente eksempelet på asymmetrisk kryptografi er såkalt offentlig-nøkkel-kryptering, der hver kommunikasjonspart har et såkalt nøkkelpar bestående av en offentlig krypteringsnøkkel og en hemmelig dekrypteringsnøkkel. Krypteringsnøkkelen er offentlig kjent og kan brukes av enhver til å kryptere informasjon som skal sendes til eieren av nøkkelparet. Dekrypteringsnøkkelen er hemmelig – uten den er det i praksis umulig å trenge gjennom krypteringen for å lese den beskyttede informasjonen.

Et annet eksempel på asymmetrisk kryptografi er digitale signaturer. Også her har hver kommunikasjonspart et nøkkelpar, som består av

[5] Se også punkt 5.5 «Utfordringer knyttet til programvareutvikling».

[6] Se også punkt 6.2.2 «Tingenes Internett» og punkt 6.4.3 «Bruk av privateid datautstyr i jobbsammenheng».

en hemmelig signeringsnøkkel og en offentlig verifiseringsnøkkel. Nå kan eieren av nøkkelparet bruke signeringsnøkkelen til å signere informasjon. Alle kan bruke verifiseringsnøkkelen til å sjekke at informasjonen kom fra eieren av nøkkelparet og ikke er endret etter signering. Uten signeringsnøkkelen er det i praksis umulig å endre eller forfalske signert informasjon.

Det er ikke slik at man bruker enten asymmetrisk eller symmetrisk kryptografi. Nesten alle moderne systemer bruker en blanding av asymmetrisk og symmetrisk kryptografi.

Det er viktig å merke seg at vi ved hjelp av asymmetrisk kryptografi ikke lenger trenger å utveksle hemmelige nøkler. Men offentlige nøkler må fortsatt utveksles. Infrastrukturen for å utveksle offentlige nøkler kalles ofte for «public key infrastructure» (PKI).[7]

En vanlig måte å lage en PKI på er ved hjelp av såkalte sertifikater. Et sertifikat består av et navn, en offentlig nøkkel og en digital signatur på navnet og nøkkelen. Den digitale signaturen er laget av en tiltrodd tredjepart, en såkalt sertifikatutsteder, og hele sertifikatet tolkes som at sertifikatutstederen går god for at det er den navngitte personen eller virksomheten som eier den offentlige nøkkelen.

Når en person kontakter Altinn for å sende inn selvangivelsen, begynner «samtalen» med at Altinn sender sitt sertifikat til personen. Hvis personen stoler på den som har utstedt sertifikatet, kan hun sjekke at signaturen i sertifikatet stemmer, og slik være sikker på at hun har fått Altinns offentlige nøkkel.

En utfordring ved denne modellen er at hemmelige nøkler iblant kompromitteres og ikke lenger kan brukes. Da må det tilhørende sertifikatet heller ikke brukes lenger. En vanlig løsning er at brukerne laster ned lister over tilbakekalte sertifikater[8] med jevne mellomrom og sjekker at sertifikatene ikke er tilbakekalt. En annen løsning er å spørre sertifikatutstederen direkte om sertifikatet fortsatt er gyldig.[9] Merk at disse løsningene har forskjellig personvernvirkning, siden direkte verifikasjon gir utstederen innsyn i bruken av de utstedte sertifikatene.

En annen utfordring er at det kan være svært mange sertifikatutstedere. Om man ikke stoler på en sertifikatutsteder, har man heller ingen grunn til å stole på sertifikatene vedkommende utsteder. Et godt eksempel på hvor komplisert dette kan bli, er den såkalte Internett-PKI-en som brukes på offentlige nettsteder i dag. Hver nettleser har en lang liste med sertifikatutstedere, men det er ingen god måte for brukeren å finne ut hvem disse sertifikatutstederne er eller hvorfor brukeren bør stole på dem.

Denne formen for kryptografi er i dag et modent fagfelt, selv om praksisen fortsatt ligger noe etter den teoretiske kunnskapen. Merk at kryptografi i dag er et mye bredere fagfelt enn bare kommunikasjonssikkerhet.

Selv om kryptografi er nødvendig for å beskytte digitale systemer, finnes det en lang rekke angrep som kryptografi ikke beskytter mot. Å si at noe er kryptert, er ikke det samme som at det er sikkert. Se eksempel i boks 5.2.

5.4.3 Overvåking

Forebyggende sikkerhet kan ikke forhindre alle uønskede hendelser. Vi er derfor avhengige av å kunne oppdage og håndtere hendelser. En metode er å plassere sensorer i nettverket for å inspisere datatrafikken inn og ut av virksomheter. De benytter hovedsakelig svartelisting, på lik linje med antivirus. Varslingssystem for digital infrastruktur (VDI) fra NSM NorCERT er et eksempel på et slikt system. Disse teknologiene kan både være passive og aktive. De aktive forsøker også å stoppe angrepet, da ofte i kombinasjon med brannmurfunksjonalitet. En stor utfordring for alle systemer som overvåker nettverkstrafikk, er bruk av kryptering som hindrer dem i å inspisere innholdet. Dette er et økende problem. Samtidig ser vi løsninger som gjør det mulig for slike overvåkingsenheter å ta del i nøkkelinformasjon, slik at de blir i stand til å inspisere på innsiden av den kryptografiske beskyttelsen. Det forskes på løsninger som oppdager unormale hendelser, såkalt anomali, men de har som oftest et altfor høyt nivå av falske alarmer til at de er praktiske i dag.

En annen strategi er å opprette såkalte lokkeduer («honeypots»), det vil si ressurser som ingen bruker, men som er attraktive for en innbryter. Ved å følge med på disse vil man i liten grad ha falske alarmer, siden legitim bruk omtrent ikke eksisterer. På mange områder er vi avhengige av at de som har tilgang, ikke misbruker den. Det er mulig å aktivere logging, slik at innlogging, opp-

---

7 Begrepet PKI gis ofte en bredere betydning enn infrastrukturen for å utveksle offentlige nøkler, for eksempel kan det peke på spesifikke kryptografiske teknologier eller hele omfanget av tjenester man kan få ved å bruke bestemte kryptografiske teknologier.

8 Certificate Revocation Lists (CRL).

9 Typisk ved hjelp av protokollen Online Certificate Status Protocol (OCSP).

Boks 5.2 Eksempel på et elektronisk valgsystem

Når en angriper har overtatt styringen av et system, heter det at det er kompromittert. Svært mange digitale systemer er sårbare overfor kompromittering av sentrale deler. For eksempel er mange registre bygd opp rundt essensielt sett én lagringsenhet som inneholder registerets informasjon. Dersom denne lagringsenheten kompromitteres, kan informasjonen bli endret uten at noen nødvendigvis legger merke til det. Dersom man får mistanke om at en feilaktig endring har skjedd, kan man ofte få bekreftet det ved å analysere gamle arkivkopier eller andre kopier av databasen. Problemet er at det digitale systemet ikke er i stand til å oppdage den feilaktige endringen.

For noen systemer lar det seg gjøre å bygge distribuerte systemer som tåler at én eller flere av delene blir kompromittert uten at evnen til å oppdage angrep blir redusert. Et eksempel er Internett-valgsystemet som ble prøvd ut i Norge ved valgene i 2011 og 2013.

I 2011 og 2013 kunne velgerne i utvalgte distrikter forhåndsstemme hjemmefra via Internett. De brukte datamaskinen sin til å logge seg på et nettsted, gjorde klar en elektronisk stemmeseddel, krypterte den og sendte den inn til valginfrastrukturen. Etter å ha stemt fikk velgerne en SMS-melding på telefonen som de kunne bruke til å sjekke at stemmen hadde blitt korrekt registrert. Valgsystemet var delt opp i fem deler – velgerens datamaskin pluss en firedelt infrastruktur. Hver del av infrastrukturen var drevet av forskjellige organisasjoner.

Om velgerens datamaskin var kompromittert og endret stemmen før den ble sendt inn, kunne velgeren bruke SMS-meldingen til å oppdage dette. Om én av de fire infrastrukturdelene skulle bli kompromittert, ville de tre andre delene sammen oppdage ethvert forsøk på å endre valgresultatet.

Det er verdt å merke seg tre ting ved Internett-valget. I 2013 gjorde en programmeringsfeil at krypteringen sviktet og ikke lenger skjulte stemmene. Ytterligere lag med sikkerhet sørget for at stemmene likevel forble hemmelige. Senere brukertester har vist at få velgere ville være i stand til å bruke SMS-meldingen riktig, så nesten ingen ville ha oppdaget om stemmen ble endret før innsending. I praksis ville man derfor ikke kunne oppdage angrep i liten skala.

Det teknologiske landskapet har endret seg. For eksempel er det viktig for sikkerheten i systemet at SMS-meldingen går til en telefon og ikke til velgerens datamaskin. Men dette gjelder ikke nødvendigvis lenger, da mange moderne telefoner kan videresende SMS-meldinger til velgerens datamaskin.

slag, endring og sletting kan tas vare på og benyttes ved stikkprøver eller ved etterforskning.

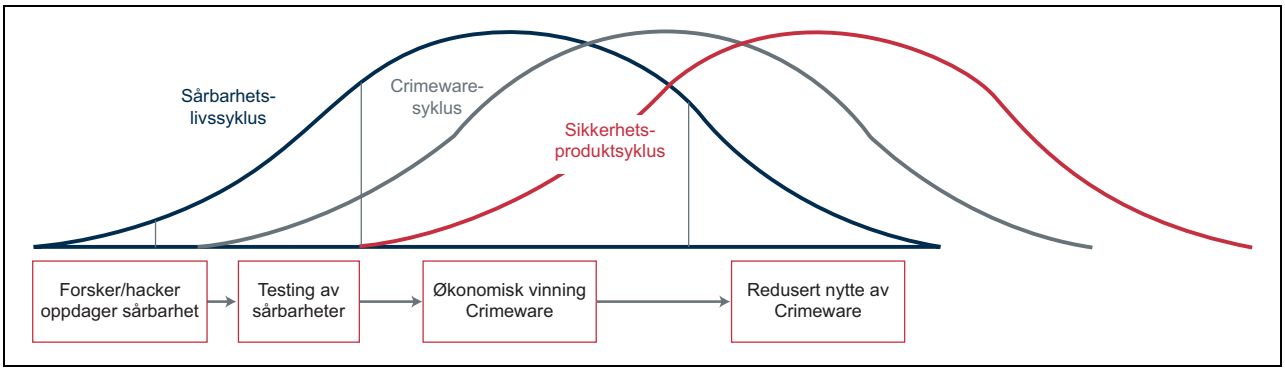
5.5 Utfordringer knyttet til programvareutvikling

Det er programvare i nær sagt alt, og vi vet ennå ikke hvordan vi skal bygge programvare som alltid fungerer slik vi ønsker. Det er vanskelig nok å få ønsket funksjonalitet til å virke, og det før noen med intensjon prøver å misbruke funksjonaliteten. Mye programkode blir også kopiert og gjenbrukt for å spare tid, noe som medfører at eksisterende svakheter blir videreført.

Det er en interessant observasjon at programutviklingsindustrien i liten grad blir ansvarliggjort for sikkerhetsfeil. Det henger igjen sammen med kompleksiteten knyttet til utviklingen. Det er normalt at programvare slippes i uferdig tilstand for så å bli fulgt opp med oppdateringer fortløpende etter som feil blir avdekket.[10] Programvare med høy utbredelsesgrad er særlig interessant for dem som leter etter sårbarheter, og der vi ikke kjenner til mange feil, har trolig få lett etter dem. Mange funksjonalitetsfeil og sikkerhetshull er derfor blitt fikset, og stadig nye introduseres i dagens jakt etter ny funksjonalitet. Mye utdatert programvare er fremdeles i bruk. Eldre Android-baserte telefoner kan ikke oppdateres, og det er fremdeles mange som bruker eldre Windows-versjoner som Microsoft har sluttet å utgi sikkerhetsoppdateringer til.

En sårbarhet kan ha en livssyklus, slik illustrert i figur 5.1. Den blir først oppdaget av noen, for eksempel en forsker eller en hacker. Så blir den kanskje publisert, og en kommer i en fase av testing. Når dette så viser seg å kunne bli utnyttet økonomisk, henger flere kriminelle seg på – kan-

[10] Noen utviklere benytter såkalt betatesting for å luke vekk noen typer feil i forkant av lansering.



Figur 5.1 Sårbarhetslivssyklus.

skje havner sårbarheten eller skadevaren på markedet, og andre kan kjøpe den. Da kommer programvareprodusentene på banen med oppdateringer og sikkerhetsindustrien med produkter. Sårbarheten og skadevaren mister sin markedsverdi etter som stadig flere tetter hullene, men nye sårbarheter er allerede inne i en ny syklus, og slik fortsetter utviklingen. For å forstå digital sårbarhet er det derfor viktig å forstå hvordan utvikling av programvare fører til utilsiktet digital sårbarhet. Utvikling av programvare handler om å bygge et komplisert system, og det er et faktum at det gjøres feil underveis i prosessen. Antall feil er grovt sett proporsjonalt med størrelsen på programvaren som utvikles, og det er vanskelig å svare på hvordan antallet utnyttbare sårbarheter øker med økt kompleksitet.[11] Feil gjøres i alle faser av programvareutviklingen, fra kravspesifikasjon via arkitektur til faktisk koding.

Noe av kvalitetsarbeidet med programvare handler om å redusere feilraten, men mye dreier seg om å finne og rette feil. Gjennomsnittlige programvareutviklere fjerner 85 prosent av feilene sine før programvaren overlates til kundene. Utviklere med høy kvalitet har vesentlig lavere feilrate og fjerner mellom 95 og 99 prosent av feilene før programvaren overlates til kundene. Det har visstnok blitt utviklet programvare der det ikke er funnet feil etter ett år, men det er sjelden. Prosjekter med høy feilrate og lav feilrettingsrate er langt vanligere.

Ikke alle feil i programvare fører til sårbarhetene omtalt i livssyklusen over. Disse sikkerhetsfeilene er gjerne annerledes enn majoriteten av programvarefeil, og vil typisk ikke påvirke den daglige driften av et system. Mange av teknikkene som brukes for å finne programvarefeil, vil derfor ikke finne sikkerhetsfeil. Metodikker for utvikling av sikker programvare forsøker både å redusere feilraten, og å øke andelen sikkerhetsfeil som oppdages og rettes.

For å redusere konsekvensene av at vi utvikler sårbar kode, må vi bli bedre til å konstruere feiltolerante systemer, der sårbarheter i én komponent ikke nødvendigvis fører til sårbarheter i systemet som helhet.

5.6 Teknologiarven

Den raske utviklingen i trusselbildet gjør at teknologi som ble vurdert å ha et høyt sikkerhetsnivå for noen år siden, vil kunne være svært usikker nå. Dette stiller infrastruktureiere og teknologibrukere overfor et krav om å ha en oppdatert og relativt nyutviklet teknologi i systemene sine. Det er imidlertid et faktum at dette ikke alltid etterleves. Årsakene til at det er slik er mange og sammensatte. I noen tilfeller har det enkle forklaringer, som motstand mot å endre en teknologi man kjenner og er vant til å bruke. I andre tilfeller kan det være mangel på investeringsvilje som gjør at man ikke bytter ut et eldre teknologisystem. I enkelte kritiske systemer vil det være slik at man unngår å oppdatere til moderne teknologi oftere enn man må, da endringen i seg selv vurderes som en sårbarhet. En siste kategori er de tilfellene der man ikke kan bytte ut eldre teknologi fordi annet kritisk utstyr er avhengig av at den gamle teknologien fremdeles er i funksjon. Et kjent eksempel på det er at mobilselskapene i Norge må ha en gammel mobiltelefonistandard i drift i tillegg til de mer moderne, selv om det er velkjente sårbarheter i den gamle standarden.

[11] For estimering av antall sikkerhetsfeil i kode, se Dan Geer (2015): *For Good Measure: The Undiscovered.* ;login april 2015, Vol. 40, No. 2.

5.7 Sikkerhet i prosesskontrollsystemer

Prosesskontrollsystemer eller SCADA[12]-systemer benyttes først og fremst om systemer som styrer og overvåker industrielle prosesser i for eksempel fabrikker, raffinerier og energi- og vannforsyningen. SCADA-systemer er imidlertid i omfattende bruk i samfunnet og benyttes blant annet til styring av heiser, ventilasjonsanlegg og trafikklys og til kontroll av tog- og flytrafikk.

En studie gjort i 2011 viste at mange prosesskontrollsystemer på verdensbasis var koblet til Internett.[13] Søkemotoren Shodan ble brukt for å identifisere 7 500 åpne prosesskontrollsystemer, deriblant 271 norske. Prosesskontrollsystemene hadde i liten grad krav til autorisering ved forespørsler, og de brukte i stor grad samme type programvare. Noen av systemene kjørte på gamle operativsystemer med kjente sårbarheter, og det var flere feilkonfigurerte brannmurer som ikke skjulte prosesskontrollsystemene tilstrekkelig. Noen var bare beskyttet med passord. Ved bruk av Shodan kan en ondsinnet aktør for eksempel søke etter versjoner av programvare med kjente sårbarheter og angripe alle søkeresultatene ved å automatisere angrepet. Sofistikerte angrep mot prosesskontrollsystemer er allerede en realitet i for eksempel USA.

I Norge hadde Dagbladet i 2013 en serie kalt Null CTRL, der journalister ved bruk av den samme søkemotoren, Shodan, klarte å identifisere norske prosesskontrollsystemer i ulike sektorer. Søkemotoren indekserer utstyr som er direkte koblet til Internett, og tilrettelegger for å søke etter spesifikt utstyr. Se boks 5.3 for detaljer rundt Null CTRL.

Digitale sårbarheter i sammenkoblede systemer går på tvers av sektorer og bransjer gjennom leverandørindustrien. Store internasjonale selskaper leverer industrikontrollsystemer til en rekke bransjer globalt, inklusiv norske virksomheter. En har sett at samme type sårbarheter går igjen i ulike produkter som benyttes i ulike bransjer. Innebygde passord i programvare blir brukt for intern eller ekstern autentisering av enheter og programmer, og representerer dermed digitale sårbarheter som kan utnyttes. Hardkodede passord er vanskelige å oppdage av systemadministratorer, og de er vanskelige å rette opp hvis de blir oppdaget.[14] I tillegg til disse sårbarhetene er det funnet programvaresårbarheter i nye og gamle produkter. Dessuten har introduksjonen av webapplikasjoner bidratt til å introdusere ytterliggere sårbarheter.[15]

Boks 5.3 Dagbladets Null CTRL-serie

Dagbladets Null CTRL-serie i 2013 skapte store overskrifter og mye oppmerksomhet rundt digital sårbarhet. Ved hjelp av søkemotoren Shodan klarte journalistene å identifisere mange åpne systemer. Dagbladet avslørte brannberedskapen i flere kommuner i Nordland, informasjon om barn på hemmelig adresse, sensitive kundedata og dokumenter om Ørland flystasjon. De avslørte hvordan flere ulike servere med dokumenter vedrørende aktivitet på norsk sokkel lå åpne og søkbare på flere tusen nett-tilknyttede databaser og servere i Norge. Mange av dem tilhørte større og mindre norske selskaper. I forbindelse med artikkelserien fant Dagbladet over 2 500 ulike typer styringssystemer i Norge koblet til Internett med lite eller ingen beskyttelse.

5.8 Elektronisk identifisering

Det er i utgangspunktet vanskelig å vite hvem man kommuniserer med på Internett. For å løse dette problemet har vi såkalt elektronisk identifikasjon (e-ID). E-ID handler om elektronisk verifikasjon av identitet mellom personer og ting som befinner seg «på andre siden av Internett». Et tilhørende problem er å knytte digital informasjon til personer og ting, på samme måte som en signatur knytter et fysisk dokument til en person. Dette kalles elektronisk signatur (esignatur).

Vanligvis bruker man kryptografi basert på digitale signaturer og en PKI til både e-ID-er og esignaturer. Ideen er at en sertifikatutsteder utste-

[12] SCADA er en forkortelse for «Supervisory Control And Data Acquisition». Tilsvarer «driftskontrollsystemer» og «prosesstyringssystemer».

[13] Éireann P. Leverett (2011): *Quantitatively Assessing and Visualising Industrial System Attack Surfaces, University of Cambridge, Dissertation.*

[14] National Cybersecurity and Communications Integration Center (2014): *ICS-CERT Monitor.* January-April 2014.

[15] Idaho National Laboratory (2011): *Vulnerability Analysis of Energy Delivery Control Systems.*

der et sertifikat til en person. Ved å bruke den hemmelige nøkkelen og sertifikatet på rett måte kan personen overbevise noen om at han sitter foran en datamaskin. Han kan også signere informasjon, slik som for eksempel en e-post eller en kontrakt.

En person kan ikke gjøre de komplekse beregningene som inngår i kryptografi. Datamaskinen må gjøre dette for eieren av e-ID-en. Men datamaskiner kan bli kompromittert. Dersom noen får tak i den hemmelige nøkkelen tilknyttet en e-ID, kan de utgi seg for å være denne personen eller signere informasjon som om de var personen.

Det tradisjonelle svaret på dette problemet er det såkalte smartkortet, en ørliten datamaskin som er spesialkonstruert for nettopp å gjøre de beregningene som kreves for e-ID-er. Denne lille datamaskinen er mye sikrere enn en vanlig datamaskin, og det er derfor mye vanskeligere å stjele nøkkelen. Likevel – om man har fysisk tilgang, kan man selvsagt stjele hele smartkortet. Når man ønsker å bruke e-ID-en, kobler man smartkortet til datamaskinen, og smartkortet utfører den nødvendige kryptografien for datamaskinen.

Et hovedprinsipp i kryptografi er at nøklene ikke er interessante i seg selv – det er hva man kan gjøre med nøklene, som er interessant. Selv om smartkortet har nøkkelen og gjør beregningene, er det datamaskinen som forteller smartkortet hvilke beregninger som skal gjøres.

Det å koble smartkortet til datamaskinen er altså det samme som å gi datamaskinen bruksrett til e-ID-en din. Dersom datamaskinen er kompromittert av kriminelle, gir du i praksis de kriminelle bruksrett til e-ID-en din. Tradisjonelle smartkortbaserte e-ID-er har altså ikke høyere sikkerhet enn datamaskinen du kobler smartkortet til.

Merk at e-ID basert på smartkort og PKI, arver alle problemene til PKI. Spesielt er det verdt å merke seg at i den tradisjonelle mentale modellen for smartkortsystemer er personvernet godt ivaretatt. Men avhengig av konkrete teknologivalg kan svært mye informasjon om bruken av en smartkort-basert e-ID i praksis tilflyte sertifikatutstederen, noe som kan være en utfordring for personvernet.

Teknologibildet er i endring, og et problem for e-ID basert på smartkort er at stadig flere terminaler folk ønsker å bruke e-ID på, ikke kan kobles til smartkort.

En e-ID behøver ikke være basert på sertifikater. Et alternativ er basert direkte på en tiltrodd tredjepart. Typisk har eieren av e-ID-en et etablert forhold til tredjeparten (for eksempel basert på passord og engangskoder). Eieren overbeviser tredjeparten om at han er den han er. Deretter kan tredjeparten gå god for eierens identitet.

Tradisjonelle e-ID basert på smartkort er ofte sårbare overfor andre angrep enn e-ID basert på tiltrodde tredjeparter. E-ID-er basert på passord og engangskoder kan for eksempel være sårbare overfor phishing, mens de kan være litt motstandsdyktige mot en kompromittert datamaskin. Hvordan en sertifikatutsteder og en tiltrodd tredjepart kan misbruke tilliten din, er også forskjellig.

Ulikt Internett-PKI-en er forskjellige e-ID-er ofte basert på svært forskjellige tekniske løsninger. Interoperabilitet blir dermed en utfordring. En måte å begrense kompleksiteten på er å lage en innloggingsportal basert på en tiltrodd tredjepart. Eieren bruker e-ID-en sin til å overbevise innloggingsportalen om at han sitter foran datamaskinen. Innloggingsportalen går deretter god for at brukeren sitter foran datamaskinen.

Dette gjør livet mye enklere for brukerstedene, som forholder seg til én innloggingsportal i stedet for mange e-ID-er. Det kan også gjøre livet enklere for eierne av e-ID-ene. På den annen side kan det oppstå en del subtile sikkerhetseffekter, der en innloggingsportal i praksis nuller ut sikkerhetstiltak i en e-ID.

En annen fordel med en innloggingsportal er at det er lett å få til såkalt engangsinnlogging («single sign-on»). I praksis handler dette om å gi datamaskinen tilgang til alle brukerstedene som er omfattet av engangsinnloggingen, noe som kan være et problem hvis datamaskinen er kompromittert.

Kapittel 6
Trender som påvirker sårbarhetsbildet

En rekke trender påvirker sårbarhetsbildet i samfunnet og vår aksept for risiko. Teknologiske, politiske og samfunnsmessige endringer har ført til store endringer også i verdikjedebildet. Der tjenesteleverandører tidligere hadde tilnærmet full kontroll over verdikjeden, er bildet i dag langt mer fragmentert. Dette illustreres best ved et eksempel. For 30 år siden eide Televerket til og med telefonen hjemme i abonnentens hus. De eide og driftet kobberlinjen inn til sentralen og videre hele veien opp til øverste nivå i tjenestekjeden. De hadde egen FoU-avdeling og store tekniske miljøer. Som et resultat av politiske, teknologiske og samfunnsmessige endringer er dette bildet nå mye mer oppstykket. Selv om Telenor fremdeles eier infrastrukturen, er deres egenkompetanse konsentrert om færre områder. Utstyrsleverandører spiller en vesentlig rolle når det gjelder driftsmessige forhold, og legger premissene for tilgjengelig teknologi. Eksterne, konkurransedyktige tjenesteleverandører tar over for eget personell på områder der det er kommersielt lønnsomt og gjennomførbart i forhold til regulatoriske krav. Organisering, metoder og kunnskap som før var tilpasset menneskelig arbeidskraft, tilpasses nå arbeidsformer der oppgaver automatiseres. Skulle det oppstå et behov for å gå tilbake til manuelle, menneskelige prosesser, for eksempel på grunn av teknologisk svikt, vil effektiviteten høyst trolig synke drastisk.

Utvalget har ikke utført noen omfattende analyse av strategiske trender som påvirker samfunnets digitale sårbarheter. Vi kan likevel konstatere at samfunnsutviklingen påvirker de fremtidige digitale sårbarhetene på overordnet nivå. Stikkord her kan være[1]

- forandringer i demografien
- urbanisering
- samfunnets økende ressursforbruk
- miljøspørsmål og klima
- helse og utviklingen innen medisin
- informasjonsteknologi og informasjonshåndtering
- utviklingen innen utdanning og kompetanse
- automatisering i hverdagen og i arbeidslivet
- kriminalitet og rettsvesen
- forsvarsutgifter og forsvarsevne
- identitet og rollen til staten

I dette kapittelet omtaler vi et utvalg trender og drivkrefter som påvirker utviklingen av samfunnets digitale sårbarheter. Både på kort og lengre sikt, og i all hovedsak med en teknologisk vinkling. Teknologirådet har bidratt med tekstlig innspill.

6.1 Digitaliseringen av samfunnet og sårbarhetsbildet

Digitalisering har forenklet hverdagen til enkeltindividet, og er en driver for innovasjon, økonomisk vekst og produktivitet. Teknologien skaper også nye sårbarheter og utfordringer. For eksempel gir den en utvidet angrepsflate for kriminelle. Utenriksdepartementet har uttrykt at Internett er blitt en generator for økonomisk vekst og sosial utvikling, men at håndtering av sikkerhetsutfordringer i det digitale rom er en forutsetning for at dette skal skje.[2]

Det er all grunn til å tro at den teknologiske utviklingen vil fortsette å gå raskere, og at etterspørselen etter kunnskap vil øke kraftig. EU-kommisjonen har estimert at 90 prosent av jobbene i EU innen 2020 vil kreve digitale ferdigheter, og advarer om at EU i inneværende år vil mangle 509 000 årsverk med denne kompetansen. Det er

[1] En bred analyse av strategiske trender finnes i *Ministry of Defence UK (2014): Global Strategic Trends – Out to 2045. Se også National Intelligence Council (2012): Global Trends 2030: Alternative World*, samt diskusjon om teknologiske og samfunnsmessige utviklingstrekk i *Nasjonal sikkerhetsmyndighet (2015): Helhetlig IKT-risikobilde 2015*.

[2] Meld. St. 37 (2014–2015) *Globale sikkerhetsutfordringer i utenrikspolitikken – Terrorisme, organisert kriminalitet, piratvirksomhet og sikkerhetsutfordringer i det digitale rom*, s. 26.

på verdensbasis estimert med rundt 5 milliarder Internett-brukere innen 2020.

Mennesker har naturlig en viss forståelse av hvordan vi sikrer informasjon i manuelle, papirbaserte prosesser. Med digitaliseringen er vi i stor grad fremmedgjort, og ingen har lenger oversikt over sårbarhetsbildet, slik vi en gang hadde.

En datamaskin er for eksempel utviklet lag for lag, der hvert lag skjuler en underliggende kompleksitet for det neste. Disse maskinene kobler vi så sammen i datanettverk basert på en tilsvarende lagdelt modell. Når vi utvider funksjonalitet og knytter sammen IKT på nye måter, glemmer vi ofte de underliggende forutsetningene og antagelsene som er gjort, og noen ganger henger vi igjen med antagelser som ikke lenger gjelder.

Lagringsmediene vi lagrer data på, var en tid tilbake bare «dumme» mekaniske enheter under full kontroll av datamaskinens sentralprosessor – som da måtte bruke mye tid på å gi lese- og skriveinstrukser. Av ytelseshensyn er harddisker i dag smarte. Sentralprosessoren kan nå utføre andre oppgaver samtidig som lagringsmediet jobber i bakgrunnen. Dette innebærer at lagringsenheten har full tilgang til systemets internminne og kan – hvis den er ondsinnet – skrive og lese til helt andre områder enn den blir bedt om. Den kan for eksempel plassere skadevare eller hente ut kryptografiske nøkler.

Et eksempel på endrede forutsetninger er bruk av SMS-meldinger med bekreftelseskoder for innlogging på webtjenester og for digital signering av digitale handlinger. En grunnleggende sikkerhetsforutsetning er at denne koden kommer via en annen kanal enn den som skal bekreftes, og slik er det når vi logger inn via en annen enhet enn telefonen. I dag foregår mye pålogging, for eksempel til nettbank, direkte fra smarttelefonen. Mange programmer på telefonen kan på lik linje med brukeren lese SMS og derfor selv fylle inn informasjonen som kommer via SMS, der den etterspørres. Vi ser også innebygd funksjonalitet for å synkronisere meldinger, inkludert SMS, på tvers av digitale enheter. Dette betyr i praksis at skillet viskes ut og er med på å redusere sikkerhetsnivået til systemer.

Et annet eksempel som viser den fremmedgjøringen vi står overfor, er knyttet til de grensesnittene vi presenteres for. Metaforer som *mapper*, *skrivebord* og *papirkurv* skjuler viktig informasjon. Vi legger filer i *papirkurven* og tømmer den for å slette informasjonen i filene. Det er naturlig å tro at informasjonen dermed er tilintetgjort. I realiteten er det bare referansene til informasjonen som er borte. Over tid vil informasjonen kunne bli overskrevet, men ofte kan informasjonen hentes tilbake lang tid etter slettingen. Det samme ser vi på nettbaserte tjenester. Når et bilde eller et kommentarinnlegg slettes fra sosiale medier, blir innholdet skjult for deg og meg, men det blir ikke nødvendigvis borte, selv om det ser slik ut.

6.2 Informasjonsteknikk og informasjonshåndtering

Det foregår hele tiden en utvikling i vår evne til å samle inn, lagre og analysere informasjon. Det har vært en dramatisk økning i regnekraft og en utvikling av algoritmer for å analysere store datamengder. Dagligdagse gjenstander kobles i økende grad til Internett. Elektronikk integreres i ting vi har på oss, som klær og annet tilbehør. Nettverket av sensorer samler inn stadig mer datamateriale om våre liv og omgivelser. Det fører til at det på sikt vil være vanskelig å fungere i samfunnet uten å være tilkoblet («off the grid»).[3]

6.2.1 Økt regnekraft, store data og stordataanalyse

Datamaskinene blir stadig raskere. Det har vært observert en vedvarende økning i antall transistorer i integrerte kretser helt tilbake til 1960-tallet. Moores lov er en stadfesting av denne trenden, der antallet transistorer dobles hvert annet år. Antall transistorer henger sammen med ytelsen, og vi kan litt forenklet si at ytelsen dobles hvert tredje år. I mange år målte vi progresjonen i klokkehastighet, men vi har nå nådd begrensninger i hvor høyt vi kan skru denne opp. Vi ser derfor nå en trend i retning av flere parallelle, uavhengige prosesseringsenheter. At vi utnytter parallell regnekraft, har igjen gitt nye utfordringer, både innenfor rammene av det vi anser som «en datamaskin», og for måten vi utnytter den samlede beregningskraften til sammenkoblede datamaskiner på.

Selv om datamaskinene blir raskere, er det måten vi instruerer dem på, som er avgjørende for nytteverdien av dem. Det er mange evner vi mennesker tar for gitt, men som datamaskiner har store problemer med – for eksempel det å identifisere gjenstander i et bilde. Det har imidlertid vært stor fremgang innen utvikling av algoritmer som lar datamaskiner «lese» håndskrift, oversette mel-

[3] Ministry of Defence UK (2014): *Global Strategic Trends – Out to 2045*.

lom språk, utføre medisinsk diagnostisering og gjenkjenne ansikter, med mer.

Store data («Big Data») er en teknologisk trend som beskriver de voksende mengdene med digital informasjon som blir produsert og gjort tilgjengelig, og som ulike aktører kan samle inn, analysere og utnytte til mange ulike formål. Datamengdene produseres i vår daglige omgang med teknologi, for eksempel via sosiale medier, nettsøk og bruk av smarttelefon, men også gjennom sensorer knyttet til maskinelt utstyr som medisinske apparater, smarte strømmålere og biler. Stordatanalyse utføres ved hjelp av statistikk og algoritmer som er tilpasset det å trekke ut mønstre og trender fra store menger data.

Bruken av store data forventes å tilta kraftig i årene som kommer. Trenden understøttes av synkende kostnader knyttet til datainnsamling, lagring og regnekraft, samtidig som teknologien blir tilgjengelig for flere gjennom ulike skytjenester.[4] Banebrytende fremskritt innen analyse og kunstig intelligens, samt fremveksten av billig sensorteknologi som bygges inn i stadig flere Internettbaserte enheter, er også viktige drivere.

Ifølge IBM blir det daglig generert mer enn 2,5 milliarder gigabyte data, og dette tallet vil bare øke. Daglig lastes det opp mer enn 500 millioner bilder på nettet, og hvert minutt mer enn 200 timer med video. I løpet av 2020 er det forventet at mer enn 80 prosent av verdens voksne befolkning vil bruke en smarttelefon i hverdagen, samtidig som kroppsnær teknologi og tingenes Internett vil gi opphav til nye informasjonsstrømmer.

Store data forsterker sikkerhetsutfordringer ved en distribuert infrastruktur, skytjenester og sanntidsregistrering av data. Risikobildet forsterkes ytterligere når teknologien blir billigere og mer tilgjengelig også for mindre virksomheter. Når bruken av store data brer om seg, kan det bidra til nye former for sårbarhet.

Størrelse, omfang og varighet. Med økende digitalisering samler både private og offentlige virksomheter inn mer data, gjerne både mer finmasket og oftere enn før. Ett eksempel er at teleselskapene automatisk registrerer mobiltelefonens kommunikasjon med ulike basestasjoner, et annet hvordan butikkjedene registrerer innkjøpene kunden gjør, gjennom ulike fordelskort. Hyppig og finmasket registrering gjør at datasett som lagres i datasentre, vokser i størrelse og omfang. Lagring i skytjenester og deling med ulike tredjeparter gjør dataene mer sårbare for datatyveri. Størrelsen på datasettene gjør slike innbrudd mer omfattende enn tidligere. Eksempelvis førte et datainnbrudd hos det amerikanske helseforsikringsselskapet Anthem Inc. i 2015 til at opplysninger som navn, bostedsadresse, fødselsnummer, inntekt og jobbsituasjon knyttet til nesten 80 millioner kunder kom på avveier. Slike innbrudd kan altså ha vidtrekkende konsekvenser for svært mange mennesker.

Ikke bare er det mulig å oppbevare store datamengder over veldig lang tid, slike datasett kan også kopieres og deles både raskere og bredere enn det som var tenkelig tidligere. Når et digitalt bilde deles over Internett, kan eieren vanskelig vite hvor mange kopier som eksisterer rundt om i verden, og hvor lenge disse lagres. Slik sett har digitale data lang varighet. Når store mengder informasjon bevares over tid og forvaltes av ulike aktører eller ukjente tredjeparter, kan det gjøre individet sårbart for misbruk lenge etter at dataene ble produsert og registrert.

Tilgangsregulering og kontroll. For å dra nytte av store data vil man ofte ønske å kombinere datasett fra ulike kilder. Når dette skal gjøres i en kompleks, distribuert infrastruktur, kan det være utfordrende å kontrollere hvem som har tilgang til hvilke datasett, og hvordan de brukes. Dermed kan det være vanskelig å se til at uvedkommende ikke får tilgang til informasjon de ikke er autorisert for. Det kan også være vanskelig å etablere robuste sporingslogger som viser nøyaktig hvem som har fått tilgang til hvilke data, til hvilket formål og til hvilken tid. Denne sårbarheten forsterkes når ulike datasett har ulike sikkerhetsbehov, og når datasett kombineres for å lage nye datasett.

Datakvalitet og opphav. Når store data brukes i beslutningsprosesser, er det viktig at man kjenner opphavet og vet når dataene er skaffet til veie. Når innsamlingen skjer fra mange ulike kilder og nye datasett oppstår som kombinasjoner av andre, eldre datasett, kan det bli stadig mer utfordrende å spore opphav og sikre kvalitet og integritet. Som en følge kan viktige beslutninger baseres på data som enten er ufullstendige eller av dårlig kvalitet. Dersom det mangler systemer for å kontrollere opphav og kvalitet, kan viktige beslutningsprosesser i verste fall også være sårbare for manipulerte datasett.

Analyse og personvern. Analyse av store data kan bidra til innsikt med stor nytteverdi, men også til å avsløre sensitiv eller hemmelig informasjon. Dette kan blant annet skje ved at man krysskobler ulike datasett. Datasett som isolert sett virker uskyldige, uten personlig eller sensitiv informasjon, og som reguleres deretter, kan, sammenstilt med andre datasett, være svært avslørende. Et

[4] Se også punkt 23.7 «Utkontraktering og skytjenester».

eksempel er at den amerikanske dagligvarekjeden Target ved å analysere kjøpemønsteret til kundene sine kunne sannsynliggjøre hvilke kunder som var gravide.

I kombinasjon med andre datasett har anonymiserte datasett i flere tilfeller vist seg å være sårbare for re-identifisering. Når innsamlingen av digital informasjon øker i omfang samtidig som datasett frigjøres for bruk eller deles mellom ulike aktører, svekkes individets kontroll over personlige data. Individet kan da fort bli stående som den mest sårbare parten, med risiko for uønsket identifisering, misbruk av sensitiv informasjon eller ID-tyveri.

Teknologien kan kanskje til slutt endre både hva vi kan holde privat i fremtiden, og synet på hva som bør holdes privat.

6.2.2 Tingenes Internett

Tingenes Internett («Internet of things» eller «Internet of everything») er et samlebegrep for hvordan Internett brukes for å koble sammen stadig flere autonome komponenter til et komplekst system. Ulike gjenstander, apparater og maskiner vi omgir oss med i hverdagen får muligheten til å kommunisere med hverandre og dele informasjon fra innebygde sensorer.[5]

Tingenes Internett gir mange anvendelsesområder i samfunnet, blant annet innen industri, butikkvirksomhet, logistikk og godshåndtering, overvåking og sikkerhet, eiendom og boliger, smart transport og helsevesen, smart infrastruktur, markedsføring, underholdning og så videre.

Begrep som *smarte strømnett*, *smarte transportsystemer*, *smarte hjem* og *smarte byer* brukes for å beskrive hvordan integrering av mikroprosessorer og digital kommunikasjon forandrer samfunnet. På denne måten kan smarte byer ses på som en visjon der mange ulike infrastrukturer kobles sammen, slik som strømnettet, muligheter for å lade elbiler, trafikklys, bygninger, posisjonsinformasjon, data fra offentlige registre, redningstjeneste og ambulanse.

Antall gjenstander som er koblet til Internett, øker raskt. Det er i dag rundt 20 milliarder tilkoblede enheter.[6] Selv om dette i hovedsak er datamaskiner, smarttelefoner og nettbrett, spås det at veksten fremover vil drives av tingenes Internett.[7] I følge estimater vil det i 2020 være mellom 40 og 50 milliarder enheter koblet til Internett.

Når flere ting vi omgir oss med i hverdagen, blir koblet på Internett, bidrar det til å forsterke eksisterende sårbarheter knyttet til sikkerhet og personvern på nett. Dette kan skyldes at produsentene bak mange gjenstander som nå kommer på nett, tidligere ikke har måttet bekymre seg for informasjons- og nettverkssikkerhet, som for eksempel mulighet for oppgraderinger. Det mangler fremdeles bransjenormer for hvordan disse skal plasseres inn i våre private nettverk.

Uberettiget tilgang til og misbruk av personlig informasjon. I likhet med datamaskiner er andre gjenstander og apparater som er koblet til Internett, sårbare for angrep fra inntrengere uten rettmessig tilgang til systemene. Slike angrep kan gi inntrengeren tilgang til sensitiv informasjon som enten ligger lagret i gjenstanden eller blir formidlet videre til andre gjenstander i nettverket. Et eksempel er en smart-TV, som også kan brukes til å surfe på Internett og til å lagre kredittkortopplysninger for å muliggjøre nettkjøp. Svekket sikkerhet kan gi uvedkommende opplysninger som kan brukes til kortsvindel eller identitetstyveri.

Tilrettelegge for angrep på andre systemer. Når gjenstander er koblet i nettverk, blir de sårbare for sikkerhetssvakheter andre steder i nettverket. En inntrenger kan utnytte svakheter i en gjenstand for å angripe systemer som gjenstanden er koblet til. Eksempelvis kan angriperen gjøre et smarthus utilgjengelig for eieren.

Skade på mennesker og systemer. Svakheter i sikkerheten kan også utgjøre en risiko for personlig sikkerhet. En angriper kan eksempelvis omprogrammere en tilkoblet bil slik at bremsesystemet ikke fungerer som forventet, eller justere innstillingene på en tilkoblet insulinpumpe for å endre medisineringsdosen. Sikkerhetsrisiko kan også følge uten at inntrengeren endrer funksjonaliteten til systemet.

Personvern. Tingenes Internett vil gjøre at vi legger igjen enda flere digitale spor i hverdagen. Gjenstander koblet til tingenes Internett vil på ulike måter kunne samle følsomme personopplysninger, som presis stedsinformasjon, bankdata eller helseopplysninger. Over tid vil slike data kunne tegne detaljerte bilder av hvor vi befinner oss, hva vi gjør, hvilke vaner vi har, og hvordan helsen vår utvikler seg. Slik informasjon vil kunne brukes og misbrukes i vurderinger av kredittverdighet, forsikring og ansettelser.

---

5 White House (2014): *Big data: Seizing opportunities, preserving values.*

6 EMC (2014): *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things.*

7 Cisco (2011): *The Internet of Things - How the Next Evolution of the Internet Is Changing Everything.*

Tingenes Internett kan også «åpne et vindu» inn til private rom. Forskere har for eksempel vist at analyse av data fra smarte strømmålere kan brukes til å fastslå hvilket TV-program eieren så på.[8]

6.2.3 Kroppsnær teknologi

De siste årene har sensorer og datachips blitt bedre, billigere og så små at de kan plasseres på kroppen, i smykker, på briller eller på klærne. Slik kan vi bruke dem hele tiden, uten at de er i veien for det vi ellers gjør. Denne typen teknologi har fått navnet «wearables», eller *kroppsnær teknologi*.

Et eksempel på kroppsnær teknologi er digitale klokker, som kan fungere som en forlengelse av smarttelefonen. Digitale armbånd og sensorer båret på kroppen kan måle vitale trenings- og helsedata som bevegelse, puls, søvnmønster og hjerterytme. Små skjermer som festes på brillene kan vise informasjon tilpasset stedet du er på. De kan integrere informasjon som fart og løypekart inn i synsfeltet i brillene eller vise målrettet reklame. Dette kalles også *forsterket virkelighet*.

Kroppsnær teknologi gir oss et utvidet sanseapparat. Vi kan samle data om oss selv og omgivelsene våre kontinuerlig. Datakraft og datalagring blir stadig rimeligere. Vi må regne med at det vil bli lagret mye mer informasjon om hva vi gjør, og hvor vi beveger oss. Dette forsterker de sårbarhetene som allerede er avdekket i nettjenester, sosiale medier og tingenes Internett, men introduserer også noen nye sårbarheter, spesielt knyttet til personvernet.

Algoritmer som analyserer og kobler data, blir stadig mer avanserte. Vi vet i dag ikke hva algoritmene kan utlede i fremtiden. Helsedata som vi samler inn i dag, kan potensielt si veldig mye om helsen vår i fremtiden. Dette er omtalt i kapittel 17 «Helse og omsorg».

Sammenkobling av informasjon. Tjenester som lover forsterket virkelighet, er i sin natur kontekstspesifikke; de trenger å vite hvor du er, hvor du fester blikket, hva du gjør, og hva du ønsker å vite. Folk som bruker kroppsnær teknologi som er rettet mot omverdenen, til å ta bilder av mennesker rundt seg, bidrar til å kartlegge oss uten at vi nødvendigvis legger merke til at det skjer. Hvordan andre deler og offentliggjør bilder, kan få store konsekvenser for oss, uten at de nødvendigvis forstår rekkevidden av det. Personer og virksomheter, en fremtidig arbeidsgiver eller forsikringsselskapet, som får tilgang til informasjonen, kan sammenstille den med ytterligere datakilder.

Algoritmer for mønstergjenkjenning kan gjenkjenne ting, bygninger og personer i bilder og video. Ansiktsgjenkjenning står dermed i en særstilling i denne sammenhengen. Når du blir identifisert i et bilde, kan andre bruke det som en nøkkel til å få tilgang til mye mer informasjon om deg. Virksomheter, myndigheter og privatpersoner har mulighet for å utlede hvor vi har vært, hva vi har gjort, og når vi har gjort det. Til sammen kan de sette sammen puslespillbrikkene om livene våre til et omfattende bilde.

6.3 Automatiseringen av hverdagen og arbeidslivet

Roboter eller ubemannede systemer – det vil si maskiner som kan utføre kompliserte instruksjoner uten direkte å involvere en menneskelig operatør – øker i anvendelse og skaper både nye muligheter og nye digitale sårbarheter i samfunnet. I dag finnes autonome systemer til bruk i hverdagen, som støvsugere, gressklippere, selvstyrende biler og ubemannede flygende kjøretøy (såkalte droner). Slike produkter øker raskt i antall. Kostnaden for ubemannede systemer som droner har falt dramatisk de seneste årene. Ubemannede systemer kommer trolig til å erstatte mennesker i høyere grad enn i dag, utføre oppgaver med økende effektivitet og samtidig redusere risikoen for mennesker. Men ubemannede systemer kan også brukes som en ressurs av kriminelle og terrorister.

Den utbredte bruken av datamaskiner har allerede i dag gjort visse yrker nesten overflødige, samtidig som nye yrker har blitt til. Utviklingen innen robotteknologi kan føre til alt fra små justeringer i måten vi jobber på, til massearbeidsløshet og sosial uro.[9] [10] Etter hvert som roboter blir mer livaktige, vil trolig også samspillet med mennesker bli mer sofistikert.

Automatiseringen fører ikke bare til at produktene i seg selv blir mer selvgående, men også til at produksjonsmetodene automatiseres, slik at produksjonen går raskere. Global produksjon har gått fra å være svært arbeidskrevende til i større grad å være basert på informasjonsteknologi. Produksjonsprosesser kan derfor komme til å flyttes

---

8 U. Greveler, B. Justus, and D. Loehr (2012): *Multimedia content identification through smart meter power usage profiles.*

9 Nicholas Carr (2014): *The Glass Cage: Automation and Us.*

10 Ministry of Defence UK (2014): *Global Strategic Trends – Out to 2045.*

nærmere forbrukerne for å unngå lange forsyningskjeder. Automatiseringen vi allerede har, understøtter denne trenden, og såkalt additiv produksjon (ved hjelp av 3D-printere) bidrar også til denne trenden.

6.3.1 Additiv produksjon – 3D-printere

Tradisjonelt har vi produsert gjenstander ved å starte med materialene, for eksempel metall, plast, stein eller treverk. Deretter er materialet blitt formet til den ønskede gjenstanden gjennom kutting, støping og bøying. I additiv produksjon bygges gjenstander fra løse materialer, enten væsker eller pulver, ved at materialene legges lag på lag.

En 3D-printer er en maskin som bygger tredimensjonale objekter ut fra en datategning. Objektene bygges lag for lag i ett stykke i stedet for å settes sammen av ulike komponenter. 3D-printere er tilgjengelige i form av alt fra svært enkle modeller til et par tusen kroner til bruk i hjemmet, til avanserte modeller til flere millioner kroner beregnet på industriell bruk.

Antallet bruksområder er økende. Det gjøres blant annet forsøk med bygging av karosserier for biler, støping av hus, proteser og høreapparater, samt printing av elektronikk og mat. Printerne forbedres kontinuerlig. De kan bygge stadig raskere, i flere materialer og med stadig større presisjon.

Bruk av 3D-printere åpner prinsipielt sett opp for tre typer sårbarhet. Felles for disse utfordringene er at de krever tilgang til den datafilen som skal brukes for å skrive ut produktet. IKT-sikkerhet er med andre ord helt avgjørende for å redusere sårbarhet knyttet til bruk av 3D-printere.

Ulovlig kopiering. Personer med tilgang til en 3D-printer vil kunne kopiere et produkt dersom de har tilgang til en datafil som beskriver produktet. Dette betinger imidlertid at produktet er av en slik beskaffenhet at det lar seg produsere ved hjelp av en 3D-printer. Per i dag gjelder dette svært få produkter.

Manipulering av designfiler. Filer som brukes i 3D-printing, kan manipuleres av personer som ønsker å forsinke en produksjonsprosess eller skade omdømmet til et firma. Man kan bygge inn små feil i en fil som gjør at produktet ikke fungerer, går i stykker eller lignende.

Produksjon av illegale produkter. 3D-printere kan gjøre det mulig å produsere illegale våpen og andre produkter der bruken er regulert.

6.3.2 Ubemannede luftfartøy – droner

Droner er en vanlig betegnelse for ubemannede luftfartøy. Den sivile bruken av droner er i kraftig vekst. Det er anslått at det ved inngangen til 2015 var solgt omkring 10 000 doner til privat bruk i Norge. Dette dreier seg i hovedsak om små kameradroner til hobbybruk, men bruken av større droner i profesjonell sammenheng øker også markant.

Droner betegnes også som RPAS (Remotely Piloted Aircraft Systems) eller UAS (Unmanned Aircraft Systems). Betegnelsene understreker at selve fartøyet må ses som del av et IKT-system som også involverer operatører, kommunikasjons- og fjernstyringsteknologi og dronens sensorutrustning. Størrelsen varierer fra helikoptre på noen få gram til fly med et vingespenn på over 40 meter.

Droner gjør det mulig å sende kameraer og annet sensorutstyr i luften raskere, enklere og billigere enn med bemannende fly og helikoptre. Fordi de er ubemannet, kan de brukes i risikofylte operasjoner og miljøer. Derfor tas droner i økende grad i bruk i for eksempel overvåkings- og beredskapssammenheng. Etter Fukushima-ulykken i Japan i 2011 ble droner brukt for å kartlegge skader og strålingsfare.

Den økende utbredelsen av droner åpner luftrommet for mange typer ny bruk og utfordrer luftfartsikkerheten. Se punkt 18.3 «Luftfart».

Hacking og digital kapring. Droner har også vist seg sårbare for hacking og digital kapring, noe som kan medføre at uønskede aktører tar kontroll over dronen eller sensordataene den sender til kontrollstasjonen. At droner kontrolleres via satellitt og datanettverk, åpner for nye muligheter for fjernhandling. Operatøren av dronen kan være ukjent, noe som åpner opp for samfunnsskadelig bruk. Droner er blitt brukt i kriminell aktivitet og i smugling, og det finnes også eksempler på at droner er blitt utstyrt med eksplosiver og forsøkt brukt i terrorangrep.

Overvåking og spionasje. Droner kan være nærmest usynlige og lydløse, og de kan manøvrere nær bakken og inn i bygninger. De er bygd for å registrere data, noe som også åpner opp for spionasje og ulovlig overvåking.

Autonome styringssystemer. Utviklingen går mot stadig mer autonome styringssystemer der droner tar egne avgjørelser om navigasjon og operasjoner. Dette er systemer som er sårbare for feil så vel som for misbruk av aktører med intensjon om å skade.

6.4 Nye digitale tjenester og endringer i adferd

Den teknologiske utviklingen skaper muligheter for nye tjenester og gir opphav til endret adferd, både på individnivå og på samfunnsnivå. Dette påvirker samfunnets digitale sårbarheter.

6.4.1 Skytjenester

Skytjenester er en felles betegnelse på alt fra dataprosessering og datalagring, til programvare som er tilgjengelige fra eksterne serverparker tilknyttet Internett. Problemstillingene slike tjenester reiser er utredet i punkt 23.7 «Utkontraktering og skytjenester».

6.4.2 Sosiale medier

Sosiale medier er nettbaserte tjenester som gjør det mulig for folk å kommunisere med hverandre og dele informasjon i grupper. I noen tilfeller vil gruppene være små, i andre tilfeller kan de involvere flere millioner brukere. Det finnes i dag mange ulike typer sosiale medier, deriblant plattformer for sosiale nettverk, informasjonsdeling, diskusjon, samarbeid og koordinering.

Bruken av sosiale medier har tiltatt kraftig de siste årene, en vekst som også er nært knyttet til utbredelsen av smarttelefoner med Internett-tilgang. Nordmenn er flittige brukere av sosiale medier. Norsk mediebarometer rapporterer i 2015 at av dem som besøker Internett i løpet av en gjennomsnittsdag, har 64 prosent besøkt Facebook og 22 prosent besøkt andre sosiale medier.[11]

Når informasjon deles på sosiale medier, er den ikke lenger privat. Det kan være vanskelig å vite eller forutse hvordan informasjonen sprer seg gjennom nettverket, og hvem som får tilgang. Feriebilder delt på sosiale medier kan for eksempel utnyttes av kriminelle som ønsker å begå innbrudd i tomme hus. Praksisen med bruk av personlige sikkerhetsspørsmål for verifikasjon av identitet har også svakheter, ved at hackere har mulighet til å besvare disse ved å studere informasjonen som blir lagt ut på sosiale medier.

Sosiale medier gir bedre muligheter for å nå målgrupper enn før, ved at nyheter kan baseres på hva man søker etter, og hva man liker. Dette gir mulighet for å presentere informasjon slik målgruppen helst vil se den.

Når stadig mer informasjon om personlige kvalifikasjoner og både private og profesjonelle nettverksrelasjoner deles på sosiale medier, blir vi mer sårbare for såkalt sosial manipulasjon. I slike tilfeller kan en angriper forsøke å bruke falske profiler for å lure til seg informasjon gjennom målrettet kommunikasjon. Slik informasjon kan brukes til å bryte seg inn i IKT-systemene til virksomheter.

Fremveksten av sosiale medier har bidratt til å senke terskelen for hvem som kan være med på å spre informasjon, og har vist seg å være en effektiv kanal for å spre førstehåndsinformasjon fra konfliktområder som er utilgjengelige for uavhengig presse.

I senere tid har sosiale medier etablert seg som et viktig middel i radikaliseringsprosesser og som rekrutteringsverktøy i terrorsammenheng. Som en motvekt brukes sosiale medier også i demokratiseringsprosesser. Den arabiske våren er et godt eksempel.

6.4.3 Bruk av privateid datautstyr i jobbsammenheng

Bring Your Own Device, forkortet *BYOD* (bruk av privat datautstyr) er et begrep som brukes når ansatte bruker sitt eget, private utstyr for å få tilgang til tjenester og informasjon som eies av virksomheten der den ansatte arbeider. Utstyret er gjerne datamaskiner, smarttelefoner eller nettbrett, mens tjenestene kan være e-post, kalenderfunksjoner og IP-telefoni.

Bruken av privat teknologi i jobbsammenheng øker kraftig. Ifølge mørketallundersøkelsene[12] har bruken av privat mobiltelefon og nettbrett doblet seg fra 2012 til 2014, og det gjelder alle typer virksomheter. Nesten 50 prosent brukte i 2014 egen mobiltelefon, mens tallene for nettbrett hang noe etter, med 36 prosent. 70 prosent av virksomhetene tillot at virksomhetens utstyr, særlig mobiltelefoner og bærbare datamaskiner, ble brukt til private formål.

Sikkerhetspolicyer i virksomheter er i utgangspunktet rettet mot utstyr som de selv eier og/eller har kontroll over. Ofte er ikke privat utstyr sikret på samme måte, og det åpner for både tilsiktede og utilsiktede sårbarheter. Flere virksomheter har imidlertid utarbeidet sikkerhetspolicyer som omfatter bruk av privat utstyr tilknyttet deres IKT-systemer og nettverk.

Kompromittering av virksomheters informasjon. Usikret informasjon som befinner seg på digitalt utstyr, eller som man har tilgang til gjennom utstyret, kan kompromitteres hvis man mister utstyret,

[11] Norsk mediebarometer, 2014.

[12] NSR (2014): *Mørketallsundersøkelsen.*

låner det bort eller gir det videre, eller når en person slutter i en virksomhet. Hvis utstyret deles med for eksempel et barn i familien, kan virksomhetens informasjon bli delt via e-post eller i skyen uten at det var meningen.

Introduksjon av virus og annen skadelig programvare. Personlig utstyr kan bli infisert med virus og annen skadelig programvare som ikke fanges opp av virksomhetens ordinære beskyttelsesmekanismer. Disse kan smitte over i virksomheten og skade IKT-systemer og informasjon.

Overvåking av privat informasjon. Virksomheter kan av sikkerhetsmessige årsaker velge å overvåke bruken av personlig utstyr. Det åpner for at arbeidsgivere kan få tilgang til personlig informasjon.

6.5 IKT-sikkerhet på den strategiske agendaen

Digitalisering av samfunnet har skapt avhengigheter og sårbarheter som går på tvers av sektorer, ansvar og landegrenser. IKT-sikkerhet får stadig større oppmerksomhet. Spørsmålene står høyt på den politiske agendaen i mange land, og har forsvars- og sikkerhetspolitiske så vel som utenriks- og handelspolitiske dimensjoner.

Digital sårbarhet og IKT-sikkerhet blir i økende grad sett på som noe som omhandler beskyttelse av velstandssamfunnet i sin helhet, ikke bare som et teknologispørsmål. Det blir stadig viktigere å utforme praksis og lover slik at sikkerhet blir et konkurransefortrinn i den globale økonomien.

Samfunnets digitale sårbarheter gir også grobunn for elektronisk kriminalitet. På Internett har det de siste par årene vokst frem tjenester for kriminalitet – «crime-as-a-service». Samspillet mellom tradisjonell og elektronisk kriminalitet øker i omfang og blir mer komplekst. Utviklingen stiller nye krav til rettsvesenet, for eksempel når det gjelder samarbeid med utenlandske politimyndigheter og private aktører,[13] se for øvrig kapittel 21 «Avdekke og håndtere digitale angrep».

I takt med at digitaliseringen av samfunnet har gjort oss mer avhengige av Internett, har også statlige myndighetsorganer tatt i bruk de mulighetene teknologien gir for å utføre spionasje mot andre lands nasjonale interesser. Cyberspionasje og cybersabotasje er allerede en del av den sikkerhetspolitiske «verktøykassen» i flere land. Denne endringen i trusselbildet handler om en økende profesjonalisering av grupperinger som ønsker å utnytte våre IKT-systemer.

Statlige trusselaktører har store ressurser og mye kunnskap, er godt organisert og har strategiske målsettinger. Vi omtaler dem som *sofistikerte angripere*: målrettede aktører, ofte statlige eller statsfinansierte, med betydelige ressurser i form av datakraft, kompetanse og andre avanserte virkemidler. Sofistikerte angripere går også under begrepet «avanserte vedvarende trusler».[14] Det som skiller denne kategorien fra organiserte kriminelle, er hovedsakelig grensene for hvor langt disse er villige til å gå for å oppnå mål som ikke direkte gir økonomisk gevinst.

6.6 Trender i sikkerhetsteknologien

De digitale sårbarhetene i samfunnet skaper et kappløp mellom de som er angripere, og de som utvikler sikkerhetsteknologien. Her følger en kortfattet omtale av noen trender innen biometri og kryptografi.

Biometri er måling av biologiske eller adferdsrelaterte mønstre, som fingeravtrykk, netthinne, stemme eller måten man signerer et brev på. Målet for biometri er å måle noe som er unikt for enkeltindividet og samtidig stabilt over tid. Det forskes aktivt på nye kilder til biometri.

Teknologien for å gjenkjenne fingeravtrykk har modnet betraktelig. Fingeravtrykk har erstattet passord på mange bærbare enheter, og brukes som et alternativ til nøkler og nøkkelkort til fysisk adgangskontroll. Fingeravtrykk brukes ikke bare til tilgang til enheter, men også til å bekrefte handlinger vi utfører på enhetene, for eksempel kjøp av digitalt innhold og andre økonomiske transaksjoner.

Bruk av biometri reiser personvernrelaterte utfordringer. Teknologien for ansiktsgjenkjenning vil snart være så god at man automatisk kan gjenkjenne og følge alle som beveger seg i et kameraovervåket område, for eksempel et kjøpesenter. I tillegg er biologiske mønstre i all hovedsak permanente. Derfor ønsker man ikke å lagre for eksempel et bilde av et ansikt eller et fingeravtrykk, men heller avledede data som bare kan brukes til gjenkjenning. På denne måten kan vi unngå at biometriske systemer bygger opp sårbare databaser med sensitiv informasjon.

Kryptografi er teknikker som skal beskytte informasjon mot uønsket innsyn og endring.[15] *Ste-*

[13] Myndigheten för samhällsskydd och beredskap (2015): *Informationssäkerhet – trender 2015.*

[14] Advanced Persistent Threat (APT).

ganografi er et relatert begrep som handler om å skjule det faktum at informasjon sendes, gjerne ved å gjemme informasjon i annen leselig informasjon for ikke å tiltrekke seg oppmerksomhet.

En vesentlig trend er at kommunikasjon og lagrede data i økende grad krypteres. Et viktig element i denne trenden er at leverandører av hyllevare og nettbaserte tjenester tar i bruk kryptering som standard, slik at det ikke lenger er noe brukeren selv trenger å konfigurere. Denne trenden er et svar på høyst reelle sikkerhetsproblemer. Kryptering av mobile enheter kan for eksempel hindre at privat informasjon kommer på avveie dersom enheten mistes eller blir stjålet. Det samme gjelder ukryptert kommunikasjon som kan avlyttes. Åpen ubeskyttet kommunikasjon kan også være en måte å lure inn skadevare i folks datamaskiner på.[16] Til en viss grad er kryptering i senere tid også blitt tatt i bruk som et svar på masseovervåking. Myndighetsaktører i flere land har ytret ønske om å forby eller regulere bruken av kryptografi.

En ny fremtidsrettet krypteringsteknologi er såkalte fullt homomorfiske kryptosystemer, forkortet FHE[17]. Vanligvis er det umulig å arbeide med krypterte data uten først å dekryptere dem. Med FHE er det mulig å gjøre beregninger på krypterte data under visse forutsetninger. Det tradisjonelle eksempelet er nettsøk, som er en av dagens utfordringer for personvernet. Med FHE kan man tenke seg at brukeren sender et kryptert søk til søketjenesten. Søketjenesten gjennomfører søket og kommer frem til et kryptert svar som den sender tilbake til brukeren. Brukeren kan så dekryptere svaret. Slik kan brukeren gjennomføre et nettsøk uten at søketjenesten vet hva søket handler om. Da FHE først ble presentert i 2009, var det som en teoretisk konstruksjon som ikke kunne gjennomføres i praksis. Siden den gang har det vært en rivende utvikling som vil kunne forbedre personvernet.

En kilde til usikkerhet i kryptografien er såkalte kvantedatamaskiner. Kvantedatamaskiner virker på en fundamentalt annerledes måte enn vanlige datamaskiner. Det gjør at kvantedatamaskiner vil være i stand til å bryte noen klasser av kryptosystemer som er mye brukt i dag. Selv om kvantedatamaskiner er blitt demonstrert, har de så langt ekstremt liten kapasitet. Det er usikkert om, og eventuelt når, vi vil være i stand til å bygge praktiske kvantedatamaskiner. Likevel har arbeidet med å utvikle og standardisere alternativer til de «sårbare» kryptosystemene begynt. Det er grunn til å tro at dette arbeidet vil være ferdig i god tid før noen eventuelt klarer å bygge en praktisk kvantedatamaskin. Man bør imidlertid være klar over at informasjon som er kryptert med «sårbare» systemer, ikke nødvendigvis vil opprettholde konfidensialitet på sikt.

Et tilsynelatende relatert fagfelt er kvantekryptografi, der resultater fra kvantemekanikken brukes til å bygge fysiske kryptosystemer som i teorien ikke kan brytes. I praksis har slik kvantekryptografi blitt brutt en rekke ganger.

---

15 Se også punkt 5.4.2 om kryptografi.

16 Et eksempel er at kriminelle kompromitterer det trådløse nettverket på hotell. Når en hotellgjest leser en nettavis, kan de kriminelle injisere skadevare i nettsidene til avisen.

17 Fully Homomorphic Encryption.

Kapittel 7
Utilsiktede og tilsiktede IKT-hendelser

Når IKT-hendelser blir oppdaget, starter prosessen med å finne ut hva som er årsakene. Det kan være forskjellige former for naturhendelser og svikt, eller det kan være tilsiktede angrep. Avhengig av årsak og hvem som står bak, vil det være flere måter å håndtere situasjonen på. For eksempel ved å følge med på angriper eller stoppe angrepet, begrense skade og gjenopprette systemer. For mange angrep forblir angriperen ukjent, til tross for tidkrevende analyse.

I Norge har Næringslivets Sikkerhetsråd i en årrekke beskrevet det digitale sårbarhetsbildet hos norske virksomheter, og flere aktører utgir periodiske trussel- og risikobilder, deriblant Nasjonal sikkerhetsmyndighet, Etterretningstjenesten og Politiets sikkerhetstjeneste. Internasjonalt er det mange som jevnlig rapporterer om IKT-situasjonen.

Det er stor variasjon knyttet til forutsigbarhet og konsekvens når det gjelder utilsiktede og tilsiktede hendelsestyper. Naturhendelser kan i stor grad predikteres basert på historisk statistikk, det samme gjelder til dels også menneskelig og teknisk svikt. For noen typer tilsiktede hendelser, som visse hyppige former for IKT-kriminalitet, vil det også tegnes et mønster. For eksempel blir «tagging» på websider, tjenestenektangrep og kjente datavirus observert svært hyppig. Sofistikerte angripere som skjuler sporene sine, for eksempel ved skjult inntrenging, informasjonslekkasjer og informasjonstyverier, er vanskeligere å oppdage og å forutsi.

7.1 Utilsiktede IKT-hendelser

7.1.1 Naturhendelser

Værfenomen på jorden. De vanligste værfenomenene her til lands er storm, flom, skred og brann. Sterk vind får trær til å knekke og falle ned på høyspentledninger, og skred river av kabler både i bakken og i master. Dette er hendelser som treffer oss regelmessig, og sannsynligheten for å bli rammet er avhengig av geografiske forhold. Øst-Norge er lite utsatt for sterk vind, mens Nord-Norge og Vestlandet er mer utsatt. Stormen Dagmar i 2011 førte til strømbortfall, og det samme skjedde under ekstremværet Hilde i 2013. Flommen i Gudbrandsdalen i 2013 førte til driftsforstyrrelser på grunn av fiberbrudd og strømbrudd. Under Lærdals-brannen i januar 2014 brant mobile knutepunkter opp. Hendelser som gir utfall av strømforsyningen til et område, vil i stor grad ramme elektronisk kommunikasjon og datasystemer. Bortfall av elektronisk kommunikasjon har vist seg å forsterke konsekvensene av naturkatastrofer, da det kompliserer krisehåndteringen og samhandlingen mellom redningsmannskaper, kommuner og private.

Romvær. Mange ganger i løpet av et år sender solen koronamasse ut i verdensrommet. Dette er et solstormfenomen som normalt blir absorbert av atmosfæren, men kan forstyrre jordens elektromagnetiske felt dersom utbruddet er kraftig. Endringer i magnetfelt kan indusere skadelig strøm i strømlinjer og elektroniske komponenter. Små strømstyrker vil føre til forstyrrelser i IKT-utstyr, og blir strømmen for sterk, vil kretsene brenne opp. I 2012 var vi ganske nær ved å bli truffet av et kraftig utbrudd. Hvis denne stormen hadde truffet atmosfæren en uke tidligere, ville massive skyer med magnetisert plasma ha truffet jorden. Den etterfølgende solstormen ville blitt minst like sterk som Carrington-hendelsen i 1859, som hadde en enormt ødeleggende kraft. Samfunnet var ikke elektrifisert på samme måte som i dag, så konsekvensene den gang kan ikke sammenliknes med konsekvensene hendelsen ville fått i dagens samfunn.

Beskyttelsen mot solstormer er noe mindre rundt polene, og det gjør at vi i Norge er ekstra utsatt. Konsekvensene av en «100-års solstorm» er vurdert til å gi forstyrrelser i satellittsignaler og strømutfall, med de følgeskadene det vil gi.[1]

[1] Direktoratet for samfunnssikkerhet og beredskap (2015): *Nasjonalt risikobilde 2014.* Scenario 09 Romvær.

7.1.2 Svikt

Mennesket. Et kjent uttrykk er at «mennesket er det svakeste leddet», og vi mennesker gjør feil selv med de beste intensjoner. Det er dokumentert at svak lederforankring, menneskelige feilhandlinger og ubevissthet, samt organisatoriske forhold, er årsaker til mangelfullt sikkerhetsarbeid og uønskede hendelser i IKT-systemer.[2] [3] Sensitive dokumenter blir sendt til feil mottakere, fiberkabler blir gravd over, og systemoppgraderinger feiler av og til katastrofalt.

Det er flere årsaker til at menneskelig svikt oppstår. Det kan dreie seg om lav brukervennlighet i sikkerhetstiltak og manglende sikkerhetskunnskap. Mennesker kan ha problemer med å følge kompliserte rutiner, særlig når de ikke forstår hvordan systemet virker. Utviklere og sikkerhetsledere må derfor ta hensyn til brukerne når de lager systemer og sikkerhetsrutiner, slik at det blir lett å bruke systemene sikkert og riktig. Bare 40 prosent av norske virksomheter gir sine ansatte slik opplæring ved nyansettelse, og bare 20 prosent gir opplæring senere i løpet av ansettelsesperioden.[4]

Utover intuitive sikkerhetstiltak og opplæring vil enkeltindividets holdninger til sikkerhetsarbeidet og sikkerhetskulturen i miljøet rundt påvirke sikkerhetsnivået. Det kan oppstå konflikter mellom det å prioritere sikkerhetsrutiner og det å få oppgaver gjort tidsnok. I tillegg er det alltid en sjanse for at det blir gjort tilfeldige feil.[5]

Det er viktig å være klar over at ansatte ofte vil erstatte tungvinte systemer og rutiner med enklere systemer og rutiner. Disse kan ha et helt annet sikkerhetsnivå. Enkeltindividet er under stort press og tillagt stort ansvar for sikkerhetsnivået. Man bør derfor spørre seg om det alltid er riktig å skylde på menneskelig svikt. Sikkerhetsrutiner kan være svært vanskelige å følge i praksis. For eksempel får ansatte beskjed om å være svært forsiktige med å trykke på lenker og åpne e-post-vedlegg, samtidig som det å åpne vedlegg er en naturlig og nødvendig del av arbeidet deres.

Organisatorisk svikt. Selv om tradisjonelle og modne sikkerhetstiltak er utbredt hos norske virksomheter og IKT-systemene teknisk sett blir mer motstandsdyktige, tyder mørketallsundersøkelser utgitt av NSR på at det er manglende kunnskap om informasjonssikkerhet ute i virksomhetene. Virksomhetene har ikke oversikt over hvilke verdier de besitter, og under halvparten har gjort en verdivurdering av informasjonen sin.[6] ENISA vurderer at mer enn halvparten av de vellykkede IKT-angrepene skyldes slurv fra virksomhetene.[7] De enklest utnyttbare sårbarhetene internasjonalt skyldes ifølge Cisco programvare som er utdatert på grunn av manglende sikkerhetsoppdateringer.[8]

Systemsvikt. Systemteknisk svikt starter ofte med at enkeltkomponenter bryter sammen, ofte som følge av overbelastning. Elektronikk kan kortslutte eller ta fyr, harddisker slutter å fungere, og logiske feil i programkode ender med systemfeil. Mange kjenner seg igjen i ufrivillig å ha mistet dokumenter, bilder og videoklipp som følge av systemsvikt, og mange oppdager i slike situasjoner at sikkerhetskopier ikke er tilgjengelige, eller at de er utdaterte – en kombinasjon av teknisk og menneskelig svikt.

Når sikkerhetsmekanismene enten mangler eller ikke blir fulgt opp tilstrekkelig, vil slike hendelser raskt kunne forplante seg i avhengige og nærliggende systemer. Strømutfallet i en ekomsentral i Ålesund 2014 førte til store tjenesteavbrudd på grunn av mangelfull alarmhåndtering, kombinert med at adgangen til sentralen var elektrisk styrt.

Et annet relevant eksempel er Tieto-hendelsen fra Sverige mot slutten av 2011.[9] Teknisk svikt hos en driftsleverandør førte til at både primær- og reservesystemet for lagring av data hos leverandøren sviktet. Ny maskinvare var på plass etter kort tid, men prosessen med å gjenopprette dataene tok flere uker. En serie uhell forsterket av manglende beredskapsplanlegging førte til at cirka 50 virksomheter, både offentlige og private, mistet datatjenester i opptil flere uker. Blant disse var 350 apotekfilialer, som ikke fikk delt ut resep-

---

2 Forsvarets forskningsinstitutt (2014): FFI-Rapport 2014/00948. *Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet.*

3 Hagen, J (2009): *How do employees comply with security policy? A comparative case study of four organizations under the security act. In: The human factor behind the Security Perimeter, Evaluating the effectiveness of organizational information security measures and employees' contribution to security.* Universitetet i Oslo.

4 Næringslivets sikkerhetsråd (2014): *Mørketallsundersøkelsen 2014 – Informasjonssikkerhet, personvern og datakriminalitet.*

5 IEEE Volume 7, Issue: 4 (2009): *Human Relationships: A Never-Ending Security Education Challenge? Security & Privacy.*

6 Næringslivets sikkerhetsråd (2014): *Mørketallsundersøkelsen 2014 – Informasjonssikkerhet, personvern og datakriminalitet.*

7 ENISA (2012): *ENISA Threat landscape 2012.*

8 CISCO (2015): *Annual security report.*

9 Myndigheten för samhäldsskydd och beredskap (2012): *Reflections on civil protection and emergency preparedness during major IT incidents.*

ter, og det svenske biltilsynet, som ikke fikk effektuert kjøretillatelser.

Tieto-hendelsen i 2011 viser en sterk avhengighet av driftsleverandøren, og er et eksempel på stor grad av konsentrasjonsrisiko. Konsentrasjonsrisiko innebærer at mange avhengigheter peker i samme retning. Den amerikanske sosiologien Charles Perrow har fremhevet at kompleksitet, tett kobling og lineære interaksjoner påvirker risikoen for systemsvikt.[10] Disse egenskapene er tydelige i det digitale samfunnet, der komponenter, systemer og menneskelige handlinger kobles stadig tettere sammen gjennom blant annet tingenes Internett, automatisering og systemintegrasjon.

7.2 Tilsiktede IKT-hendelser

IKT-kriminalitet, digitale angrep, spionasje, sabotasje og terror brukes i utvalgets mandat for å omtale tilsiktede hendelser.[11] Begrepene kan henvise til ulike grupper av trusselaktører, som har ulik motivasjon, ulik tilgang på ressurser og ulik grad av kunnskap og organisering. Motivene spenner fra å demonstrere ferdigheter og påvise sårbarheter til å utøve makt og politisk press. Angrep kan være målrettet mot et spesifikt offer, eller de kan være opportunistiske ved å ramme tilfeldige.

Blant de minst teknisk avanserte truslene har vi såkalte «script kiddies» og sosiale hackere. Dette er ofte enkeltpersoner på jakt etter utfordringer, og de bruker helst eksisterende hackerverktøy eller sosial manipulasjon. Kripos er bekymret for at det bygges opp nettverk av unge mennesker i Norge som lærer hverandre ulike former for IKT-kriminalitet uten fullt ut å skjønne konsekvensene av slike lovbrudd. Det er også en fare for at slike nettverk kan fungere som rekrutteringsarena for alvorligere former for IKT-kriminalitet.[12]

De som representerer trusler med høy kapasitet, de såkalte sofistikerte angriperne, kan være statlige eller statsfinansierte grupperinger som bryter seg inn i IKT-systemer for å samle inn informasjon knyttet til politiske eller militære formål. Motivene kan i ytterste konsekvens være forberedelser til fremtidige sabotasjeoperasjoner. Leverandører, utviklere og operatører knyttet til kritisk infrastruktur er utsatte grupper, for eksempel i forbindelse med plassering av digitale bakdører og utro tjenere.

I spennet mellom disse ytterpunktene kan det være mange ulike aktører. Politisk motiverte enkeltpersoner og grupper bruker digitale verktøy for å true og påvirke. De kalles ofte *hacktivister*. Økonomisk motiverte kriminelle bruker forskjellige former for svindel og ID-tyveri. *Cyberterrorister* tilhører ideologisk motiverte grupper som bruker IKT for å ramme grupper eller samfunnsfunksjoner med vold eller trusler om vold. Selv virksomheter kan tenkes i rollen som trusselaktør dersom de søker å oppnå konkurransefortrinn ved hjelp av ulovlig innsamling av informasjon eller destruktive dataangrep mot konkurrenter.

Aktørene benytter seg av ulike metoder og verktøy: Anonymiseringstjenester, kryptering og virtuell valuta blir stadig mer avansert, og Europol uttrykker bekymring for denne utviklingen.[13] Teknikkene er med på å skjule hvem som kommuniserer, og hva som blir sagt, og vanskeliggjør sporing av økonomiske transaksjoner.

Skadevare («malware») benytter tekniske sårbarheter for å oppnå tilgang og rettigheter til utstyret den infiserer. Skadevare kan klassifiseres etter spredningsform, som virus, orm, bakdør eller trojansk hest. De kan også klassifiseres ut fra intensjon, som reklamevare, løsepengevirus, spionprogramvare og logiske bomber[14]. Mange trusselaktører samler maskiner de tar kontroll over, i store nettverk kalt *botnett*. Dette foregår ved at en bakdør installeres på maskinen, som i sin tur opprettholder kontakten med kommandoinfrastrukturen under kontroll av trusselaktøren. En aktør med tilgang til et stort botnett kan bruke den totale datakraften til eksempelvis å sende ut spam, automatisk generere klikk på nettannonser, overbelaste nettsteder med datatrafikk eller tjene penger ved å misbruke utregningskraft.[15] Se for øvrig boks 7.1.

«*Crime-as-a-service*». Det har oppstått et globalt marked for kjøp og salg av tjenester for å understøtte IKT-kriminalitet,[16] der kriminelle fritt kan kjøpe kriminelle tjenester som botnett, tjenes-

[10] Perrow, Charles (1984): *Normal Accidents: Living with High Risk Technologies.* Basic Books.

[11] Se definisjoner i kapittel 21 «Avdekke og håndtere digitale angrep».

[12] Kripos (2014): *Trendrapport 2015 – den organiserte kriminaliteten i Norge.*

[13] Europol (2014): *The internet organized crime threat assessment* (IOCTA).

[14] Skadevare som utløses ved en forhåndsdefinert hendelse i systemet eller på et bestemt tidspunkt.

[15] For eksempel deltagelse i beregningsnettverk for «mining» av digitale kryptopenger.

[16] UNODC (2013): *Comprehensive Studyon Cybercrime (Draft).*

Boks 7.1 Nyttevare eller skadevare?

Det er et faktum at grensen mellom nyttig programvare og skadevare i en del tilfeller ikke er klar. Etter som trusselen øker, utvikles det stadig flere sikkerhetsverktøy for å dekke behovet for overvåking, analyse og reaksjon. Brukt på en annen måte kan sikkerhetsverktøy bli en del av et innbruddsverktøy. Eksempler på det er programvare for å lese av passerende datatrafikk og for å søke etter åpne porter over datanettverk.

I 2015 ble det kjent at private tekstmeldinger ble oppbevart i en skjult fil i en mobilapplikasjon utviklet av en strømleverandør. Programkode utviklet under test ble liggende igjen i produksjonsversjonen. Eksemplet belyser det faktum at en ondsinnet aktør kan lage en tilsvarende nyttig applikasjon som på enkelt vis kan sende tekstmeldingene dine til et arkiv ute på Internett.

tenektangrep, utvikling av skadevare, data- og passordtyveri på et globalt marked. Det har gjort IKT-kriminalitet attraktivt for tradisjonelle organiserte kriminelle grupper. Dette markedet er modent, og trolig større enn narkotikamarkedet.[17] Her handler ulike aktører, både stater, organisasjoner og privatpersoner.

Sosial hacking. Med økende grad av tekniske barrierer kan kriminelle oppleve det som vanskeligere å gå direkte på systemene. Da er det lettere å gå indirekte via menneskene i organisasjonen. En vanlig metode er å sende ansatte persontilpassede e-postmeldinger (nettfiskeangrep) med infiserte vedlegg eller linker. En annen metode er oppringing for å lure den ansatte til å oppgi informasjon om virksomhetens sikkerhetssystemer. Det er erfaringsmessig alltid noen som lar seg lure av slike angrep,[18] og det rapporteres om en økning i antall nettfiskeangrep.[19] Tilsvarende kan også foregå via SMS og sosiale medier.

Kriminelle bak nettbankangrep trenger ofte hjelp til å sende penger ut av landet, og rekrutterer derfor hvitvaskere (money mules), som for eksempel stiller kontoen sin til disposisjon. Kjente prinsipper er manipulasjon basert på fristelser, autoritet, tiltrekning og sympati. I eksemplet med hvitvaskere kan det være høy lønn, bonus og muligheten til å jobbe hjemmefra det fristes med. Tiltrekning kan misbrukes ved at kriminelle oppretter falske profiler på nettdatingtjenester for å innlede falske forhold og lure offeret til å overføre penger. Det er også flere eksempler på at politi- og myndighetslogoer blir misbrukt i kombinasjon med «bøter», og falske veldedighetsorganisasjoner kan utnytte vår sympati til å lure fra oss verdier.

7.2.1 IKT-kriminalitet

Internasjonalt. Europol gir årlig ut rapporter med vurderinger av gjeldende og forventede trender innenfor organisert Internett-kriminalitet.[20] Rapporten for 2015 beskriver at IKT-kriminalitet[21] skiller seg fra annen kriminalitet ved at den kriminelle ikke trenger å være i fysisk nærhet til offeret, kan angripe flere ofre samtidig og med minimale muligheter for å bli oppdaget. Som en konsekvens reises behovet for mer samarbeid mellom politimyndigheter på tvers av landegrenser. Slikt samarbeid blir riktignok hindret ved at flere jurisdiksjoner utenfor Europa mangler juridiske rammeverk for slikt samarbeid.

I en studie av FN som sammenligner 21 land, rapporterer mellom 1 prosent og 17 prosent av befolkningen at de har vært utsatt for kriminalitet via Internett, som kredittkortsvindel, ID-tyveri, nettfiskeforsøk og ulovlig adgang til e-postkonto. Til sammenligning rapporterte mindre enn 5 prosent av befolkningen i studien at de hadde vært utsatt for konvensjonell kriminalitet. Blant europeiske bedrifter rapporterte mellom 2 prosent og 16 prosent at de hadde vært utsatt for cyberkriminalitet.[22]

I henhold til internasjonal rett skal kriminelle saker ivaretas av det enkelte lands interne politi og rettsvesen. En rapport fra FN hevder at å beskytte seg mot cyberkriminalitet globalt er så komplekst at det ikke kan løses av stater enkelt-

[17] Ablon, Lillian, Martin C. Libicki og Andrea A. Golay (2014): *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar.* Santa Monica, CA: RAND Corporation, 2014.

[18] Nasjonal sikkerhetsmyndighet (2015): *Sikkerhetsfaglig råd.* Side 15.

[19] Symantec (2015): *Internet Security Threat Report.*

[20] Europol: *The Internet Organised Crime Threat Assessment (IOCTA)*.

[21] IKT-kriminalitet er IKT-hendelser som er kriminalisert etter norsk lov, og deles ofte inn i kriminalitet rettet mot selve IKT-systemene, og kriminelle handlinger begått ved hjelp av IKT som et vesentlig redskap. Kapittel 21 omtaler IKT-kriminalitet i konteksten av å avdekke, håndtere og etterforske digitale angrep.

[22] UNODC (2013): *Comprehensive Study on Cybercrime (Draft)*.

vis, men må løses gjennom etablerte samarbeidsfora og bilateralt.[23] Det nærmeste man kommer en helhetlig tilnærming, er enn så lenge Europakonvensjonen mot cyberkriminalitet.[24]

Etter hvert som antall Internett-brukere, inkludert mobilbrukere, globalt stiger, vil virksomheter og innbyggere i EU kunne bli utsatt for et stadig større antall digitale angrep fra utviklingsland. Relativt større rikdom, avansert infrastruktur og økende avhengighet av Internett innenfor økonomi og betalingssystemer gjør EU-landene til attraktive mål for cyberkriminelle, samtidig som angrepene stort sett gjennomføres fra land utenfor EU.[25] Men vel så viktig er den sårbarheten utviklingsland utsetter seg selv for, da med tanke på landenes modenhet på IKT-sikkerhetsområdet. Utenriksdepartementet skriver at «Norge kan spille en viktig rolle i å bistå med kapasitetsbygging på cyberfeltet i utviklingsland slik at flere land i større grad også evner å håndtere digitale utfordringer og digitale trusler». Et av tiltakene til regjeringen er å intensivere samarbeidet og dialogen med EU om slik kapasitetsbygging.[26]

IKT-kriminaliteten i Norge. Ifølge Kripos er IKT-kriminalitet i ferd med å bli et reelt samfunnsproblem. Den teknologiske utviklingen har ført til at tradisjonell kriminalitet kan begås på nye måter, blant annet ved bruk av Internett. Oppdagelsesrisikoen er lav og fortjenestepotensialet høyt. Bruk av Internett som kommunikasjonskanal utfordrer politiets bekjempelse av en rekke former for kriminalitet – som bedragerier, seksuelle overgrep og narkotikakriminalitet.[27]

Det pågår kontinuerlig forsøk på å innhente personlig informasjon som senere skal brukes til kriminelle handlinger. Identitetstyveri, bedrageri og planting av skadelig programvare er bare noen av metodene som benyttes. Det finnes en rekke eksempler på tjenestenektangrep mot banker, mediehus, politiske partier, myndigheter og offentlig sektor. Disse angrepene kan være både ideologiske, politiske, økonomiske og personlig motivert.

Så godt som alle de norske bankene har opplevd at kriminelle infiserer kundenes PC-er med skreddersydd og skadelig programvare i den hensikt å gjennomføre urettmessige pengetransaksjoner. Kripos vurderer det som svært sannsynlig at norske banker vil bli utsatt for omfattende hackerforsøk der profesjonelle aktører står bak.[28]

Det er en utvikling i retning av at stadig flere typer bedragerier finner sted med Internett som kommunikasjonskanal mellom lovbryter og offer.[29] Svindel på digitale markedsplasser er et økende problem, både med ulovlige og falske varer.

I en NorSIS-undersøkelse fra 2014 oppgir 3,2 prosent av befolkningen at de har opplevd at noen har benyttet deres identitet til å begå straffbare handlinger. Dette er en nedgang fra 5,9 prosent i 2013.

Flere mennesker blir i dag ofre for cyberkriminalitet enn for konvensjonell kriminalitet. Forsikring mot ID-tyveri er også i ferd med å innta forsikringsmarkedet.

Internetts opplevde anonymitet, utbredelse og billige tilgang, sammen med utbredelsen av digitale muligheter for bilder og film, gjør at produksjonen og tilgjengeligheten av overgrepsbilder øker raskt, både nasjonalt og internasjonalt. Internett benyttes også i økende utstrekning til kjøp og salg av ulike typer narkotika og bestanddeler som kan brukes til å fremstille syntetiske narkotiske stoffer.[30]

Europakonvensjonen mot cyberkriminalitet beskriver flere former for IKT-kriminalitet rettet mot selve teknologien, blant annet:

Uautorisert tilgang til et IKT-system kan oppnås for eksempel ved å utføre et datainnbrudd eller ved å misbruke autorisasjon. Enhver datamaskin, spesielt når den er tilkoblet Internett, kan ha verdi for en angriper med økonomiske motiver. Selv en tilfeldig infisert maskin uten spesielt interessant innhold kan benyttes til blant annet angrep på andre datamaskiner, lagring av ulovlige filer, utsendelse av «spam», innhenting av brukerkonti og kredittkortnumre og en rekke andre formål. Dette kan igjen omsettes for penger. I 2010 var det store oppslag om at noen hadde skaffet seg ulovlig tilgang til regjeringens ugraderte IKT-systemer gjennom et datainnbrudd, og at store mengder dokumenter hadde blitt kopiert. Lekkasje av data kan også skje ved ulovlig avlytting av

---

23 Krutskikh, A.V. (2012): *Developments in the Field of Information and telecommunications in the Context of International Security.* Study Series 33, Part 1: A/65/201, United Nations, New York.

24 Council of Europe (2001): *Convention on Cybercrime, Additional Protocol, Budapest, 23.XI.2001. ETS No 185.*

25 Europol (2014): *The internet organized crime threat assessment (IOCTA).*

26 Meld. St. 37 (2014–2015) *Globale sikkerhetsutfordringer i utenrikspolitikken – Terrorisme, organisert kriminalitet, piratvirksomhet og sikkerhetsutfordringer i det digitale rom.* Side 60.

27 Politiet (2010–2012): *Tendenser i kriminaliteten.*

28 Kripos (2014): *Trendrapport 2015 – den organiserte kriminaliteten i Norge.*

29 Politiet (2010–2012): *Tendenser i kriminaliteten.*

30 Ibid.

datakommunikasjon der informasjon overføres uten sterk kryptering eller tilsvarende beskyttelse.

Hindre tiltenkt funksjonalitet til et IKT-system. Det har vært en økning i antall distribuerte tjenestenektangrep (DDoS) i Norge. Det kan være ideologiske, politiske, økonomiske eller personlige motiver som ligger bak tjenestenektangrep.[31] Politiets datanettverk ble i 2009 infisert av skadevaren «conficker», noe som førte til to uker med nedetid. Et tjenestenektangrep ble i 2014 rettet mot norske banker og andre store bedrifter av en 17-åring. Angrepet pågikk bare noen timer. Konsekvensene var hovedsakelig økonomiske tap samt noe nedetid på systemene som ble rammet. *Jamming* er en form for tilsiktet interferens med hensikt å blokkere sendere eller mottakere av radiokommunikasjon. Rent teknologisk har slikt utstyr blir lettere, billigere og mer effektivt.[32]

Utvikling og distribusjon av verktøy og metoder for å utføre handlingene som er nevnt ovenfor, hører også til IKT-kriminalitetsformen rettet mot selve teknologien. Eksempler er utvikling av skadevare og distribusjon av stjålne tilgangsdata i forbindelse med ID-tyveri.

Kostnaden ved IKT-kriminalitet

Mange land ønsker å vite hva IKT-kriminalitet koster. Dette skaper et behov for nøyaktig statistikk over IKT-kriminalitet og økonomiske tap. Imidlertid er mange av studiene på dette området gjort av organisasjoner med en agenda. Eksempler er sikkerhetsselskaper og politiske organisasjoner. En pekepinn på omfanget gir Center for Strategic and International Studies (CSIS), som har estimert at de årlige globale tapene knyttet til IKT-kriminalitet er på mellom 375 milliarder og 575 milliarder dollar per år på verdensbasis. IKT-kriminalitet ødelegger handel, konkurranseevne og innovasjon.

For Norge ligger CSIS-estimatet på cirka 20 milliarder kroner. Dette tallet står i skarp kontrast til det norske virksomheter selv rapporterer at de har hatt av direkte og indirekte tap, i Mørketallsundersøkelsen 2014. Det er stor usikkerhet knyttet til norske mørketall både når det gjelder antall estimerte hendelser, og når det gjelder kostnader som følge av hendelser. Et problem er at norske virksomheter ikke vet at de er angrepet. Mørketallsundersøkelsen viser store avvik mellom estimerte hendelser og hendelser som er anmeldt til politiet. Sammenligner vi data fra NSM og mnemonic med svar fra store virksomheter, ser vi at over halvparten har vært utsatt for datainnbrudd i en eller annen form, og ikke bare 5 prosent som det er rapportert om i Mørketallsundersøkelsen.

7.2.2 Sabotasje, spionasje og terror

Antall registrerte hendelser ved NSM NorCERT øker. NSM vurderer denne økningen som en indikasjon på at aktivitet fra ulike trusselaktører øker, til tross for at både antall sensorer og antall nasjonale og internasjonale samarbeidspartnere øker. Dette er blant annet basert på hva internasjonale samarbeidsparter beskriver. Figur 7.1 viser antall hendelser per kvartal siden 2011.

Fra 2011 til 2014 økte antallet håndterte hendelser og antallet hendelser klassifisert som alvorlige hos NSM NorCERT. Tallene for 2015 viser en nedgang. Nedgangen i antall håndterte angrep kan forklares med et unormalt høyt nivå i tredje kvartal 2014. Nedgangen i antall klassifiserte alvorlige hendelser forklares av NSM med en kombinasjon av økt kompleksitet og endrede prioriteringer av bistand.[33] Se figur 7.2.

Vi må anta at sofistikerte aktører kan trenge gjennom kryptografiske beskyttelsesmekanismer og kompromittere systemer før de når kunden, og at de har høy kapasitet når det gjelder å oppdage svakheter i programvare som ikke bevisst er satt inn.

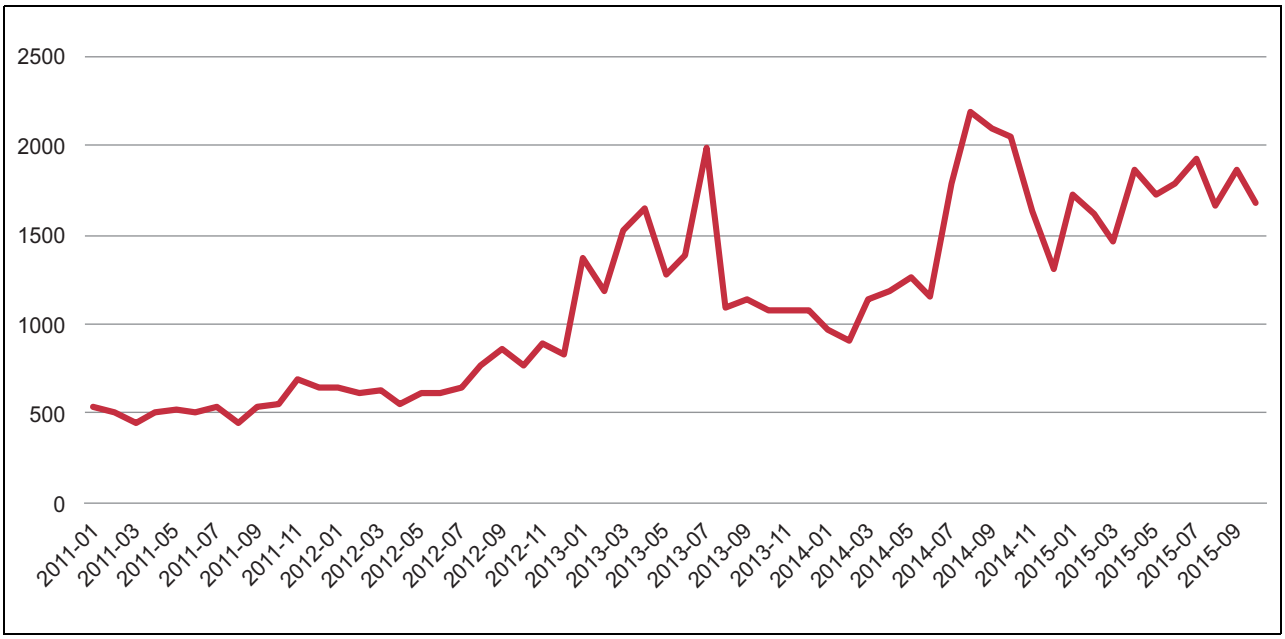
Sofistikerte aktører kan angripe kryptografisk beskyttelse ved hjelp av kryptoanalyse, ved å stjele nøkler eller ved å sabotere komponenter i kryptosystemet. En angriper kan enten angripe tegningene til systemet, byggingen av systemet eller selve systemet under transport til kunden, og det er grunn til å tro at sofistikerte angripere manipulerer systemer under transport til kundene.

Nesten all programvare vi bruker, inneholder sårbarheter med varierende grad av kompleksitet og alvorlighet. Sofistikerte aktører angriper systemer ved å finne og utnytte sårbarheter i programvaren. Det er mange eksempler på feil som er funnet i programkode, men det er uklart om det er bevisste eller utilsiktede feil. Det er grunn til å tro at sofistikerte angripere er vesentlig bedre

[31] Kripos (2014): *Trendrapport 2015 – den organiserte kriminaliteten i Norge.*

[32] Forsvarets forskningsinstitutt (2004): *TEK14: Militærteknologiske trender – Oversiktsrapport.*

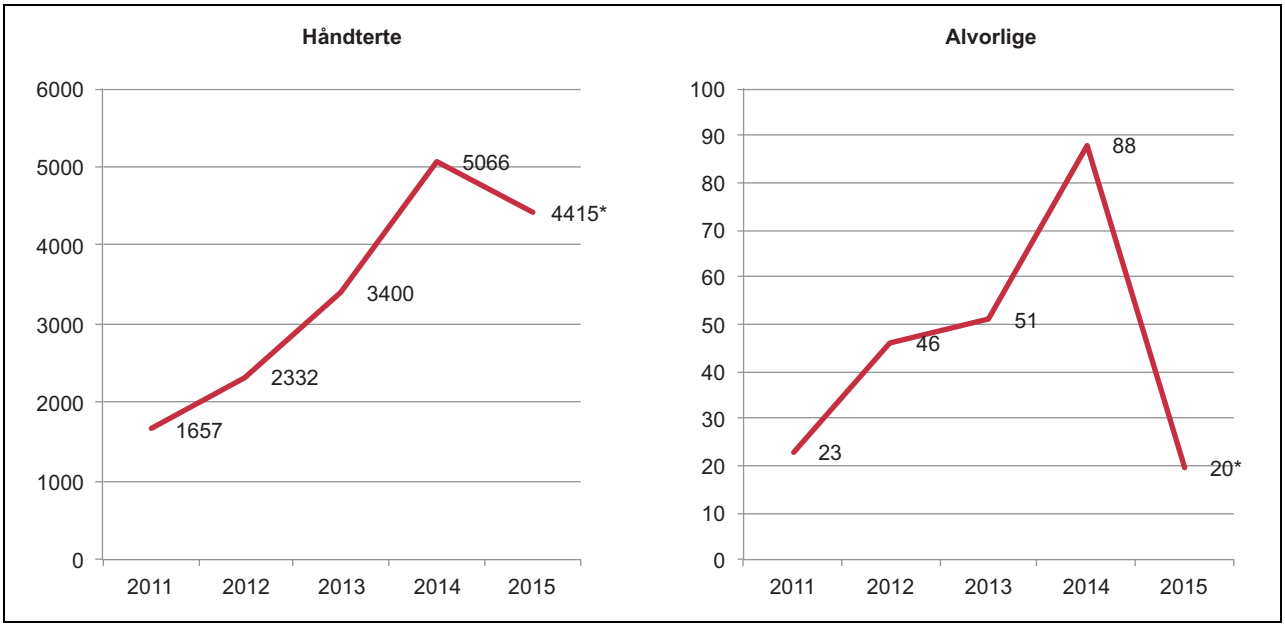
[33] NSM sier at hver enkelt sak krever mer bistand på grunn av kompleksitet og omfang. Skadevaren blir også mer kompleks og tar lengre tid å analysere. I 2015 fikk eiere av kritisk infrastruktur eller samfunnskritiske funksjoner betydelig høyere prioritet.



Figur 7.1 Det har vært en økning i antall registrerte hendelser. Den kraftige økningen i fjerde kvartal 2014 skyldes et målrettet angrep mot olje- og gassektoren.

enn akademikere og andre åpne analytikere[34] til å finne sårbarheter i programvare. Vi må legge til grunn at velfinansierte, sofistikerte angripere er i stand til å bygge opp større grupper, som ikke bare kan analysere programvare mer systematisk, men også er i stand til å bygge et miljø, samt utvikle og vedlikeholde analyseverktøy. Slike grupper vil være i stand til å finne sårbarheter som akademikere eller åpne analytikere ikke har kapasitet til å finne. De vil også ha en mye større total analysekapasitet.

[34] Analytikere som offentlig publiserer sine funn.



Figur 7.2 Oversikt over antall manuelt håndterte og antall alvorlige saker observert ved NSM NorCERT.[1]

* Tallene for 2015 er et lineært estimat fra henholdsvis 2943 og 13 saker per 31. august 2015.

[1] Nasjonal sikkerhetsmyndighet (2015): *Helhetlig IKT-risikobilde 2015.*

I det påfølgende er åpne kilder benyttet for å beskrive sentrale aktørers vurdering av digital spionasje, sabotasje og terrorisme. Tekstutdrag er gjengitt i teksten for å unngå å forvrenge budskapet.

Digital spionasje

Digitaliseringen av det norske samfunnet og internasjonaliseringen av forskning og næringsliv har forenklet arbeidsvilkårene for fremmede etterretningstjenester.[35] Risikoen for spionasje (også kalt nettverksbaserte etterretningsoperasjoner) mot norske verdier vurderes å være høy og økende. Flere større norske virksomheter har ikke kapasitet til å håndtere nivået på flere av trusselaktørene, og de har i varierende grad evne til å oppdage at sikkerhetsgradert og annen sensitiv informasjon blir stjålet. En liten leverandør med lav sikkerhetsbevissthet kan utgjøre en vesentlig sårbarhet for en stor kunde. Skadepotensialet er stort på grunn av økt sammenkobling på tvers av sektorer og at systemer kobles til Internett. NSM ser at datahaller ofte er dårligere sikret enn markedsføringen og verdiene tilsier. Sosiale media har skapt nye arenaer der det er lett å forsnakke seg om sensitive forhold. For eksempel har mange forsvarsansatte delt informasjon om utenlandsoppdrag i sosiale medier uten å ha sjekket sikkerheten i disse systemene.[36]

Ifølge Etterretningstjenesten angriper fremmed etterretning daglig norsk digital infrastruktur, og det er statlige aktører som står bak den mest alvorlige trusselen.[37] Vurderinger av spionasjetrusselen tar blant annet utgangspunkt i de land Norge oppfatter å ha motstridende interesser med. Blant de land Norge ikke har et sikkerhetspolitisk samarbeid med, vurder PST at Russland er den staten med størst kapasitet og skadepotensial knyttet til etterretning mot norske interesser (herunder nettverksbaserte etterretningsoperasjoner), etterfulgt av Kina. Datanettverksoperasjoner[38] vurderes som den etterretningsmetoden som kan ha de mest alvorlige og omfattende skadevirkningene på hele spekteret av norske interesser.

Russiske myndigheter har i mange år benyttet seg av nettverksbaserte etterretningsoperasjoner for å skaffe seg informasjon om andre lands politiske beslutninger samt aktuelle militære og finansielle forhold. Russland har under Ukraina-konflikten benyttet nettverksbaserte etterretningsoperasjoner i kombinasjon med en rekke andre virkemidler.

Kinesiske nettverksbaserte etterretningsoperasjoner har først og fremst til hensikt å understøtte landets økonomiske vekst og være et redskap for å innhente Vestens teknologiske forsprang. Operasjonene utføres av en rekke statlige og ikke-statlige grupperinger. Sentrale sektorer innen kinesisk industri understøttes av den statlige etterretningsvirksomheten.

Utover disse vises det til at enkelte andre stater har etablert samarbeid mellom sine hemmelige tjenester og organiserte kriminelle som utfører nettverksbaserte etterretningsoperasjoner på deres vegne.

Metadata etterlatt i digitale tjenester, som sosiale medier, kan ved analyse avdekke kunnskap om både enkeltpersoner, grupper og lokasjoner. E-tjenesten fremhever at utenlandsk etterretning kan få tilgang til denne kunnskapen der disse tjenestene blir forvaltet gjennom skytjenester, og ved serverparker i utlandet.

Angrepsmetodene preges i dag av e-post og kompromitterte websider med skadelig innhold (vannhull[39]). Utnyttelse av tjeneste- og underleverandører brukes også som en indirekte vei til målet gjennom sammenkoblede nettverk eller gjennom felles brukere.

Et internasjonalt eksempel på tyveri av informasjon er hackergruppen Dragonfly, som hadde som mål å stjele informasjon. Gruppen benyttet to typer ondsinnet programvare i angrepet, begge såkalte fjernstyrings- og tilgangsverktøy. Disse ble distribuert gjennom e-post, vannhullsangrep og programvare lastet ned fra leverandørene av industrikontrollsystemer. Et annet eksempel er Telenor som i 2013 ble rammet av målrettede forsøk på datatyveri mot nøkkelpersonell.

Digital sabotasje

Nettverksbasert sabotasje utgjør en alvorlig, men foreløpig langt mindre spesifikk trussel enn etterretningstrusselen. Fremmede makter kan gjennom nettverksbaserte etterretningsoperasjoner i fredstid erverve inngående kjennskap til kritisk

[35] Politiets sikkerhetstjeneste (2015): *Åpen trusselvurdering 2015.*

[36] Nasjonal sikkerhetsmyndighet (2015): *Risiko 2015.*

[37] Etterretningstjenesten (2015): *Etterretningstjenestens vurdering, FOKUS.*

[38] Datanettverksoperasjoner er av NSM definert som «Datatangrep, datainnbrudd via internett».

[39] En metode der skadevare plantes på steder der det er sannsynlig at målgruppen vil bli eksponert. For eksempel gjennom å kompromittere annonsefunksjonalitet på en populær webside.

infrastruktur. Kunnskapen kan senere benyttes til å gjennomføre sabotasjeaksjoner. Flere stater utvikler skadevare som vil kunne brukes til å sabotere infrastruktur eller forstyrre kritiske samfunnsfunksjoner. Utviklingen minner mer og mer om et våpenkappløp. Skadevare kan ramme alle systemer som er koblet til nett. Brannmurer og antivirusprogramvare er ingen garanti mot kompromittering, selv om slike tiltak reduserer risikoen.

Internasjonalt finnes det eksempler på digital sabotasje med militærpolitisk motivasjon, kanskje så langt tilbake som tidlig på 1980-tallet. Bekreftelse på hvem som står bak slike sabotasjehandlinger, får vi sjelden, og om vi får det, er det lenge etter at handlingen fant sted. Det spekuleres i om eksplosjonen i de sovjetiske transsibirske gassledningene i 1982 var forårsaket av en innplantet logisk bombe i programvaren til styringssystemet. Andre tidlige eksempler er sabotasjeaksjoner mot serbiske og syriske luftvernsystemer for å sette disse ut av spill under de alliertes luftoperasjoner.

I nyere tid har vi blant annet sett digitale angrep mot Estland i 2007, der tjenestenektangrep ble brukt i stor skala for å avskjære befolkningen fra myndighetene, samt andre viktige samfunnsfunksjoner som bankvesenet. Websider ble kompromittert for å spre propaganda. I 2008 eksploderte rørledninger i Baku i Aserbajdsjan, og det er også der mistanke om manipulasjon av overvåkingssystemene. I 2010 herjet Stuxnet-skadevaren, som var utviklet for å sabotere sentrifugeanlegg for å anrike grunnstoffet uran i Iran. Et tysk stålverk fikk store skader i 2014 som følge av et digitalt innbrudd i kontrollsystemene.[40]

Digital terrorisme

Angrep i og gjennom det digitale rom er også attraktivt for idelogiske grupperinger og privatpersoner. Disse kan bruke enkle, nedlastbare verktøy for eksempel for å endre på websider eller gjennomføre nektelsesangrep. Mer avanserte angrep mot godt beskyttede systemer krever imidlertid helt andre ressurser både til å drive etterretning og til å utføre selve angrepet. Realisering av den digitale terrortrusselen er foreløpig begrenset av trusselaktørenes mangel på evne og kunnskap.[41]

Terrorister bruker Internett til rekruttering, spredning av ideologi og til å samle inn informasjon om hvordan de kan lage bomber. De bruker kodede meldinger ved hjelp av teknikker som skjuler meldinger i vanlig tekst i e-post og på nettsider. I tillegg stenges og åpnes nettsider stadig, noe som gjør det vanskelig å spore dem. Å stoppe slik aktivitet er bortimot umulig.[42] Internett er en viktig arena for rekruttering, radikalisering og spredning av propaganda.[43]

---

40 BBC (2014): «Hack attack causes 'massive damage' at steel works».

41 Etterretningstjenesten (2015): *Etterretningstjenestens vurdering, FOKUS.*

42 Hubbard, Z.P. (2007): *Information Operations in the Global Ear on terror: Lessons Learned From Operations in Afghanistan and Iraq. In Information Warfare. Separating hype from reality*, L. Armistead, ed., Dulles, Virginia: Potomac Books Inc, pp. 45–72.

43 Politiets sikkerhetstjeneste (2015): *Åpen trusselvurdering 2015.*

Kapittel 8
Organisering av roller og ansvar

8.1 Overordnede mål og prinsipper for IKT-sikkerhetsarbeidet

IKT-sikkerhet følger de fire overordnede prinsippene for samfunnssikkerhet – ansvar, nærhet, likhet og samvirke.[1]

Ansvarsprinsippet innebærer at den myndigheten, virksomheten eller etaten som til daglig har ansvaret for et område – for eksempel en funksjon eller et system – også har ansvaret for nødvendige sikkerhets- og beredskapsforberedelser og for den utøvende tjenesten ved kriser og katastrofer.

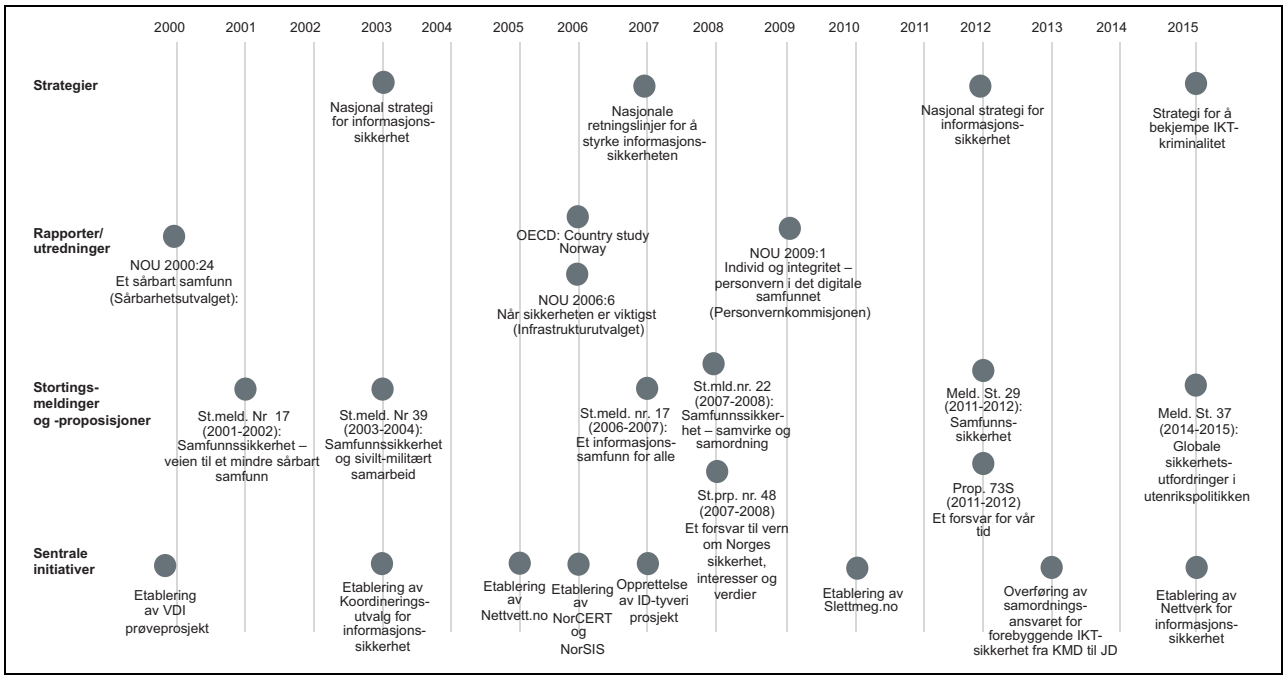
Likhetsprinsippet innebærer at den organisasjonen man opererer med under kriser, skal være mest mulig lik den organisasjonen man har til daglig. Dette er en utdyping av ansvarsprinsippet, og innebærer at ansvarsforholdene internt og mellom virksomheter/organisasjoner ikke skal endres i forbindelse med krisehåndtering.

Nærhetsprinsippet innebærer at kriser organisatorisk skal håndteres på lavest mulig nivå. Dette bygger på en forutsetning om at den som har størst nærhet til krisen, i de fleste tilfeller også vil ha best situasjonsforståelse og være best egnet til å håndtere krisen.

Samvirkeprinsippet viser til at myndigheten, virksomheten eller etaten har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering. For å sikre en best mulig utnyttelse av ressurser på tvers av sektorer er det et stort behov for samarbeid på tvers av ansvarsområder.

En rekke utredninger og strategier peker på utfordringer innen IKT-sikkerhet, og flere initiativer er iverksatt for å redusere sårbarhetene. Figur 8.1 gjengir utvalgte sentrale, tverrsektorielle dokumenter og initiativer de siste 15 årene.

[1] St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet – veien til et mindre sårbart samfunn* og Meld. St. 29 (2011–2012) *Samfunnssikkerhet*.



Figur 8.1 Sentrale utredninger og IKT-sikkerhetsinitiativer i Norge i perioden 2000 – 2015. Figuren er ikke uttømmende.

Nasjonal strategi for informasjonssikkerhet ble lansert i 2012, og angir retning og prioriteringer for myndighetenes informasjonssikkerhetsarbeid. Strategien definerer fire overordnede mål for informasjonssikkerhetsarbeidet, som igjen er operasjonalisert gjennom sju strategiske prioriteringer:

- å ivareta informasjonssikkerheten på en mer helhetlig og systematisk måte
- å styrke IKT-infrastrukturen
- å sørge for en felles tilnærming til informasjonssikkerhet i statsforvaltningen
- å sikre samfunnets evne til å oppdage, varsle og håndtere alvorlige IKT-hendelser
- å sikre samfunnets evne til å forebygge, avdekke og etterforske IKT-kriminalitet[2]
- kontinuerlig innsats for bevisstgjøring og kompetanseheving
- høy kvalitet på nasjonal forskning og utvikling innenfor informasjons- og kommunikasjonssikkerhet

Strategien slår fast at IKT-sikkerhet først og fremst er den enkelte virksomhetens ansvar. Fagdepartementene har et overordnet ansvar for å ivareta sikkerheten i sektorens IKT-infrastruktur og for at det forebyggende IKT-sikkerhetsarbeidet i sektoren er tilfredsstillende.

Til strategien er det utarbeidet en handlingsplan med konkrete tiltak og fordeling av ansvar for oppfølging. I 2014 initierte Justis- og beredskapsdepartementet en rapportering fra departementene om oppfølgingen av strategi- og handlingsplanen. Rapporteringen viste at alle departementene er kjent med strategien, og at det er iverksatt en rekke tiltak på bakgrunn av denne. Justis- og beredskapsdepartementet ser imidlertid behov for ytterlige oppfølging, og har på bakgrunn av dette gitt en individuell tilbakemelding til hvert departement.

Departementenes ansvar for samfunnssikkerhet og beredskap følger av en instruks fra 2012.[3] Formålet med instruksen er å fremme et helhetlig og koordinert samfunnssikkerhets- og beredskapsarbeid som bidrar til å øke samfunnets evne til å forebygge kriser og uønskede hendelser og til å håndtere kriser. Instruksen stiller krav til både forebyggende beredskapsarbeid og evne til å håndtere kriser. Instruksen fastsetter at departementene blant annet skal

- på grunnlag av oversikt over risiko og sårbarhet i egen sektor og DSBs nasjonale risikobilde vurdere risiko, sårbarhet og robusthet i kritiske samfunnsfunksjoner i egen sektor som grunnlag for kontinuitets- og beredskapsplanlegging og hensiktsmessige øvelser, samt arbeide systematisk for å utvikle og vedlikeholde oversikten over risiko og sårbarhet i egen sektor
- vurdere og iverksette forebyggende og beredskapsmessige tiltak
- dokumentere at det er gjennomført tiltak som avbøter manglende robusthet i kritisk infrastruktur og funksjoner innenfor departementets ansvarsområde
- være forberedt på å håndtere alle typer kriser i egen sektor og yte bistand til andre departementer i kriser som involverer flere sektorer
- være forberedt på å være lederdepartement

Punktene over omfatter alle typer forebygging, beredskap og krisehåndtering, inkludert IKT-hendelser. Kravene fra instruksen er bindende, og det blir ført tilsyn med departementenes oppfølging av kravene. En oversikt over ansvar for ulike samfunnsfunksjoner fremgår av vedlegg 25.2.

Styringsverktøyene til den enkelte statsråden og de enkelte departementene overfor underlagte etater og virksomheter er det årlige tildelingsbrevet, virksomhetenes rapportering på måloppnåelse, instrukser, etatsstyringsmøter med mer. Departementene er gjennom den tidligere nevnte instruksen[4] pålagt å «synliggjøre mål og prioriteringer for samfunnssikkerhets- og beredskapsarbeidet i de årlige budsjettproposisjonene».

I tillegg skal de kunne «dokumentere at det er gjennomført tiltak som setter dem i stand til å ivareta prioriterte funksjoner og oppgaver i hele krisespekteret, herunder også forebyggende tiltak og at virksomheter i egen sektor er i stand til å ivareta ansvar for kritiske samfunnsfunksjoner uavhengig av hvilke hendelser som måtte inntreffe». Videre er sektorenes regelverk og tilsynsvirksomhet sentrale. Disse er nærmere omtalt for de samfunnsområdene NOU-en beskriver.

---

[2] Dette punktet er fulgt opp gjennom Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet, medio 2015.

[3] Justis- og beredskapsdepartementet (2012: Kgl.res. 15.6.2012: *Instruks for departementenes arbeid med samfunnssikkerhet og beredskap, Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering.*

[4] Ibid.

8.2 Sentrale myndighetsaktører med særlig ansvar for oppfølging av IKT-sikkerhet

Utover det generelle ansvaret til alle fagdepartementene har enkelte departementer og underlagte virksomheter en særskilt rolle knyttet til IKT-sikkerhet.

Statsministerens kontor (SMK) bistår statsministeren i å lede og samordne regjeringens arbeid, også i en krisesituasjon. SMKs involvering i den enkelte krisen vil avhenge av krisens art, omfang med videre. I kriser som faller innenfor beredskapslovens virkeområde, er statsministeren delegert særskilte fullmakter i situasjoner der det er uomgjengelig nødvendig å treffe beslutninger for å ivareta samfunnets interesser. Statsministerens kontor må planlegge for at statsministeren og regjeringen skal kunne utføre sine oppgaver også i krisesituasjoner, og for at kontoret skal kunne utføre oppgaver som sekretariat for regjeringskonferanser, Regjeringens sikkerhetsutvalg (RSU) og Kongen i statsråd. Kontoret må kunne yte både administrativ støtte og sekretariatsfunksjoner og bidra med rådgivning.[5] Statsministerens kontor har ansvar for beskyttelsesinstruksen.

Justis- og beredskapsdepartementet (JD) har en generell samordningsrolle for samfunnssikkerhet og beredskap i sivil sektor, og et samordningsansvar innen IKT-sikkerhet. Justis- og beredskapsdepartementet har videre et overordnet ansvar for å bekjempe IKT-kriminalitet.

Justis- og beredskapsdepartementets totale ansvar for IKT-sikkerhet utledes fra

- instruks for departementenes arbeid med samfunnssikkerhet og beredskap, Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering (kgl.res. 15. juni 2012)
- overføring av samordningsansvaret for forebyggende IKT-sikkerhet fra Fornyings-, administrasjons- og kirkedepartementet til Justis- og beredskapsdepartementet (kgl.res. 22. mars 2013)
- fordeling av ansvar for forebyggende sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet (kronprinsreg.res. 4. juli 2003)

I kgl.res. 15. juni 2012 fremgår følgende:

> «Departementet skal gjennom sin samordningsrolle sikre et koordinert og helhetlig arbeid med samfunnssikkerhet og beredskap på tvers av sektorgrenser.»

I kronprinsreg.res. 4. juli 2003 går det frem at JD skal ha

> «et overordnet sektorovergripende ansvar – konstitusjonelt og parlamentarisk – for forebyggende sikkerhet i sivil sektor i henhold til sikkerhetsloven».

I forbindelse med overføringen ble Justis- og beredskapsdepartementets ansvar ytterligere konkretisert i kgl.res. 22. mars 2013, ved at departementet skal

- utforme en nasjonal politikk og nasjonale krav på IKT-sikkerhetsområdet som omfatter offentlig og privat sektor
- utarbeide og følge opp nasjonale strategier med tilhørende handlingsplaner
- identifisere sektorovergripende spørsmål og bidra til at ansvar blir plassert og oppgaver håndtert på en god måte
- drive arenaer for erfaringsutveksling
- bidra til bevisstgjørings- og veiledningsaktiviteter rettet mot hele samfunnet, for eksempel gjennom tilskudd til Norsk senter for informasjonssikring (NorSIS)
- ivareta kontakten med næringslivet, for eksempel gjennom Næringslivets Sikkerhetsråd
- være Norges deltager i internasjonale fora og bidra til at internasjonale relasjoner på området blir håndtert på tvers av departementsområder
- videreutvikle et fagmiljø (NSM) som kan understøtte JD

Justis- og beredskapsdepartementet fører jevnlig tilsyn med departementenes arbeid med samfunnssikkerhet og beredskap. Tilsynene utføres av DSB på vegne av JD, og er basert på risiko og vesentlighet. Departementenes ansvar for å ta vare på kritisk infrastruktur og kritiske samfunnsfunksjoner inngår som et viktig tema i tilsynene. En nærmere redegjørelse av PODs, PSTs og Kripos' ansvar er beskrevet i kapittel 21 «Avdekke og håndtere digitale angrep».

Forsvarsdepartementet (FD) har ansvar for forebyggende IKT-sikkerhet i forsvarssektoren. FD skal, som overordnet ansvarlig for sektoren, sørge for at informasjonssikkerhet i cyberdomenet og cyberoperasjoner er en integrert del av departementets planleggings-, ledelses- og styringsprosess. FD har blant annet etatsstyringsansvar for Nasjonal sikkerhetsmyndighet (NSM) og forvaltningsansvar for sikkerhetsloven.

---

[5] Forsvarsdepartementet, Justis- og beredskapsdepartementet (2015): *Støtte og samarbeid. En beskrivelse av totalforsvaret i dag.*

Forsvaret planlegger, leder og gjennomfører alle militære operasjoner i hele krisespekteret. Forsvaret planlegger, etablerer, drifter, forsvarer og utvikler Forsvarets kommunikasjonsinfrastruktur og leverer administrative og operative IKT-systemer til forsvarssektoren. Forsvarsdepartementets underliggende etat Etterretningstjenesten er beskrevet i kapittel 21 «Avdekke og håndtere digitale angrep».

Begrepet *sivilt–militært samarbeid* omfatter i prinsippet alt sivilt–militært samarbeid på alle nivåer og spenner over et svært bredt felt med mange ulike aktører. Begrepets innhold er i stor grad situasjonsbetinget. I noen tilfeller støtter Forsvaret sivil virksomhet, mens Forsvaret i andre situasjoner støttes av sivile ressurser.

Totalforsvaret som konsept skal sikre en best mulig utnyttelse av samfunnets begrensede ressurser når det gjelder forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering i hele krisespekteret. Totalforsvarskonseptet er dermed en del av et sivilt–militært samarbeid, men er avgrenset til å omfatte gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunnet i forbindelse med kriser.

Utenriksdepartementet (UD) har som oppgave å arbeide for Norges interesser internasjonalt. Norges interesser bestemmes blant annet av vår geografiske plassering i et strategisk område, vår åpne økonomi, vår posisjon som kyststat og forvalter av store marine ressurser og en omfattende eksport av olje og gass. UDs rolle innenfor IKT-sikkerhet er primært å samarbeide med andre berørte departementer og bistå med koordinering av norsk deltagelse på ulike arenaer. I tillegg kan UD spille en rolle i å fremme norsk næringsliv og norsk teknologi og i å samarbeide med norsk næringsliv på aktuelle arenaer når det er naturlig. UD vil ha en ledende rolle på arenaer der cybersikkerhet diskuteres i en internasjonal kontekst. Blant annet uttrykkes det i UDs stortingsmelding om globale sikkerhetsutfordringer i utenrikspolitikken at det skal etableres en gruppe «for koordinering av norske posisjoner i internasjonal cyberpolitikk for å styrke arbeidet med å fremme norske interesser og verdier i det digitale rom internasjonalt».[6]

Samferdselsdepartementet (SD) har ansvar for en fungerende og sikker IKT-infrastruktur og for IKT-sikkerheten knyttet til elektroniske kommunikasjonsnett og -tjenester, herunder Internett. I tillegg har SD ansvar for å sikre pålitelig person- og godsfremføring på sjø, vei, bane og i luften. SDs ansvar for elektronisk kommunikasjon er regulert gjennom lov om elektronisk kommunikasjon med forskrifter, og følges opp av Nasjonal kommunikasjonsmyndighet (Nkom). Nkom er nærmere beskrevet i kapittel 11 «Elektronisk kommunikasjon».

Kommunal- og moderniseringsdepartementet (KMD) har ansvar for å koordinere regjeringens IKT-politikk, og har et særskilt ansvar for å arbeide for en styrket og mer helhetlig tilnærming til informasjonssikkerhet i statsforvaltningen. KMD har etatsstyringsansvar for Departementenes servicesenter (DSS), som leverer IKT-tjenester til elleve av departementene, og for Direktoratet for forvaltning og IKT (Difi). KMD har i tillegg ansvar for regjeringens personvernpolitikk og etatsstyringsansvar for Datatilsynet.

Nasjonal sikkerhetsmyndighet (NSM) er et nasjonalt fagmiljø for IKT-sikkerhet og skal understøtte og bidra til utøvelsen av FDs og JDs ansvar på IKT-sikkerhetsområdet. NSMs oppgaver er å

- etablere og vedlikeholde et IKT-risikobilde som omfatter statssikkerhet, samfunnssikkerhet og individsikkerhet, og foreslå tiltak, gi anbefalinger og fremme forslag til krav innen IKT-sikkerhet i samfunnet, samt følge opp med råd og veiledning
- utøve et overordnet og sektorovergripende ansvar for forebyggende sikkerhetstjeneste i henhold til sikkerhetsloven
- utøve sertifiseringsmyndighet for IKT-sikkerhet i produkter og systemer (SERTIT)
- organisere og drive et nasjonalt varslingssystem for digital infrastruktur
- koordinere håndteringen av alvorlige IKT-angrep mot samfunnskritisk infrastruktur og andre viktige samfunnsfunksjoner
- koordinere arbeidet mellom myndigheter som har en rolle innenfor forebyggende IKT-sikkerhet, og legge til rette for hensiktsmessig samhandling mellom disse
- være Norges representant i internasjonale fora innen forebyggende sikkerhet og i bi- og multilateralt samarbeid på fagområdet
- gi støtte til norsk kryptoindustri
- ved behov iverksette nødvendige beredskapsmessige tiltak innenfor gitte fullmakter, herunder i sikkerhetsloven og i Nasjonalt beredskapssystem (NBS)

NSM fører tilsyn med styringssystemer for sikkerhet i virksomheter som er underlagt sikkerhetsloven, sikring av digital informasjon gradert

[6] Meld. St. 37 (2014–2015) *Globale sikkerhetsutfordringer i utenrikspolitikken – Terrorisme, organisert kriminalitet, piratvirksomhet og sikkerhetsutfordringer i det digitale rom.*

etter sikkerhetsloven og sikring av objekter klassifisert som skjermingsverdige i henhold til sikkerhetsloven. Et stort antall av de skjermingsverdige objektene er komponenter i digital infrastruktur.

Regjeringen har i Forsvarets langtidsplan for 2012 lagt opp til at NSM skal videreutvikles som det sentrale direktoratet for beskyttelse av informasjon og infrastruktur av betydning for samfunnskritiske og andre viktige samfunnsfunksjoner.[7] Dette har materialisert seg gjennom en jevn økning av tildelingen til NSM i inneværende langtidsperiode, styrking av NorCERT-funksjonen i 2013 og en styrking av rådgivningsfunksjonen for IKT-sikkerhet i 2015.

Direktoratet for samfunnssikkerhet og beredskap (DSB) har et samordningsansvar for samfunnssikkerhet og beredskap på vegne av JD som også omfatter IKT-området. DSBs arbeid med IKT-sikkerhetsspørsmål omfatter forebygging, tilsiktede og ikke-tilsiktede hendelser og gjenoppretting. DSB fører tilsyn med departementenes styringssystem for IKT-sikkerhet, med hjemmel i kgl.res 20. juni 2012 på vegne av JD. DSB gjennomfører et systemrettet tilsyn og går ikke i dybden på tekniske løsninger. DSB gjennomfører halvårlige møter med NSM for å samordne tilsynsvirksomheten.

DSB har ansvar for å gjennomføre nasjonale øvelser på tvers av sektorer, der det blant annet øves på IKT-scenarioer. DSB understøtter JDs samordningsrolle innen samfunnssikkerhet og beredskap og legger til rette for tverrsektorielle arenaer for samarbeid, blant annet gjennom arbeidet med Nasjonalt risikobilde (NRB) og Kritisk infrastruktur og kritiske samfunnsfunksjoner (KIKS). Ved større hendelser og krisesituasjoner har DSB ansvar for å sammenstille tverrsektoriell informasjon fra lokalt, regionalt og direktoratsnivå for å bidra til en felles situasjonsforståelse for kriserådet og JD.

Direktoratet for forvaltning og IKT (Difi). KMDs ansvar for å arbeide for en styrket og mer helhetlig tilnærming til informasjonssikkerhet i offentlig forvaltning er delegert til Difi. I tråd med handlingsplanen til Nasjonal strategi for informasjonssikkerhet er det bygd opp en seksjon for informasjonssikkerhet i Difi som skal utgjøre et kompetansemiljø for informasjonssikkerhet i statsforvaltningen. Difi har også ansvar for veiledning av internkontroll for informasjonssikkerhet etter eForvaltningsforskriften for offentlig sektor. I tillegg er Difi ansvarlig for flere felleskomponenter i offentlig sektor og for informasjonssikkerheten i disse løsningene. Dette gjelder blant annet utvikling og forvaltning av ID-porten og digital postkasse.

Datatilsynet er en faglig uavhengig forvaltningsmyndighet i medhold av personopplysningsloven. Personopplysningsloven med forskrift er en tverrsektoriell lov og spesielt utformet med tanke på digital bruk av personopplysninger. Tilsynet forvalter derfor også myndighet etter flere andre lover, blant annet helseregisterloven og politiregisterloven. Tilsynet kontrollerer at personopplysninger blir behandlet i samsvar med lov og forskrift, herunder at det etableres nødvendig og tilstrekkelig informasjonssikkerhet ved innsamling, bruk, lagring og utlevering av opplysninger. Kontrollen utøves dels gjennom forhåndskontroll, konsesjon, og dels gjennom etterkontroll i form av tilsyn.

Personvernnemnda er klageorgan for Datatilsynets beslutninger. Personvernmyndighetene er administrativt underlagt KMD, mens ansvaret for personopplysningsloven ligger i JD. Datatilsynet har også en ombudsrolle overfor befolkningen og gir bistand i form av råd og veiledning. Videre bistår Datatilsynet bransjeorganisasjoner med råd og utarbeidelse av normer for å sikre personopplysninger i virksomheter.

Fylkesmannen har i henhold til egen instruks ansvar for å samordne, holde oversikt over og informere om samfunnssikkerhet og beredskap i fylket. Det innebærer blant annet en plikt til å ha oversikt over risiko og sårbarhet i fylket. I den forbindelse kan Fylkesmannen innhente nødvendige opplysninger fra alle statlige, fylkeskommunale og kommunale myndigheter i fylket. Fylkesmannen innhenter også nødvendig informasjon fra øvrige relevante virksomheter med ansvar for kritiske samfunnsfunksjoner i fylket. I tillegg skal Fylkesmannen ha oversikt over og samordne myndighetenes krav og forventninger til kommunenes samfunnssikkerhets- og beredskapsarbeid. Fylkesmannen fører også tilsyn med kommunenes samfunnssikkerhets- og beredskapsarbeid og oppfølging av lov om kommunal beredskapsplikt og rapporterer til DSB på området.

Kommunene har et generelt og grunnleggende ansvar for å ivareta befolkningens sikkerhet og trygghet innenfor sitt geografiske område. Gjennom kommunal beredskapsplikt er kommunene blant annet pålagt et ansvar for å gjennomføre en helhetlig risiko- og sårbarhetsanalyse, herunder kartlegge, systematisere og vurdere sannsynligheten for uønskede hendelser som kan inntreffe i kommunen, og hvordan disse kan påvirke

[7] Prop. 73 S (2011–2012) *Et forsvar for vår tid.*

kommunen. Kommunene har også et ansvar for å være forberedt på å håndtere uønskede hendelser, og skal med utgangspunkt i den helhetlige risiko- og sårbarhetsanalysen utarbeide en overordnet beredskapsplan. Kommunens overordnede beredskapsplan skal samordne og integrere øvrige beredskapsplaner i kommunen.

8.3 Øvrige aktører

Nedenfor listes en rekke sentrale aktører innen IKT-sikkerhet opp. Utover dette er det en rekke sektorvise responsmiljøer, interesseorganisasjoner og foreninger. Disse er beskrevet i de øvrige kapitlene. Det samme gjelder utdanningsinstitusjoner, forskningsinstitutter og forskningsprogrammer som er sentrale for utdanning innen IKT-kompetanse og forskning på IKT-relaterte problemstillinger.

Norsk senter for informasjonssikring (NorSIS) er en uavhengig og ideell virksomhet som jobber for å styrke informasjonssikkerheten i samfunnet. Målgruppen er små og mellomstore norske virksomheter, herunder kommunene. NorSIS jobber aktivt i media og med å skape møteplasser. NorSIS tilbyr veiledning på nett, kurs og konferanser, arrangerer Nasjonal sikkerhetsmåned og drifter tjenestene slettmeg.no og idtyveri.no.

Teknologirådet er et uavhengig, offentlig organ som gir råd til Stortinget og regjeringen om ny teknologi. Deres visjon er «teknologiråd for fremtidens samfunn». Teknologirådet skal gi Stortinget og øvrige myndigheter nyskapende og begrunnede innspill om ny teknologi og sette muligheter og utfordringer ved ny teknologi på dagsordenen.

Næringslivets Sikkerhetsråd (NSR) er en medlemsforening uten profittformål, og representerer gjennom sine stifterorganisasjoner og medlemmer bredden i norsk næringsliv. NSR er en privat organisasjon som ikke er tillagt myndighetsutøvelse, men deltar i forebyggende og utviklende arbeid og har formalisert samarbeid med en rekke myndigheter. NSR fungerer som en samarbeidsarena og et knutepunkt mellom næringslivet og myndighetene, og arbeider i hovedsak med forebyggende rådgivning og veiledning overfor bedrifter i norsk næringsliv. Et overordnet mål for NSR er å styrke bedriftenes egen evne til å ivareta IKT-sikkerhet helhetlig og systematisk innenfor egen organisasjon, og søkelyset er rettet mot de grunnleggende tiltakene virksomhetene selv kan iverksette for å beskytte seg, heller enn på trusselaktørene og risikobildet. NSR gir både generelle og spesielle råd til næringslivet om alle former for IKT-hendelser som kan ramme medlemsvirksomhetene, og veileder næringslivet generelt og medlemmene spesielt om hvor de bør henvende seg hvis de mistenker at de er utsatt for IKT-kriminalitet.

Næringslivets sikkerhetsorganisasjon (NSO) er en privat organisasjon med myndighetsoppgaver innen industrivern. NSO rapporterer til Direktoratet for samfunnssikkerhet og beredskap (DSB) og Næringslivets Hovedorganisasjon (NHO). Deres myndighetsoppdrag innebærer å følge opp – herunder føre tilsyn med – cirka 1 100 virksomheter som har plikt til å etablere industrivern i henhold til forskrift om industrivern. Industrivern er beredskap innen sikkerhet/safety. NSO har ikke myndighetsoppgaver innen sikring/security.

KS er kommunesektorens interesse- og arbeidsgiverorganisasjon i Norge. Alle landets 428 kommuner og 19 fylkeskommuner er medlemmer i KS, i tillegg til mer enn 500 bedrifter. *KommIT* er et program i KS som skal høyne forståelsen av og kunnskapen om IKT som virkemiddel for effektivisering og kvalitetsheving i kommunal forvaltning og tjenesteproduksjon.

Den Norske Dataforening (DND) er Norges største IT-faglige forening, og er et åpent, frittstående forum av og for IT-profesjonelle og avanserte IT-brukere. Dataforeningen skal være et samlende fagmiljø for utøvere og brukere av IT-fagene. En av oppgavene deres er å belyse problemstillinger vedrørende informasjonsteknologi og databehandling overfor norske offentlige myndigheter, andre faglige sammenslutninger og allmenheten, blant annet for å bidra til å heve det generelle kunnskapsnivået om IT.

Norsk Informasjonssikkerhetsforum (ISF) er en ideell organisasjon som arbeider med informasjonssikkerhet for medlemmene. Medlemmene er organisasjoner innen offentlig forvaltning og privat næringsliv, og de har uttrykt et ønske om å etablere og opprettholde et høyt sikkerhetsnivå. ISF jobber for å være det foretrukne samlende fagmiljøet for informasjonssikkerhet og for å heve sikkerhetsnivået hos medlemsvirksomhetene og i det norske samfunnet generelt.

IKT-Norge er IKT-næringens interesseorganisasjon og har 440 medlemsbedrifter, som representerer en omsetning på 120 milliarder kroner. IKT-Norge er opptatt av at myndigheter, næringsliv og brukere skal ha tillit til IKT-produkter og -systemer. Deres interesser innen sikkerhet omfatter alt fra enkle problemstillinger som virus og trojanere til sårbarhet i digital samfunnskritisk

infrastruktur og problemstillinger rundt personvern.

Riksrevisjonen skal bidra til at fellesskapets midler og verdier blir brukt og forvaltet slik Stortinget har bestemt. Dette gjør de gjennom revisjon, kontroll og veiledning. Bakgrunnen er at de har myndighet til å kontrollere at arbeidet med samfunnssikkerhet som politikerne har bestemt blir fulgt opp. De rapporterer til Stortinget, og de er dermed et viktig og sterkt virkemiddel for å følge opp politiske vedtak, også på samfunnssikkerhetsområdet.

8.4 Sentrale koordineringsarenaer for IKT-sikkerhet

Kriserådet er det overordnede administrative koordineringsorganet som ivaretar og sikrer strategisk koordinering. Kriserådet har fem faste medlemmer; regjeringsråden ved Statsministerens kontor, utenriksråden i Utenriksdepartementet og departementsrådene i Justis- og beredskapsdepartementet, Helse- og omsorgsdepartementet og Forsvarsdepartementet. Rådet suppleres med departementsråder fra andre departementer og ledere fra berørte etater avhengig av krisens karakter. Kriserådet gjennomfører faste møter og møter ved behov, der overordnede beredskaps- og krisehåndteringsutfordringer drøftes for å sikre god samordning av departementenes beredskaps- og krisehåndteringsarbeid.

Regjeringens sikkerhetsutvalg (RSU) er et politisk utvalg som ledes av statsministeren og er regjeringens organ for å diskutere og ta beslutninger i viktige graderte sikkerhets- og beredskapsspørsmål. Det avholdes møter i RSU minst én gang hver måned. Sikkerhetsutvalget har faste medlemmer. I tillegg møter statsråder fra berørte departementer og representanter fra ulike relevante etater, avhengig av hvilke saker som behandles. I juli 2015 ble det besluttet å opprette et sekretariat for RSU. Sekretariatet skal ledes av en fagdirektør som er ansatt på Statsministerens kontor. Håndtering av IKT-angrep med nasjonale konsekvenser vil være en typisk hendelse som håndteres i RSU.

Departementenes samordningsråd for samfunnssikkerhet ble etablert i 2007 og er et forum for informasjons- og erfaringsutveksling mellom departementene i arbeidet med samfunnssikkerhet og beredskap, redningstjeneste og sivilt–militært samarbeid. Rådet består av representanter for alle departementene og Statsministerens kontor. Justis- og beredskapsdepartementet har en tilretteleggende funksjon for rådet, og alle departementene har ansvar for å ta initiativ til å bringe aktuelle og relevante problemstillinger til drøfting. Samordningsrådet utgjør en felles arena i departementsfellesskapet for å drøfte overordnede retningslinjer og rammer for sikkerhets- og beredskapsarbeidet.[8]

Ifølge kgl.res. fra 2012 skal Justis- og beredskapsdepartementet legge til rette for systemer for en robust, helhetlig og koordinert kommunikasjon mellom myndighetene og for at dette blir ivaretatt blant annet gjennom koordinering av informasjon i samordningsrådet.

Koordinerings- og rådgivningsutvalget (KRU) er et samarbeidsorgan for spørsmål som gjelder etterretnings- og sikkerhetstjenestene, og et rådgivningsutvalg for de berørte statsrådene. Utvalgets oppgaver er å ivareta overordnet koordinering av de tre tjenestenes arbeidsoppgaver, prioriteringer og mål og å analysere og utrede felles problemstillinger knyttet til trusselbildet. Deltagere i KRU er én representant fra Forsvarsdepartementet, én representant fra Justis- og beredskapsdepartementet og én representant fra Utenriksdepartementet, alle på ekspedisjonssjefnivå eller høyere, sjefen for Etterretningstjenesten, sjefen for Nasjonal sikkerhetsmyndighet og sjefen for Politiets sikkerhetstjeneste.

Nettverk for informasjonssikkerhet er en møteplass for departementene for å drøfte sentrale tema innen informasjonssikkerhet og er et verktøy for JDs samordningsansvar for forebyggende IKT-sikkerhet i sivil sektor. Nettverket ble etablert høsten 2015 og erstatter det tidligere Koordineringsutvalget for informasjonssikkerhet (KIS). Sentrale oppgaver omfatter blant annet å følge opp implementeringen av Nasjonal strategi for informasjonssikkerhet og drøfte behovet for å iverksette tverrsektorielle tiltak.

Sentralt totalforsvarsforum er det forumet på etatsnivå som i størst grad representerer bredden i totalforsvaret. Forumet består av de mest sentrale sivile og militære etatene og direktoratene innenfor samarbeidet i totalforsvaret og skal bidra til gjensidig orientering, samordning og overordnet koordinering av alle aktuelle totalforsvarsrelaterte problemstillinger og spørsmål knyttet til sivilt–militært samarbeid, beredskap og samfunnssikkerhet. Rådet ledes av Forsvaret og DSB på rundgang.[9]

---

8 St.meld. nr. 22 (2007–2008) *Samfunnssikkerhet – samvirke og samordning.*

9 Prop. 73 S (2011–2012) *Et forsvar for vår tid.*

Cyberkoordineringsgruppen (CKG) er en koordineringsgruppe for EOS-tjenestene. NSM leder CKG, og formålet er å sikre at EOS-tjenestene er koordinert i håndteringen av alvorlige IKT-hendelser. Det er utarbeidet en egen instruks for CKG-samarbeidet, der det blant annet går frem at CKG skal skaffe tidsriktig informasjon og beslutningsgrunnlag til den operative og strategiske ledelsen om trusler og sårbarheter i cyberdomenet. For dette formålet har man informasjonsutveksling med sektororganer, herunder Forsvaret og politiet. Videre står det at CKG ved alvorlige cyberhendelser skal koordinere varsling, rådgivning og informasjonsutveksling innen sine fullmakter. I den enkelte sak skal én av tjenestene være koordineringsansvarlig, og denne skal lede arbeidet og ta initiativ til å koordinere og avstemme tiltak mellom EOS-tjenestene, herunder det som gjelder informasjonsdeling og samhandling med andre aktører i den enkelte saken.

Skate (Styring og koordinering av tjenester i e-forvaltning) er et strategisk samarbeidsråd sammensatt av toppledere på virksomhetsnivå. Skate er et rådgivende organ som skal bidra til at digitaliseringen av offentlig sektor blir samordnet og gir gevinster for innbyggerne, næringslivet og forvaltningen. Skate består blant annet av felleskomponentforvaltere, kommunesektoren, ved KS/KommIT, og et utvalg av statlige tjenesteeiere. Rådet ledes av Difi.

NorCERT Sikkerhetsforum er et forum for NSM NorCERT-medlemmer og -partnere, der NSM NorCERT presenterer hva man har arbeidet med (koordinert håndtering av, bistått med, analysert med videre) siste halvår. I tillegg er Nasjonalt Cybersikkerhetssenter (NCSS), Operativt forum og NCSS myndighetsforum etablert. En nærmere omtale av disse finnes i kapittel 21 «Avdekke og håndtere digitale angrep».

Kommunal Informasjonssikkerhet (KINS) er en idealistisk forening basert på medlemskap og dugnadsarbeid for kommuner og fylkeskommuner. KINS' rolle er å stimulere til bedre informasjonssikkerhet. KINS har ikke formelt ansvar for IKT-sikkerheten i kommunene, men gir informasjon om hva som kreves av kommuner på informasjonssikkerhetsområdet. KINS er gjennom sin medlemsorganisering i direkte kontakt med medlemskommunene og er opptatt av hvordan medarbeiderne i kommuneorganisasjonen håndterer sikkerhet.

I tillegg til disse er det etablert en rekke koordineringsgrupper i de enkelte sektorene. Disse arenaene er beskrevet i del III «Sårbarheter i kritiske samfunnsfunksjoner» og del IV «Tverrsektorielle forhold».

Kapittel 9
IKT-sikkerhetsarbeid i andre land

Utfordringene ved samfunnets stadig større grad av digitalisering er grenseoverskridende og mange. Nasjonale myndigheter i de fleste land det er naturlig å sammenligne Norge med, anerkjenner at den digitale utviklingen fører med seg nærmest grenseløse positive muligheter, så vel som en rekke sikkerhetsutfordringer som må håndteres.

Det har i tråd med utvalgets mandat vært naturlig å se på hvordan andre land arbeider på nasjonalt nivå for å møte disse utfordringene. Det er derfor foretatt en gjennomgang av offentlige dokumenter og nasjonale strategier i følgende land: USA, Canada, Tyskland, Nederland, Storbritannia, Sverige, Finland og Estland. I tillegg er landenes myndigheter spurt om å komme med innspill.

Det er identifisert en rekke forhold ved andre lands arbeid med informasjonssikkerhet som potensielt kan ha overføringsverdi for norske forhold. Noen momenter er identifisert i alle eller de fleste av landene. For eksempel legger alle stor vekt på en helhetlig tilnærming, selv om de organisatoriske løsningene for å ivareta denne er noe ulike. Samtlige land har også ett eller flere nasjonale responsmiljøer for håndtering av IKT-hendelser. Videre har flere av landene prioritert å inkludere offentlige og private virksomheter, sikkerhetsindustrien, akademia, organisasjoner og øvrige institusjoner både i utviklingen av cybersikkerhetsstrategier og i gjennomføringen av tiltak. FoU-innsatsen er i alle landene fremhevet som et samarbeidsprosjekt mellom myndigheter, akademiske miljøer og privat sektor. Hvor det er overføringsverdi til Norge, er omtalt i relevante kapitler i NOU-en. Utvalgets omtale av IKT-sikkerhetsarbeid er i all hovedsak basert på rapporten «Andre lands arbeid med digitale sårbarheter» (BDO), se elektronisk vedlegg.

9.1 Generelle betraktninger

Digitale sårbarheter, som en del av den digitale utviklingen, har vært gjenstand for diskusjon i mange år. Det er likevel først de siste tiårene nasjonale myndigheter har løftet dette høyt på den politiske agendaen. Siden 2010 har samtlige av de landene som er omtalt i dette kapittelet, utviklet egne nasjonale strategier for informasjonssikkerhet, IKT-sikkerhet eller cybersikkerhet. De fleste av landene har en nasjonal sikkerhetsstrategi som cybersikkerhetsstrategien blir forankret i.

De siste fem årene har myndighetene i flere av disse landene vært svært tydelige i det offentlige rom på at dette er et høyt prioritert område. Amerikanske myndigheter har uttalt at cybertrusselen er den største nasjonale sikkerhetsutfordringen. I Storbritannia er cybertrusselen kategorisert som en «tier 1 threat». I 2011 gikk *UK Cabinet Office* ut i sin rapport *The cost of cybercrime*[1] og slo fast at nasjonen tapte 27 milliarder pund årlig som følge av manglende cybersikkerhet.

De digitale utfordringene er grenseoverskridende. I 2013 lanserte Den europeiske union (EU) en egen strategi – *EU Cyber Security Strategy*. Strategien angir prioriteringer for EUs internasjonale politikk for det digitale rom, grunnleggende rettigheter som også skal gjelde i det digitale samfunnet, og et fritt og åpent Internett. Videre har EU-kommisjonen lagt frem et forslag til europaparlaments- og rådsdirektiv om tiltak for å sikre et felles høyt nivå for nettverks- og informasjonssikkerhet i hele unionen, *Network and information security directive*.

Med det formål å identifisere relevante forhold som kan ha overføringsverdi til norske forhold, er det sett til andre lands gjennomførte og pågående arbeid for å håndtere digitale utfordringer. Områder som myndighetenes organisering og ansvar, nasjonale strategier, hendelseshåndtering, FoU og regulering er omhandlet. I tillegg er det gitt en generell og overordnet beskrivelse av landenes

[1] Detica, Cabinet Office (2011): *The cost of cyber crime.*

arbeid med personvern. Det presiseres at personvern er et sentralt hensyn i informasjonssikkerhetssammenheng.

9.2 Nasjonale myndigheters organisering og ansvar

Samtlige land ser på cybertrusselen som en alvorlig sikkerhetsutfordring, og den økende risikoerkjennelsen har ført til at arbeid med cybersikkerhet er plassert høyt på den politiske agendaen i alle de utvalgte landene.

Alle landene legger vekt på å organisere cybersikkerhetsarbeidet på en måte som sikrer at det forebyggende sikkerhetsarbeidet blir sett i sammenheng med kriminalitetsbekjempelse, beredskap og hendelseshåndtering. Samtidig er det en gjennomgående økende bevissthet om at det er nødvendig å inkludere alle relevante aktører i cybersikkerhetsarbeidet. Dette gjenspeiles blant annet ved at myndighetene i USA har etablert en såkalt «whole of government»-tilnærming til cybersikkerhet (samme tilnærming som i kontraterrorarbeidet). I praksis betyr dette at alle offentlige organer samvirker på tvers av ansvarslinjer for å nå et felles mål om å redusere sikkerhetsrisikoen. En slik tilnærming stiller strenge krav til etablering av funksjonelle samarbeidsstrukturer der alle relevante aktører deltar. Flere land erkjenner at myndighetsorganenes mandater og kompetanse ofte er overlappende, og at manglende samarbeid og samvirke kan føre til at det oppstår «blindsoner».

Behovet for en helhetlig tilnærming har i mange tilfeller ført til omfattende organisatoriske endringer. I Nederland medførte dette at Justis- og sikkerhetsdepartementet ble utnevnt som overordnet ansvarlig for informasjonssikkerhet. Med denne organisatoriske strukturen samordnes sikkerhets- og etterretningstjenesten innenlands og kontra-terrorarbeidet med cybersikkerhetsarbeidet. Som en del av NCTV ble *National Cyber Security Centre (NCSC)* etablert i 2012. Senteret fungerer som bindeledd mellom de ulike ansvarlige organene innen cybersikkerhet, og skal dermed sikre koordinering av de ulike aktivitetene.

Alle de åtte landene uttrykker at de har en helhetlig tilnærming til cybersikkerhetsarbeidet sitt, men konkretiseringen av helhetstilnærmingen varierer noe. De fleste av landene satser på samarbeid mellom offentlige og private virksomheter («public–private cooperation»). Denne samarbeidsformen springer ut av et behov for informasjonsdeling både for å forebygge uønskede hendelser og for å begrense skadene når slike hendelser likevel har inntruffet. Særlig Nederland, USA og Storbritannia har fokusert på å forbedre cybersikkerheten gjennom å etablere strukturer for informasjonsdeling og gjennom samarbeid mellom offentlig og privat sektor. *The National Cybersecurity and Communications Integration Center (NCCIC)* i USA har som oppdrag å sikre at relevant informasjon knyttet til risikobildet, hendelser og analyser blir beskyttet og delt. NCCIC deler informasjon mellom offentlige og private virksomheter, og er også et 24/7-senter som utgjør et samlepunkt for føderale myndigheter, etterretningstjenestene og politimyndighetene.

I de tre landene som er nevnt ovenfor, er det også skapt markedsincentiver for innovasjon og utvikling av sikkerhetsløsninger, samt lagt grunnlag for implementering av overordnede standarder for cybersikkerhet. Disse landene inkluderer offentlige og private virksomheter, sikkerhetsindustrien, akademia, organisasjoner og øvrige institusjoner i utviklingen av sine cybersikkerhetsstrategier og gjennomføringen av tiltak.

De offentlige budsjettene til organer med ansvar for cybersikkerhet har økt betydelig de senere årene. Dette reflekterer en økende bekymring for IKT-risikobildet og en større vilje til å demme opp for denne utviklingen. Landene satser på oppbygging av både offensive og defensive kapasiteter knyttet til cybersikkerhet. Det er i dag ingen land som har overordnede nasjonale indikatorer for måling av IKT-sikkerhet. Det er derfor vanskelig, om ikke umulig, å fastslå om gitte nasjonale strategier, budsjettsatsinger og øvrige virkemidler faktisk gir en tilfredsstillende sikkerhets- og beredskapsmessig effekt eller ikke.

Det er et gjennomgående trekk at justis-/innenriksdepartementene og forsvarsdepartementene har sentrale roller i alle de åtte aktuelle landene. Videre er det tydelig at alle legger stadig større vekt på de sikkerhetspolitiske aspektene ved cybersikkerhetsarbeidet. Som et resultat utvikler flere land et eget «cyberdiplomati» som en del av utenrikstjenesten. Her er USA et foregangsland.

Canada, Storbritannia og Tyskland har organer med mandater der formålet er å sikre kritisk infrastruktur og kritiske samfunnsfunksjoner, uavhengig av om dette er sivilt eller militært.

9.3 Nasjonale strategier

OECDs *Guidelines for the security of information systems and networks: Towards a culture of security*[2] var på mange måter startskuddet for utarbeidelsen av nasjonale strategier for informasjonssikkerhet[3]. De fleste sammenlignbare land har som følge av den digitale utviklingen og utviklingen i risikobildet i flere omganger revidert sine nasjonale strategier på dette området. I de senere årene er blant annet ENISAs *Good practice guide on national cyber security strategies* brukt som utgangspunkt i flere lands strategier.[4]

Informasjonssikkerhet prioriteres høyt på den politiske agendaen og fremheves som en nødvendig forutsetning for å opprettholde samfunnets funksjonsdyktighet, nasjonale sikkerhet og økonomiske vekst. Det er en økende erkjennelse av at manglende risikohåndtering knyttet til digitale sårbarheter kan true vitale nasjonale interesser og føre med seg enorme økonomiske tap. Dette har ført til økt oppmerksomhet rundt organiseringen av informasjonssikkerhetsarbeidet, samt etablering av hensiktsmessige systemer for risikohåndtering på nasjonalt nivå. Begge aspektene har bidratt til å øke graden av nødvendig samordning og koordinering, samtidig som de har utfordret de tradisjonelle ansvarslinjene og organisasjonsstrukturene i både offentlig og privat sektor. Eksempelvis har USA gjennomført en omfattende evaluering av sitt strategiske arbeid, for at det skal bli mest mulig målrettet.

Det er et gjennomgående trekk ved landene at de har en helhetlig tilnærming til informasjonssikkerhet i sine nasjonale strategier. Strategiene omfatter tiltak rettet mot både enkeltindivider, offentlige og private virksomheters egenbeskyttelse og det samlede statlige virkemiddelapparatet. Samtidig blir behovet for operative og strategiske samarbeidsmekanismer på tvers av myndighetsorganer og mellom alle relevante aktører i offentlig og privat sektor fremholdt som helt nødvendig for å redusere digitale sårbarheter og IKT-kriminalitet på en effektiv og målrettet måte. Dette gjelder både nasjonalt og internasjonalt.

Storbritannia fremhever behovet for regionale samarbeids- og informasjonsdelingsmekanismer. Flere land, deriblant USA og Tyskland, fremhever særlig behovet for økt innovasjon knyttet til sikkerhetsløsninger som følge av stadig strengere krav til effektivitet og mobilitet.

Nedenfor følger en oversikt over hvilke temaer som er felles for de åtte landenes nasjonale strategier:

- styring og ledelse
- samarbeids- og informasjonsdelingsmekanismer
- hendelseshåndtering
- IKT-kriminalitet
- sikkerhetskultur og bevisstgjøring
- kunnskapsutvikling og innovasjon
- sikkerhetsutdanning
- rammeverk og standarder
- menneskerettigheter og personvern

9.4 Hendelseshåndtering

Alle de åtte landene har ett eller flere nasjonale responsmiljøer for håndtering av IKT-hendelser. Samtlige har også nasjonale CERT-er (Computer Emergency Response Team), men organiseringen er noe ulik, både når det gjelder ansvarsområder og plasseringen i forhold til myndighetsstrukturene. Landene poengterer i sine nasjonale strategier at CERT-arbeidet er en avgjørende del av den strategiske tilnærmingen til håndtering av IKT-hendelser på nasjonalt nivå. I tillegg fremhever flere at hendelseshåndtering og IKT-sikkerhet er et virksomhetsansvar. Flere land har publisert planer som beskriver hvordan IKT-hendelser håndteres nasjonalt. Når det gjelder å håndtere IKT-kriminalitet, er det flere ulike måter å organisere polisiære ressurser på. Én fremgangsmåte er være å etablere et IKT-kriminalitetssenter i en eller annen form.

Nederland har valgt å samle hovedtyngden av sin IKT-sikkerhetsekspertise og hendelseshåndtering på nasjonalt nivå i et nasjonalt cybersikkerhetssenter (NCSC). Dette inkluderer både et nasjonalt rapporteringspunkt, CERT-funksjonen fra den tidligere GOVCERT-NL, koordineringsansvar ved IKT-hendelser, monitoring og informasjonsdeling. NCSC opererer i tillegg et offentlig varslingssystem rettet mot mindre virksomheter og befolkningen for øvrig.

I 2011 etablerte også Tyskland sitt *Nationales Cyber-Abwehrzentrum* (nasjonalt cyber-responssenter). I senteret samarbeider *Bundesamt für Sicherheit in der Informationstechnik* (BSI) blant

---

2 OECD (2002): *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.*

3 Benevnelsen informasjonssikkerhet brukes her synonymt med cybersikkerhet. På engelsk benevnes de nasjonale strategiene for informasjonssikkerhet National cyber security strategy.

4 ENISA (2012): *National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyberspace.*

annet med føderale politimyndigheter, etterretningstjenesten og forsvaret. Formålet med senteret er å optimalisere samarbeidet mellom de statlige myndighetene. Ved BSI finnes også funksjonene CERT-Bund og Nationales IT-Lagezentrum.

USA har en noe annerledes tilnærming. Her er de nasjonale kapasitetene på IKT-sikkerhet spredt på flere aktører, herunder US-CERT, en egen ICS-CERT (CERT for SCADA-systemer), en nasjonal task force for etterforskning i det digitale rom (NCIJTF) i regi av FBI, *US Cyber Command* under Forsvarsdepartementet, *Intelligence Community-Incident Response Center (IC-IRC)*, *National Security Agency / Central Security Services Threat Operations Center (NTOC)*, *DoD Defense Cyber Crime Center (DC3)* og det nylig etablerte *Cyber Threat Intelligence Integration Center (CTIIC)*. Samtidig er ambisjonen at IKT-hendelseshåndtering skal være en samlet innsats fra disse aktørene, koordinert gjennom *National Cyber Security and Communications Integration Center (NCCIC)*. NCCIC skal blant annet ha et oppdatert situasjonsbilde, drive IKT-hendelseshåndtering og styring og være et nasjonalt knutepunkt for føderale myndigheter, etterretningssamfunnet og politimyndighetene. US-CERT og ICS-CERT er en integrert del av NCCIC. Department of Homeland Security (DHS) har ansvaret for *National Cyber Incident Response Plan (NCIRP)*.

De ulike organene i den amerikanske satsingen på IKT-sikkerhet utfyller det flersidige bildet i et stort land med en kompleks organisering. Mens DHS, gjennom *National Cyber Security and Communications Integration Center (NCCIC)*, proaktivt skal håndtere digital risiko og sørge for informasjonsdeling om digitale sårbarheter, har *The National Cyber Investigative Joint Task Force (NCIJTF)*, som består av 19 etterretningsbyråer og rettshåndhevende myndigheter, som mål å trygge Internett gjennom aktivt å jakte på trusselaktører.

For IKT-hendelseshåndtering i Storbritannia har man på nasjonalt nivå delt ansvaret mellom GovCERT.uk og CERT-UK. Sistnevnte ble grunnlagt i 2014, og var en viktig satsing som oppfølging av den nasjonale cybersikkerhetsstrategien. CERT-UK fokuserer på å ha et oppdatert situasjonsbilde, hendelseshåndtering på nasjonalt nivå, samt å støtte virksomheter med samfunnskritisk infrastruktur. GovCertUK har på sin side ansvaret for å koordinere hendelseshåndtering og tiltak for myndighetsorganer. Den nasjonale håndteringen av alvorlig IKT-kriminalitet koordineres av *National Cyber Crime Unit (NCCU)* ved *National Crime Agency (NCA)*.

I juni 2014 lanserte britiske myndigheter satsingen «Cyber Essentials», en sertifiseringsordning som støttes av industrien, og som skal stimulere til utbredt bruk av grunnleggende sikkerhetskontroller for å beskytte organisasjoner mot mindre avanserte IKT-hendelser. Sertifiseringen kommer med et merke som benyttes av bedrifter til å demonstrere sitt sikkerhetsnivå til kunder og investorer, og som forsikringsselskaper kan ta i betraktning når de vurderer IKT-sikkerhetsnivået i forbindelse med at de beregner forsikringspremie til bedrifter. Som et annet initiativ har *The Council for Registered Ethical Security Testers (CREST)* nylig innført en godkjenningsordning for selskaper som jobber med IKT-sikkerhet i Storbritannia. Ordningen er godkjent av Government Communications Headquarters (GCHQ) og Centre for the Protection of National Infrastructure (CPNI) og fokuserer på aktuelle standarder for hendelseshåndtering justert til å passe alle sektorer og industrier.

I Sverige er CERT-SE tillagt *Myndigheten för samhällsskydd och beredskap (MSB)*, som på oppdrag fra regjeringen har utarbeidet *Nationell hanterandeplan för allvarliga IT-incidenter*. Den 1. oktober 2015 ble det etablert et nasjonalt IKT-kriminalitetssenter av *Polismyndigheten*. Senteret har en nasjonal koordineringsfunksjon og er internasjonalt kontaktpunkt for IKT-relatert kriminalitet og IKT-kriminalitet. I Canada er *Canadian Cyber Incident Response Centre (CCIRC)* lagt til *Public Safety Canada (PSC)*. I tillegg har *Royal Canadian Mounted Police (RCMP)* opprettet *Cyber Crime Fusion Centre* med ansvar for å etterforske mistenkelige nasjonale og internasjonale hendelser i det digitale rom. PSC har også ansvaret for *Cyber Incident Management Framework for Canada*.

9.5 Informasjonsdeling og offentlig–privat samarbeid

Det er enighet om viktigheten av å dele informasjon, både i det forebyggende sikkerhetsarbeidet og ved hendelseshåndtering, i et flertall av de nasjonale myndighetene. Dette understrekes både i de nasjonale strategiene og i annet informasjonsmateriell fra disse myndighetene. Mekanismer og plattformer for å dele informasjon er tett integrert med hendelseshåndteringsmiljøene, herunder USAs *National Cyber Security and Communications Integration Center (NCCIC)*, Nederlands *National Cyber Security Center (NCSC)* og Storbritannias *CERT-UK*.

Tyskland har etablert *National Cyber Security Council* ved *Federal Government Commissioner for Information Technology*. Målet er å styrke samarbeidet mellom den føderale regjeringen og privat sektor, samt gi anbefalinger om strategiske spørsmål til politisk nivå. I Nederland har NCSC etablert *National Cyber Security Council* med representanter fra privat og offentlig sektor samt akademia. Målet er å øke forståelsen for cybersikkerhet og støtte beslutningstagere ved cyberkriser.

NCFTA[5] er et samarbeid mellom myndigheter, private og akademia, tilrettelagt ved FBI og lokalisert ved universitetet Carnegie Mellon.[6] Representanter for andre lands politistyrker deltar også. Formålet er å identifisere aktører bak digitale angrep, begrense skade og nøytralisere identifiserte aktører. Styrende for samarbeidet er virksomhetenes egne behov, rask deling, sektoruavhengighet og et ugradert arbeidsmiljø på «nøytral grunn». I motsetning til CERT-miljøene fokuserer NCFTA på de kriminelles verdikjeder. De kartlegger nettverk av kriminelle grupperinger og deler indikasjoner på datainnbrudd seg imellom. NCFTA har også en underavdeling av FBI kalt *CIRFU*[7], som følger den innledende etterforskningen ved teknisk kompleks IKT-kriminalitet før saken overføres til lokalt eller internasjonalt politi. Samarbeidet har oppnådd resultater særlig knyttet til å stoppe botnett og ta utviklere av skadevare.

I Storbritannia er det også satt i gang et fellesinitiativ mellom myndighetene og industrien angående informasjonsdeling og samarbeid for å møte de digitale truslene, kalt *Cyber-Security Information Sharing Partnership (CISP)*. Allerede ved utgivelsen av den nasjonale strategien i 2011 ble det gjort klart at myndighetenes tilnærming til cybersikkerhet er risikobasert, og at arbeidet må gjøres i partnerskap med private aktører.

President Obamas *Executive order 13691* angir et rammeverk for utvidet informasjonsdeling og promoterer informasjonsdeling både innad i privat sektor og mellom private virksomheter og myndighetene i USA.

Offentlig–privat samarbeid er også løftet som et satsingsområde i flere av de andre landene. Det legges generelt stor vekt på at deling av informasjon mellom offentlige og private aktører er et viktig premiss for at samfunnet skal kunne møte utfordringene som følger av den digitale utviklingen. Nederland reviderte sin første nasjonale strategi allerede to år etter utgivelsen. I 2013-versjonen var rundt 130 nye aktører, fra både offentlig og privat sektor, involvert i forarbeidet.

9.6 Forskning og utvikling

Alle landene har over tid fokusert på og prioritert forsknings- og utviklingsarbeid i sine nasjonale strategier. Alle legger vekt på viktigheten av FoU-området, da særlig med tanke på sårbarhetsreduksjon, men også når det gjelder effektiv utnyttelse av samfunnets samlede informasjonsteknologi. I de fleste nasjonale strategiene er FoU-begrepet nært knyttet til myndighetenes og næringslivets behov for informasjonssikkerhet. Enkelte av landene kobler også begrepet opp mot befolkningens behov for økt sikkerhetsbevissthet (og -kunnskap).

Et annet fellestrekk er at FoU-innsatsen er et samarbeidsprosjekt mellom myndigheter, akademiske miljøer og privat sektor. Imidlertid er selve finansieringen av utdanningsprogrammer og lignende i liten grad beskrevet i strategiene. Et unntak er Tyskland, der Utdannings- og forskningsdepartementet tilsynelatende har finansiert en rekke større forskningsprosjekter de siste årene.

Måten å operasjonalisere FoU-begrepet på i strategiene varierer. Generelt vektlegger samtlige av landende behovet for spesialiserte utdannings- og forskningsprogrammer, særlig på universitetsnivå. De fleste har også iverksatt særskilte strategier og initiativer som skal sikre tilgang på stabil og kvalifisert arbeidskraft. USA og Storbritannia fremhever spesielt hvordan deres sikkerhets- og etterretningstjenester har et særskilt samarbeid med utvalgte universiteter.

Den bredeste tilnærmingen til FoU-begrepet finner vi i Finland, Storbritannia, Nederland og delvis i Estland. Her vektlegger man at IKT-sikkerhet må være en del av det generelle utdanningsløpet allerede fra barneskolen av.

9.7 Regulering

Gjennomgående vurderer landene det slik at de lovene og reglene vi i dag har i den fysiske verden, også gjelder i den digitale verden. Samtidig erkjenner de at det kan være utfordrende å finne de riktige regulatoriske virkemidlene og å oppda-

---

5 National Cyber Forensics and Training Alliance i Pittsburgh/Pennsylvania.

6 Lokasjonen gjør at medlemmene kan kommunisere uhindret ved at kommunikasjonen foregår på et sikkerhetsnivå som ikke ekskluderer noen.

7 Cyber Initiative and Resource Fusion Unit (CIRFU).

tere lovverket slik at det blir anvendbart i det digitale rom.

Selv om det er variasjon i tradisjonene for rettslig regulering i de forskjellige landene, synes det å være et fellestrekk at de benytter både særlovgivning og generell lovgivning. Regulering av informasjonssikkerhet kan følge begge spor, avhengig av om det er særlige faglige hensyn som må ivaretas, eller om et generelt lovverk dekker behovene for sikkerhet. Slik særregulering er for eksempel brukt for kraftsektorens informasjonssikkerhetsarbeid. Personopplysningslover er generelle lover som gjelder alle offentlige og private virksomheters behandling av personopplysninger, med mindre de har egne lovverk. Eksempelvis er mandater og oppgaver til både BSI i Tyskland og DHS i USA gitt i egne spesiallover. Det er foreløpig uvanlig med en overordnet cybersikkerhetslov. Det pågår imidlertid regelverksarbeid knyttet til dette i flere land. Eksempelvis søker Obama-administrasjonen å få vedtatt en slik overordnet cyberlov.

Selv om det ikke er vanlig med en overordnet lov for cybersikkerhet, legges et økende antall standarder til grunn for informasjonssikkerhetsarbeid. Mange av disse standardene er overlappende i det at de regulerer implementeringen av et styringssystem for informasjonssikkerhet, med mål om et mer strukturert og systematisk arbeid for å bedre kvaliteten på informasjonssikkerheten generelt og implementeringen av risikoreduserende tiltak spesielt. Et eksempel på en slik standard er *Framework for Improving Critical Infrastructure Cybersecurity,* utgitt av *National Institute of Standards and Technology (NIST)* i USA, og det helhetlige veiledningsmaterialet i cybersikkerhet utarbeidet av britiske *GCHQ, CPNI* og *Department for Business Innovation and Skills (BIS)*. Sistnevnte inkluderer blant annet en lett tilgjengelig og svært anerkjent veileder, kjent som *10 Steps to Cyber Security*.

President Obama utstedte i 2013 ordre EO 13636, *Improving Critical Infrastructure Cybersecurity* og *Presidential Policy Directive-21 (PPD) Critical Infrastructure Security and Resilience*. I disse dokumentene ble det henstilt til føderale myndigheter om å iverksette tiltak for å styrke sikkerheten og robustheten i kritisk infrastruktur mot økende trusler, gjennom et oppdatert og overordnet nasjonalt rammeverk som anerkjenner IKTs økte rolle i å sikre fysiske verdier. Sammen angir disse to dokumentene en retning mot en «whole of community»-tilnærming til risikostyring, sikkerhet og robusthet. Ordren (EO 13636) ga også *National Institute of Standards and Technology (NIST)* i oppdrag å utvikle det ovennevnte rammeverket for cybersikkerhet, basert på en sammenstilling av standarder og beste praksis i bransjen. Denne ordren henstilte også til DHS om å etablere et frivillig program for cybersikkerhet i kritisk infrastruktur, om å fungere som en føderal koordineringsenhet for cybersikkerhetsressurser og om å støtte økt digital motstandsdyktighet ved å fremme bruk av rammeverket. Programmet skal legge til rette for en felles tilnærming til risikostyring, sikkerhet og robusthet.

Utarbeidelse av standarder for cybersikkerhet synes å være styrt av markedsincentiver. Eksempelvis er alle myndighetsorganer i Storbritannia forpliktet til å kreve at leverandører som skal behandle sensitiv informasjon, overholder gitte standarder for informasjonssikkerhet. Videre pågår det en diskusjon i USA om erstatningsansvar ved uaktsomhet knyttet til informasjonssikkerhet, som følge av hendelser som har hatt store økonomiske konsekvenser. Manglende juridisk forankring av spesifikke sikkerhetskrav kan imidlertid gjøre dette vanskelig å gjennomføre.

De fleste land har et regelverk rundt informasjonssikkerhet som regulerer klassifisering av skjermingsverdig informasjon, tilsvarende det norske graderingssystemet i sikkerhetsloven. Det er imidlertid ikke fullt ut samsvar mellom antall graderingsnivåer, noe som kan skape utfordringer med hensyn til deling av skjermingsverdig informasjon mellom nasjoner.

9.8 Personvern

Ivaretakelse av innbyggernes rett til beskyttelse av personlig integritet er anerkjent som et viktig premiss for arbeidet med IKT-sikkerhet. EU- og EØS-land er underlagt felles regelverk, som personverndirektivet. Direktivet pålegger statene å innarbeide direktivet i sine lands lovverk og å etablere uavhengige personvernmyndigheter, «Data-protection Authority (DPA)», for å unngå direkte politisk styring og for å sikre en mest mulig ensartet praksis i landene.

Canada har et tilsvarende lovverk som EU. Det er derimot ingen enkelt lov i USA som gir en omfattende beskyttelse av personopplysninger. Personvern løftes likevel frem som et viktig premiss, blant annet av DHS, og nevnes i både strategier og annet lovverk som omhandler IKT-sikkerhet.

Kapittel 10
Folkerett og internasjonalt samarbeid

Den digitale utviklingen har endret samfunnet og den menneskelige samhandlingen vår på måter som var utenkelige for få år siden. Det digitale rom, også omtalt som cyberdomenet eller cyberspace, har i all hovedsak bidratt til positive endringer. Det har bidratt til økonomisk utvikling, det har etablert nye former for demokratiske kanaler, og det har bidratt til å fremme menneskerettigheter. Samtidig åpner cyberdomenet for nye og alvorlige trusler fra både statlige og ikke-statlige aktører. Området krever politikkutvikling og operative tiltak både nasjonalt og internasjonalt.

Vesentlig for forståelsen av det digitale rom er at reguleringene i vesentlig grad er blitt til gjennom avanserte kontraktsrettslige konstruksjoner innenfor rammene av amerikansk rett og jurisdiksjon. Dette er ikke til hinder for at andre stater prinsipielt kan utøve myndighet eller jurisdiksjon, men det at sentrale næringsaktører på dette området har kontraktsfestede standardvilkår med transnasjonale virkninger, medfører i realiteten sterke begrensninger på effektiv reguleringsmyndighet av andre stater. Dette spørsmålet er imidlertid blitt reist blant annet i EU og i Europarådet i forskjellige former. Blant annet er rammevilkårene i det europeiske indre marked og menneskerettigheter av vesentlig betydning for en fremtidig regelutvikling.

Det digitale rom kjennetegnes derfor av uoversiktlige strukturer, kompleksitet og stor grad av privat eierskap. Den teknologiske utviklingen går på mange områder langt raskere enn myndighetenes evne til å forstå og iverksette tiltak for å forebygge sårbarhet, for eksempel i samfunnskritisk infrastruktur. Samtidig har forvaltningen av Internett («Internet governance») – cyberdomenets desidert viktigste arena – skapt dyptgripende internasjonal debatt og de siste to årene utviklet seg til et av vår tids store spørsmål, med betydelige maktpolitiske dimensjoner. Dette stiller stater overfor helt særegne spørsmål av rettslig og sikkerhetspolitisk karakter og krever et nært samarbeid både mellom stater og mellom privat og offentlig sektor, både nasjonalt og internasjonalt. Spørsmål knyttet til det digitale rom har derfor på kort tid blitt sentrale utenrikspolitiske spørsmål.

Mange utenrikstjenester som Norge kan sammenligne seg med, har de siste par årene styrket sine kapasiteter til å håndtere utenrikspolitiske spørsmål knyttet til cyberdomenet. I norsk UD ble det i 2013 etablert en egen stilling som cyberkoordinator som koordinerer utvikling og samordning av norske posisjoner i internasjonal cyberpolitikk, både internt i Utenriksdepartementet og sammen med andre berørte departementer.

Utvalget har mottatt en grundig skriftlig redegjørelse om Norges folkerettslige forpliktelser fra UDs rettsavdeling vedrørende spørsmålene som er behandlet under punktene 10.1 til 10.5. jf. elektronisk vedlegg «Folkerettslige rammer for grenseoverskridende informasjonsinnhenting». For øvrig har vi hatt et møte med UDs cyberkoordinator som orienterte om FNs arbeid og andre sentrale internasjonale organisasjoners arbeid med forvaltning av Internett og Domenenavn. Omtalen av EU og EØS er hovedsakelig basert på NOU 2012: 2 *Utenfor og innenfor.* Øvrig omtale er hentet fra organisasjonenes hjemmesider og SOU 2015: 23 *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten.* Oversikten er ikke uttømmende.

10.1 Folkerettslige rammer for grenseoverskridende informasjonsinnhenting

Først behandles alminnelige folkerettslige skranker for grenseoverskridende informasjonsinnhenting, herunder først og fremst suverenitetsprinsippet (punkt 10.2). Deretter vil vi kort omtale begrensninger som følger av Wien-konvensjonen om diplomatisk samkvem (punkt 10.2.1). Overvåking og informasjonsinnhenting må videre skje innenfor rammene av de internasjonale menneskerettighetene (punkt 10.3). Vi vil også omtale Europarådets konvensjon nr. 108 om personvern

(punkt 10.4) og Europarådets konvensjon nr. 185 om datakriminalitet (punkt 10.5).

Den stadig økende digitaliseringen av samfunnet har medført nye folkerettslige problemstillinger. Det er enighet om at den alminnelige folkeretten i utgangspunktet kommer til anvendelse på overvåking og informasjonsinnhenting i det digitale rom. Samtidig kan det være usikkerhet og diskusjon knyttet til hvilket resultat anvendelse av gjeldende folkerett vil få i konkrete saker. Dette er derfor et område hvor folkeretten fortsatt ikke nødvendigvis alltid gir klare svar og hvor den kan være under utvikling. Dessuten medfører den teknologiske utviklingen at det kan være uklart om en stat utfra de konkrete omstendighetene kan holdes ansvarlig for en bestemt handling eller unnlatelse, dvs. om staten har jurisdiksjon.

De ulike folkerettslige spørsmålene som gjennomgås nedenfor er bare i begrenset grad regulert i traktater. Når det gjelder avgjørelser fra internasjonale domstoler, finnes det noen, men de er hovedsakelig knyttet til menneskerettslige problemstillinger (punkt 10.3). Enkelte folkerettslige vurderinger kan gjøres ut fra statspraksis og alminnelige folkerettslige prinsipper. Det foreligger også uttalelser fra for eksempel FNs høykommissær for menneskerettigheter og resolusjoner fra FNs generalforsamling. Selv om den folkerettslige rettskildeverdien av disse er begrenset, får de omtale nedenfor (punkt 10.3.3), bl.a. i lys av utvalgets anmodning til Utenriksdepartementet om å gjennomgå de internasjonale fora der problemstillingene blir drøftet.

Omtalen av menneskerettighetsforpliktelser gis relativt sett en bred plass i det følgende. Disse anses særlig relevant for utvalgets arbeid, og på dette området i folkeretten finnes det flere internasjonale rettsavgjørelser, særlig fra Den europeiske menneskerettighetsdomstolen.

10.2 Alminnelige folkerettslige skranker for grenseoverskridende informasjonsinnhenting

Med unntak for visse avgrensede områder er det få eksempler på traktatfestede forbud mot utenlandsetterretning eller spionasje i fredstid. Man må derfor falle tilbake på alminnelige folkerettslige prinsipper, herunder først og fremst suverenitetsprinsippet, dvs. prinsippet om en stats suverene myndighet på sitt territorium. Av suverenitetsprinsippet utledes bl.a. forbudet mot innblanding i en annens stats indre anliggende på dets territorium. Den internasjonale domstolen i Haag uttalte i dom av 7. september 1927 i Lotus-saken (Frankrike mot Tyrkia):

> «*[T]he first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State*».

Det er sjelden at stater har påberopt at etterretningsvirksomhet utgjør folkerettsbrudd. Det foreligger heller ingen avgjørelser fra internasjonale domstoler eller tribunaler som konkluderer med at spionasje i seg selv utgjør en suverenitetskrenkelse. Statenes manglede vilje til å påberope seg folkerettsbrudd skyldes nok dels at stater har ansett det nødvendig å ivareta sin egen mulighet til å drive etterretningsvirksomhet i utlandet. Til dette bildet hører også at statene har kunnet straffeforfølge spioner under nasjonal jurisdiksjon, eller – dersom disse har hatt diplomatisk immunitet – erklære disse *persona non grata*, jf. Wienkonvensjonen om diplomatisk samkvem av 1961 art. 9 (punkt 10.2.1).

Det legges på denne bakgrunn til grunn at det ikke er internasjonal konsensus om at grenseoverskridende etterretningsvirksomhet, herunder i det digitale rom, som utelukkende består i informasjonsinnhenting, og som ikke forårsaker noen form for fysisk skade eller tap av funksjonalitet, i seg selv utgjør en suverenitetskrenkelse. Det kan imidlertid diskuteres, ikke minst i lys av den tekniske utviklingen, om det kan tenkes situasjoner der de negative konsekvenser for eksempel på en stats økonomi (industrispionasje) er av en slik art at handlingen vil kunne utgjøre et brudd på suverenitetsprinsippet. Hensikten med informasjonsinnhentingen, og hvordan denne er foretatt, vil også kunne ha betydning.

Det nevnes i denne forbindelse at *NATO Cooperative Cyber Defence Centre of Excellence*, med kontor i Tallinn, har invitert en uavhengig ekspertgruppe til å utarbeide en manual om anvendelsen av folkeretten i det digitale rom i fredstid (som en oppfølgning av den såkalte Tallinn-manualen 1.0 som gjelder anvendelse av folkeretten på digital krigføring). Tallinn-manual 2.0 forventes å ville kaste nærmere lys over suverenitetsprinsippets anvendelse i en digital kontekst.

10.2.1 Wien-konvensjonen om diplomatisk samkvem

Wien-konvensjonen om diplomatisk samkvem av 1961 fastsetter rapportering om forholdene i vertslandet som en av funksjonene for en diplomatisk stasjon, jf. artikkel 3 nr. 1 (bokstav d). Informasjonsinnhenting er da en forutsetning. Imidlertid fremgår det av samme bestemmelse at denne aktiviteten skal foregå ved lovlige midler («by all lawful means»). Videre fremgår det av artikkel 41 nr. 1 og nr. 3 at vertslandets lover skal følges, og at ambassadens lokaler ikke skal benyttes på en måte som er i strid med stasjonens funksjoner slik de er fastsatt i konvensjonen. Dette legger begrensninger på denne type aktivitet.

Vertslandet kan erklære en diplomat som uønsket, *persona non grata*, dersom den anser at disse bestemmelsene ikke respekteres, jf. artikkel 9 nr. 1.

Wien-konvensjonen har også bestemmelser som beskytter den diplomatiske stasjons lokaler, områder, arkiver og korrespondanse, og setter derved grenser for vertslandets aktivitet overfor stasjonen.

10.3 Menneskerettslige skranker for informasjonsinnhenting

Overvåking og informasjonsinnhenting kan først og fremst komme i strid med retten til respekt for privatliv og korrespondanse, som vil bli behandlet nærmere under punkt 10.3.2. nedenfor. Andre menneskerettigheter kan imidlertid også være relevante. Overvåking av en journalist vil for eksempel kunne innebære både et inngrep i journalistens privatliv og i vedkommendes ytringsfrihet.[1] Forsamlingsfriheten kan også etter omstendighetene være berørt.

Når det gjelder grenseoverskridende informasjonsinnhenting, reiser det seg et tilleggsspørsmål om internasjonale menneskerettigheter kan påberopes mot den staten som har innhentet opplysningene, også av personer som befinner seg utenfor statens territorium. Tilsvarende spørsmål reiser seg når en stat innhenter opplysningene på eget territorium, men virkningen i form av inngrep i privatliv eller kommunikasjon skjer utenfor statens territorium. Dette er spørsmål om menneskerettighetenes ekstraterritorielle anvendelse og vil bli nærmere belyst under punkt 10.3.2.

Det foreligger omfattende rettspraksis fra EMD vedrørende retten til et privatliv. Vi antar at hemmelig overvåking og informasjonsinnhenting av hensyn til nasjonal sikkerhet og kriminalitetsbekjempelse er særlig relevant i tilknytning til utvalgets mandat. Vi fokuserer derfor særlig på dette i det følgende. Av særlig interesse mht. de menneskerettslige rammene for hemmelig overvåking og informasjonsinnhenting er EMDs avvisningsavgjørelse *Weber og Saravia mot Tyskland* av 29. juni 2006, hvor EMD vurderte tysk etterretningstjenestes myndighet til å drive såkalte strategisk overvåking av nasjonale sikkerhetshensyn, så vel som bruk og videreformidling av informasjonen oppnådd på denne måten. Det vises også til dommen *Liberty m.fl. mot UK* av 1. juli 2008, hvor dagjeldende britisk lovgivning for overvåking av kommunikasjon ble funnet å være i strid med EMK, jf. også den senere frifinnelsesdommen *Kennedy mot UK* av 18. mai 2010. Av fremtidige avgjørelser nevnes *Big Brother Watch m.fl. mot UK* (klage nr. 58170/13 av 4. september 2013), som vil kunne kaste nærmere lys over rettstilstanden på dette området.

10.3.1 Den europeiske menneskerettskonvensjonen art. 8 og FNs konvensjon om sivile og politiske rettigheter art. 17

Den europeiske menneskerettskonvensjonen (EMK) art. 8 og FNs konvensjon om sivile og politiske rettigheter (SP) art. 17 om rett til respekt for ens privatliv og korrespondanse er noe ulikt formulert:

EMK art. 8 lyder:

1. *Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.*
2. *Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.*

Mens SP art. 17 fastsetter at:

1. *Ingen må utsettes for vilkårlige eller ulovlige inngrep i privat- eller familieliv, hjem eller korrespondanse, eller ulovlige inngrep på ære eller omdømme.*

[1] Se for eksempel EMDs avgjørelse *Weber og Saravia mot Tyskland* (klage nr. 54934/00) av 29.6.2006.

2. *Enhver har rett til lovens beskyttelse mot slike inngrep eller angrep.*

Praksis fra de to konvensjonenes overvåkingsorganer, henholdsvis Den europeiske menneskerettsdomstolen (EMD) og FNs menneskerettskomité, viser imidlertid at de nærmere vurderingstemaene etter de to bestemmelsene vil være sammenfallende. Vi vil derfor i det følgende forholde oss til EMK art. 8 og EMDs rettspraksis med mindre det skulle være særlig grunn til også å nevne FN-konvensjonen.

Hva utgjør et inngrep i ens privatliv eller korrespondanse?

Det følger av EMDs rettspraksis at alle typer korrespondanse vil være beskyttet av EMK art. 8, herunder e-post og andre typer elektronisk kommunikasjon, video-klipp og lydopptak og GPS-overvåking. EMD har også lagt til grunn at ikke bare innsamling av innhold i kommunikasjon, men også av trafikkdata eller metadata (data om kommunikasjon) er et inngrep i privatlivet (se *Malone mot UK* av 2. august 1984, avsnitt 84). Videre utgjør ikke bare selve innsamlingen av kommunikasjon, men også senere lagring og bruk av personlige opplysninger et inngrep i privatlivet (se for eksempel *Leander mot Sverige* av 26. mars 1987, avsnitt 48). Deling av informasjonen som utvider gruppen med kjennskap til personlige opplysninger, utgjør et ytterligere selvstendig inngrep i privatlivet (*Weber og Saravia mot Tyskland*, avsnitt 79). Til og med selve eksistensen av lovgivning som tillater hemmelige overvåking av kommunikasjon, kan utgjøre et inngrep i privatlivet, selv om klager selv ikke har vært overvåket (se *Weber og Saravia,* avsnitt 78 med videre henvisninger).

Ikke bare individer, men også selskaper er vernet av EMK artikkel 8, jf. EMDs dom *Societé Colas Est m.fl. mot Frankrike* av 16. april 2002. Når det gjelder hvilken type opplysninger som er beskyttet av EMK art. 8, har EMD sett hen til Europarådets personvernskonvensjons vide definisjon av personopplysninger, som er «enhver opplysning som gjelder en bestemt eller identifiserbar enkeltperson» (se for eksempel *Rotaru mot Romania* av 4. mai 2000 avsnitt 42–43).

Retten til privatliv er ikke absolutt

Inngrep i privatlivet kan imidlertid skje dersom det har sitt grunnlag i lov og kan anses nødvendig i et demokratisk samfunn av hensyn til et legitimt formål, jf. EMK art. 8 nr. 2. Legitime formål er iht. bestemmelsen nasjonal sikkerhet, offentlig trygghet, landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter eller friheter.

EMD fremhevet i sin første avgjørelse om hemmelig overvåking, *Klass m.fl. mot Tyskland* av 6. september 1978, at moderne demokratiske samfunn er truet av svært sofistikerte former for spionasje og terrorisme og derfor under særlige omstendigheter må kunne være i stand til å gjennomføre hemmelig overvåking av kommunikasjon for effektivt å bekjempe slike trusler (dommens avsnitt 48).

Inngrep må være i samsvar med loven

For at inngrep i privatlivet eller korrespondanse skal være tillatt, må det skje i samsvar med loven. Det følger av EMDs rettspraksis at dette innebærer at inngrepet må ha hjemmel i nasjonal lov som må oppfylle visse kvalitative krav. Lovgivningen må være tilstrekkelig tilgjengelig, sikre forutberegnelighet mht. under hvilke omstendigheter overvåking kan skje, og være i tråd med rettsstatsprinsipper (jf. *Weber og Saravia* avsnitt 84).

EMD har lagt til grunn at selv om kravet om forutberegnelighet i konteksten hemmelig overvåking selvfølgelig ikke kan bety at den overvåkede skal forhåndsinformere om overvåkingen, må lovgivningen ha klare og detaljerte regler om innsamling av kommunikasjon for å forebygge vilkårlighet. Det må herunder ikke åpnes opp for stor grad av diskresjonær myndighet for den utøvende makt eller domstolene, men trekkes opp klare rammer for skjønnsutøvelsen (se bl.a. *Malone* avsnitt 67–68 og *Weber og Saravia* avsnitt 93–94). I tillegg må et minimum av rettssikkerhetsgarantier være oppfylt for hemmelig overvåking, jf. nærmere *Weber og Saravia* avsnitt 95:

> «In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstan-

ces in which recordings may or must be erased or the tapes destroyed…»

EMD har videre lagt til grunn at inngrep ikke bare må være i samsvar med nasjonal lovgivning, men også internasjonale offentligrettslige regler som staten er bundet av, herunder folkerettens regler om staters suverenitet, jf. følgende uttalelse i *Weber og Saravia* avsnitt 87:

> «The Court reiterates that the term «law» within the meaning of the Convention refers back to national law, including rules of public international law applicable in the State concerned (…). As regards allegations that a respondent State has violated international law by breaching the territorial sovereignty of a foreign State, the Court requires proof in the form of concordant inferences that the authorities of the respondent State have acted extraterritorially in a manner that is inconsistent with the sovereignty of the foreign State and therefore contrary to international law.»

EMD kom i saken *Weber og Saravia* til at det ikke var bevist at den tyske lovgivningen vedrørende strategisk overvåking, var blitt anvendt på en på en måte som kom i strid med en fremmed stats suverenitet, jf. avsnitt 88:

> «The Court observes that the impugned provisions of the amended G 10 Act authorise the monitoring of international wireless telecommunications, that is, telecommunications which are not effected via fixed telephone lines but, for example, via satellite or radio relay links, and the use of data thus obtained. Signals emitted from foreign countries are monitored by interception sites situated on German soil and the data collected are used in Germany. In the light of this, the Court finds that the applicants failed to provide proof in the form of concordant inferences that the German authorities, by enacting and applying strategic monitoring measures, have acted in a manner which interfered with the territorial sovereignty of foreign States as protected in public international law.»

Inngrepet må være nødvendig i et demokratisk samfunn av hensyn til et legitimt formål

Dersom man kommer til at inngrepet er i samsvar med loven, blir spørsmålet om inngrepet også er nødvendig i et demokratisk samfunn pga. et legitimt hensyn (eller i FN-konvensjonens terminologi om inngrepet er vilkårlig).

EMDs rettspraksis viser at domstolen generelt sett har akseptert at overvåking og informasjonsinnsamling har tilstrebet et legitimt formål, uten å dra statenes vurdering av dette i tvil. EMDs drøftelser har først og fremst dreid seg om overvåkingen og informasjonsinnhentingen kan anses «nødvendig i et demokratisk samfunn». For at inngrepet skal anses nødvendig i et demokratisk samfunn må det være *forholdsmessig* («proportional») i forhold til det legitime formålet som forfølges. Forholdsmessighetsvurderingen er en konkret skjønnsmessig vurdering hvor en rekke faktorer tas i betraktning. EMD har lagt til grunn at statene har en nokså vid skjønnsmargin når de skal foreta interesseavveiningen mellom retten til et privatliv og hensynet til å beskytte nasjonal sikkerhet. Se for eksempel avvisningsavgjørelsen *Weber og Saravia mot Tyskland* avsnitt 106 med videre henvisninger:

> «[W]hen balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, it has consistently recognized that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security…».

Samtidig understreker domstolen samme sted at dette ikke betyr at statene har ubegrenset diskresjonær myndighet til å gjøre personer innen sin jurisdiksjon gjenstand for hemmelig overvåking, og at interesseavveiningen vil avhenge av en konkret vurdering av alle sakens omstendigheter:

> «Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate effective guarantees against abuse (…) . This assessment depends on all the circumstances of the case such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law...».

På grunn av at hemmelig overvåking ikke kan påklages, da den som overvåkes ikke er kjent med den, har EMD videre lagt til grunn at overvåkingen må være underlagt effektiv kontroll. Kontrollen bør normalt sett ligge til den dømmende myndighet, i alle fall i siste instans, da domstolene gir de beste garantier for uavhengighet og upartiskhet (jf. *Klass m. fl. mot Tysland* avsnitt 55–56 og *Kennedy mot UK* avsnitt 167). EMD har imidlertid lagt til grunn at fravær av rettslig kontroll ikke automatisk fører til brudd på EMK art 8. I *Klass m.fl.* fant EMD at en parlamentarisk komité med balansert politisk sammensetning og en uavhengig myndighetskommisjon som gjennomførte overvåkingen, var tilstrekkelig for å oppfylle kravet om effektiv, uavhengig og permanent kontroll. Det ble også lagt vekt på at en person som mistenkte at han var gjenstand for overvåking, hadde klageadgang til kommisjonen, selv om denne adgangen bare forelå under særlige omstendigheter (se *Klass m. fl. mot Tyskland* avsnitt 56).

Lagring i lang tid av opplysninger innhentet gjennom overvåking kan også anses som et uforholdsmessig inngrep, jf. *Segerstedt-Wiberg og andre mot Sverige* av 6. juni 2006. EMD kom til at oppbevaring gjennom lang tid av opplysninger om at noen hadde planlagt et bombeattentat, ikke var i strid med EMK art. 8, mens oppbevaring av informasjon vedr. deltakelse på et politisk møte i 1967 eller at en klager hadde planlagt å utøve voldelig motstand mot politiet under en demonstrasjon i 1969, ble ansett for å være uforholdsmessig, tatt i betraktning opplysningenes natur og deres alder.

Som det fremkommer foran vil videreformidling av innhentet informasjon utgjøre et selvstendig inngrep i privatlivet. Selv om selve innhentingen av informasjonen var forholdsmessig av hensyn til et legitimt formål, er det ikke dermed sagt at videreformidling av informasjonen vil være det, enten informasjonen deles med andre nasjonale myndigheter eller med utenlandske myndigheter.

10.3.2 I hvilken grad kommer menneskerettighetene til anvendelse ved grenseoverskridende overvåking og informasjonsinnhenting, jf. EMK art. 1 og SP art. 2 nr. 1?

For at en stat skal kunne holdes ansvarlig for handlinger eller unnlatelser som gir grunnlag for brudd på menneskerettskonvensjonene, er det et vilkår at staten må kunne anses å utøve jurisdiksjon, jf. EMK art. 1 og SP art. 2 nr. 1.

Hvor en stat overvåker noen som befinner seg på statens territorium, er det på det rene at staten kan bli holdt ansvarlig for menneskerettsstridige inngrep i vedkommendes privatliv, selv om dette skulle skje i form av grenseoverskridende informasjonsinnhenting. Men hvordan stiller jurisdiksjonsspørsmålet seg hvis informasjonsinnhentingen finner sted på statens territorium, men hvor den som overvåkes ikke befinner seg der (for eksempel hvor en stat henter ut opplysninger om personer i utlandet fra en fiberoptisk kabel som befinner seg på statens territorium eller i statens territorialfarvann)? Og hva hvis man fjerner seg enda lengre fra statens territorium, ved at den som er gjenstand for et inngrep i sitt privatliv ikke befinner seg på statens territorium og heller ikke statens inngrep skjer der (for eksempel hvor en stat hacker seg inn i PCen til noen i utlandet eller fanger opp vedkommendes e-post i et annet land)? I begge tilfeller har statens handling virkning utenfor statens territorium.

Spørsmålet om menneskerettighetenes ekstraterritorielle anvendelse var et vanskelig punkt under forhandlingene i 2013 og 2014 om FNs generalforsamlings resolusjon om retten til et privatliv i den digitale tidsalder, jf. nærmere nedenfor om denne. Iht. FNs konvensjon om sivile og politiske rettigheter art. 2 nr. 1 skal statene «respektere de rettigheter som anerkjennes i konvensjon, og sikre dem for alle som befinner seg på dens territorium og er undergitt dens jurisdiksjon» («within its territory and subject to its jurisdiction»). USAs offisielle holdning er at SP art. 2 nr. 1 inneholder to kumulative vilkår for jurisdiksjon, som begge må være oppfylt for at konvensjonen skal komme til anvendelse, og at menneskerettighetene derfor ikke kan komme til ekstraterritoriell anvendelse. Dette er et syn som ikke har støtte i internasjonal rettspraksis, og som Norge sammen med en rekke andre stater ikke deler. Norge er dessuten i tillegg bundet av EMK, som har en jurisdiksjonsbestemmelse som ikke refererer til territorium, bare til jurisdiksjon. Etter EMK art. 1 skal statspartene sikre enhver konvensjonens rettigheter og friheter «innen sitt myndighetsområde» («within their jurisdiction»). EMD har gitt EMK ekstraterritoriell anvendelse i en lang rekke saker under visse vilkår. Tilsvarende har FNs menneskerettskomité gjort med FNs konvensjon om sivile og politiske rettigheter. At menneskerettighetene derfor generelt sett, avhengig av de nærmere omstendighetene, *kan* komme til ekstraterritoriell anvendelse er etter vårt syn på det rene.

Også EMD har imidlertid lagt til grunn i sin rettspraksis at en stats jurisdiksjon etter EMK art. 1 først og fremst er territoriell, og at handlinger begått av en statspart som er utført på, eller som har virkninger utenfor en stats territorium, bare unntaksvis kan utgjøre utøvelse av jurisdiksjon etter EMK art. 1.[2] Om slike eksepsjonelle omstendigheter foreligger, må etter EMDs rettspraksis besluttes utfra de særlige omstendighetene i den foreliggende sak. EMD har i sin rettspraksis anerkjent en rekke slike eksepsjonelle omstendigheter som kan medføre jurisdiksjonsutøvelse utenfor en stats eget territorium.

For det første har EMD lagt til grunn at *statlige agenters utøvelse av myndighet og kontroll* («authority and control») utenfor eget territorium kan gi grunnlag for jurisdiksjon. (Se nærmere for eksempel *Al- Skeini m.fl. mot UK* av 7.7.2011 avsnitt 133–137). For det andre har EMD lagt til grunn at en stat kan ha ekstraterritoriell jurisdiksjon etter EMK art. 1 når staten utøver *effektiv kontroll over et område*. Den kontrollerende staten har i disse tilfeller ansvar for å sikre alle konvensjonsrettighetene staten er bundet av på det kontrollerte området. (Se nærmere for eksempel *Al-Skeini m.fl.* avsnitt 138–140.) FNs menneskerettskomité har lagt til grunn tilsvarende vurderingstema etter FN-konvensjonen om sivile og politiske rettigheter.[3]

EMD har så langt, så vidt vi er kjent med, ikke avsagt noen avgjørelse hvor domstolen tar uttrykkelig stilling til jurisdiksjonsspørsmålet i grenseoverskridende internettrelaterte saker eller om grenseoverskridende informasjonsinnhenting. Spørsmålet ble berørt i den ovennevnte saken *Weber and Saravia mot Tyskland* fra 2006, hvor klagerne klaget over at Tyskland hadde brutt deres konvensjonsrettigheter i forbindelse med overvåking av telekommunikasjon fra deres telefonforbindelser i Uruguay. Tyskland argumenterte bl.a. med at «*the monitoring of telecommunications made from abroad, however, had to be qualified as an extraterritorial act. In accordance with the Court's decision in the case of Bankovic and Others v. Belgium and Others (…) the applicants therefore did not come within Germany's jurisdiction within the meaning of Article 1 of the Convention – a concept which was primarily territorial – on account of that act*». Domstolen fant det imidlertid ikke nødvendig å ta stilling til spørsmålet siden klagen uansett måtte avvises da domstolen fant at det ikke hadde funnet sted noe konvensjonsbrudd. I ovennevnte sak *Liberty m.fl. mot Storbritannia* fra 2008 ble Storbritannia domfelt for brudd på EMK art. 8 for overvåking av samtaler mellom en britisk og to irske organisasjoner basert i henholdsvis London og Dublin. Kommunikasjonen frem og tilbake mellom Dublin og London ble fanget opp på «Capenhurst Electronic Test Facility» på britisk territorium. Det ble ikke anført av Storbritannia i saken at EMK ikke kom til anvendelse på saksforholdet for så vidt gjaldt de irske klagerne, og EMD reiste heller ikke spørsmålet av eget tiltak.

Hvor informasjonsinnhentingen skjer på en stats territorium, som i *Liberty m.fl.*, kan det argumenteres for jurisdiksjon på grunnlag av territorialprinsippet, selv om virkningen er ekstraterritoriell. Når det gjelder situasjoner hvor både informasjonsinnhentingen og virkningen av inngrepet i privatliv eller kommunikasjon skjer utenfor statens territorium, for eksempel hvor en stat hacker seg inn i PCen til noen eller fanger opp vedkommendes e-post i et annet land, vil det derimot være modellen med myndighet og kontroll over personer som er relevant. Samtidig kan det stilles spørsmål ved om det er noen grunn til å behandle de to situasjonene forskjellig. I begge tilfeller er virkningen av menneskerettsinngrepet ekstraterritoriell.

Det er uklart hvordan EMD vil forholde seg til kriteriene effektiv kontroll over et område eller myndighet og kontroll over personer i fremtidige saker om grenseoverskridende overvåking og informasjonsinnhenting dersom spørsmålet kommer på spissen, evt. om domstolen kan komme til at det kan tenkes andre typer av eksepsjonelle omstendigheter som kan nødvendiggjøre og berettige ekstraterritoriell jurisdiksjon enn det som er dekket av disse to vurderingstemaene.

I denne forbindelse synes bl.a. følgende uttalelse i EMDs avgjørelse *Ben El Mahi mot Danmark* (klage nr. 5853/06) av 11.12.2006 relevant, hvor EMD begrunner de unntakene fra territorialprinsippet som domstolen har fastsatt gjennom sin rettspraksis:

> *«Accountability in such situations stems from the fact that Article 1 cannot be interpreted so as to allow a State Party to perpetrate violations of the Convention on the territory of another State which it would not be permitted to perpetrate on its own territory.»*

---

2 Se for eksempel. *Al- Skeini m.fl. mot UK* av 7.7.2011 avsnitt 131.

3 Se FNs høykommissær for menneskerettigheters rapport om rett til privatliv i den digitale tidsalder av 30. juni 2014, avsnitt 32.

Hvis man skulle konkludere med at EMK art. 8 ikke kan komme til ekstraterritoriell anvendelse på overvåking eller informasjonsinnhenting, fordi staten ikke vil kunne anses å ha effektiv kontroll over området hvor vedkommende befinner seg, eller myndighet og kontroll over vedkommende, vil en stat med relativt enkle hjelpemidler og uten å pådra seg nevneverdige kostnader kunne begå omfattende konvensjonsbrudd utenfor sine grenser som ikke vil være tillatt etter konvensjonen på statens eget territorium. Det har også blitt argumentert med at dette ville kunne åpne for samarbeid om deling av etterretningsinformasjon mellom stater med sikte på å omgå statenes menneskerettsforpliktelser overfor personer på eget territorium. Det kan derfor argumenteres for at dette, etter omstendighetene, vil kunne gi et lite tilfredsstillende resultat, og utfordrer derfor EMDs og FNs menneskerettskomites hittil utviklede rettslige vurderingstema mht. ekstraterritoriell jurisdiksjon. På den annen side kan det imidlertid også argumenteres med at innhenting av informasjon om personer som befinner seg på et statskontrollert territorium eller som på annen måte er underlagt statens myndighet og (fysiske) kontroll, lettere kan brukes, herunder misbrukes, mot vedkommende av staten, enn når det gjelder informasjonsinnhenting rettet mot personer på andre staters territorium, og at EMDs gjeldende kriterier for ekstraterritoriell jurisdiksjon derfor er relevante og ikke bør strekkes for langt.

FNs høykommissær for menneskerettigheter omtaler spørsmålet om ekstraterritoriell anvendelse av SP art. 17 i rapport om retten til et privatliv av 30. juni 2014, utarbeidet på anmodning av FNs generalforsamling i resolusjon 68/167 om samme tema (se rapportens avsnitt 32–34). I rapportens avsnitt 34 uttaler høykommissæren:

> *«It follows that digital surveillance (….) may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control in relation to digital communications infrastructure, wherever found, for example, through direct tapping or penetration of that infrastructure. Equally, where the State exercises regulatory jurisdiction over a third party that physically controls the data, that State also would have obligations under the Covenant. If a country seeks to assert jurisdiction over the data of private companies as a result of the incorporation of those companies in that country, then human rights protection must be extended to those whose privacy is being interfered with, whether in the country of incorporation or beyond. This holds whether or not such an exercise of jurisdiction is lawful in the first place, or violates another State's sovereignty».*

FNs generalforsamling uttrykte i enstemmige resolusjoner om rett til et privatliv i den digitale tidsalder av desember 2013 og desember 2014 (res. 68/167 og res. 69/166) at den var «*deeply concerned at the negative impact that surveillance and/or interception of communication, including extraterritorial (...), may have on the exercise and enjoyment of human rights*». Men statene klarte ikke å enes om tekst som reflekterte Høykommissærens uttalelser ovenfor.

Som belyst ovenfor er det betydelig usikkerhet knyttet til jurisdiksjonsspørsmålet ved grenseoverskridende overvåking og informasjonsinnhenting, hvor den som overvåkes ikke befinner seg på statens territorium. Det forventes imidlertid at det etter hvert vil komme rettsavgjørelser som vil kaste lys over dette spørsmålet.

Vi finner avslutningsvis grunn til å understreke at selv om EMK art. 8 skulle komme til anvendelse på overvåking av og informasjonsinnhenting om personer i utlandet, betyr selvfølgelig ikke dette at slik informasjonsinnhenting av sikkerhetshensyn ikke vil være tillatt. Dette vil beror på en nærmere forholdsmessighetsvurdering. Det kan ikke utelukkes at denne vurderingen vil kunne slå annerledes ut dersom det er tale om innhenting av informasjon relatert til eksterne trusler.

10.3.3 FN-resolusjonene om retten til et privatliv i den digitale tidsalder

Vi nevner også FNs generalforsamlings to resolusjoner om retten til et privatliv i den digitale tidsalder. Resolusjonene er ikke rettslig bindende, men kan anses å reflektere visse minstestandarder. Resolusjon 68/167 av 18. desember 2013 hadde først og fremst betydning ved at den innledet en internasjonal dialog om personvern i det digitale rom. Resolusjonen ga FNs høykommissær for menneskerettigheter i mandat å utarbeide en rapport om temaet, som forelå 30. juni 2014.

Høykommissærens rapport dannet så utgangspunktet for forhandlingene om en ny resolusjon på området, nr. 69/166, vedtatt av FNs generalforsamling 18. desember 2014. Som oppfølging av Generalforsamlingens sistnevnte resolusjon, vedtok FNs menneskerettsråd 24. mars 2015 å oppnevne en spesialrapportør for personvern.

10.4 Europarådets personvernkonvensjon

Europarådets konvensjon nr. 108 av 28. januar 1981 om personvern i forbindelse med elektronisk databehandling av personopplysninger ble ratifisert av Norge 20. februar 1984. Konvensjonen er så langt ratifisert av 46 stater, hvorav én ikke-Europarådsstat (Uruguay). Det er den eneste internasjonale konvensjonen som gjelder behandling av personopplysninger, herunder som søker å regulere grenseoverskridende strømmer av data.

Konvensjonens formål, nedfelt i artikkel 1, er

> *«å sikre respekt for enhver enkeltpersons rettigheter og grunnleggende friheter og især retten til privatlivets fred på territoriet til enhver part, uten hensyn til statsborgerskap eller bopel, i forbindelse med elektronisk databehandling av personopplysninger som vedrører ham».*

I konvensjonens forklarende rapport understrekes det at de garantier konvensjonen gir, ikke kan begrenses til statens egne borgere eller personer med lovlig opphold i staten:

> *«The guarantees set out in the convention are extended to every individual regardless of nationality or residence. This provision is in accordance with the general principle of the Council of Europe and its member States with regard to the protection of individual rights. Clauses restricting data protection to a State's own nationals or legally resident aliens would be incompatible with the convention.»*

Konvensjonen definerer personopplysninger vidt: «*enhver opplysning som gjelder en bestemt eller identifiserbar enkeltperson*», jf. konvensjonens art. 2 bokstav a.

Ved bearbeiding av denne type opplysninger ved elektronisk databehandling, skal de iht. konvensjonens art. 5:

> *«a) innsamles og bearbeides på rettferdig og lovlig vis;*
> *b) lagres for bestemte og lovlige formål og ikke nyttes på en måte som er uforenlig med disse formål;*
> *c) være adekvate, relevante og ikke for omfattende i relasjon til de formål de lagres til;*
> *d) være nøyaktige og, der det er nødvendig, holdt a jour;*
> *e) oppbevares på en måte som ikke gir anledning til å identifisere datasubjektene lenger enn nødvendig for det formål som disse opplysningene lagres til.»*

Konvensjonen gir enhver rett til å vite om det eksisterer et elektronisk persondataregister, dets formål og få vite om og evt. korrigert eller slettet opplysninger som er lagret i strid med konvensjonen, samt ha klageadgang dersom disse rettighetene ikke respekteres, jf. konvensjonens art. 8.

Konvensjonens art. 6 peker på kategorier av særlig sensitive opplysninger som skal nyte et særskilt vern:

> *«Personopplysninger som åpenbarer rasemessig opprinnelse, politiske oppfatninger samt religiøs eller annen tro, så vel som personopplysninger vedrørende helse eller seksualliv, kan ikke behandles elektronisk med mindre intern lovgivning gir tilstrekkelig vern. Det samme skal gjelde for personopplysninger som gjelder domfellelser for straffbare handlinger.»*

Det kan gjøres unntak fra konvensjonens art. 5, 6 og 8, nevnt ovenfor, når dette er fastsatt i lov og er et nødvendig tiltak i et demokratisk samfunn av hensyn til a) beskyttelse av statens sikkerhet, offentlig sikkerhet, statens økonomiske interesser eller bekjempelse av kriminelle handlinger eller b) beskyttelse av datasubjektet eller andres rettigheter og friheter. Dette er mer eller mindre sammenfallende med ordlyden i EMK art. 8 nr. 2.

10.5 Europarådets konvensjon nr. 185 om datakriminalitet

Europarådets konvensjonen nr. 185 om datakriminalitet (Budapestkonvensjonen) ble ratifisert av Norge 30. juni 2006. Så langt har 39 Europarådsmedlemsstater og seks ikke-medlemsstater, deriblant USA og Japan, sluttet seg til konvensjonen. Partene til Budapestkonvensjonen har forpliktet seg til gjensidig strafferettslig samarbeid i saker vedrørende datakriminalitet, herunder til å bistå hverandre med innhenting av elektroniske bevis for datakriminalitet. Vi nøyer oss med å vise til konvensjonens kapitel III om strafferettslig samarbeid som i artiklene 25–34 gir nærmere og detaljerte regler om grenseoverskridende informasjonsinnhenting for dette formål.

10.6 Norges forpliktelser som følger av EØS-avtalen og øvrige avtaler med EU

EUs regelverk omfatter i dag store deler av informasjonssamfunnet. Regelverket er i all hovedsak tatt inn i norske lover og forskrifter gjennom EØS-avtalen, og omfatter blant annet ekom/telekom, elektronisk handel, elektroniske signaturer, frekvensforvaltning, gjenbruk av offentlige data og personvern.[4]

Det indre markedet i EU består av over 500 millioner innbyggere. I EU har det helt fra samarbeidet startet, vært store forventninger til dette markedets betydning for europeisk økonomi, og det satses i stor grad på at en felles digital politikk vil realisere intensjonen om ett felles europeisk indre marked. Dette krever felles regelverk og strategiprogrammer som skaper tillit til markedet hos både næringsliv og forbrukere. Et sentralt mål er derfor at både næringslivet og forbrukerne skal beskyttes gjennom sikker kommunikasjon, sikre betalingsløsninger, forbrukerrettigheter og ivaretagelse av borgernes personvern. For å kunne realisere et trygt indre digitalt handelsmarked stilles det også krav til felles forebygging og bekjempelse av kriminalitet som må innrettes slik at tilliten mellom markedsaktørene og forbrukerne opprettholdes.

EØS-avtalen er Norges mest omfattende folkerettslige avtale. Avtalen er multilateral og omfatter i dag 31 land – de 28 EU-statene og de tre EFTA-statene Island, Liechtenstein og Norge. For å delta i EUs indre marked forpliktet Norge seg til å overta EU-retten og gjennomføre den på samme måte som i EU. Norge har tatt inn tre fjerdedeler av EUs rettsakter i norsk rett.[5] Å gjennomføre rettsreglene på samme måte som i EU innebærer også at reglene skal fortolkes og anvendes på samme måte som i de øvrige medlemslandene. Det betyr at EU-domstolens avgjørelser også er bindende for Norge. Videre forpliktet Norge seg til å utvikle avtalen i pakt med den underliggende EU-retten. EØS-avtalen og de øvrige avtalene Norge har inngått med EU, er langt mer omfattende enn det som tradisjonelt omfattes av folkerettslige avtaler. Det som kjennetegner de folkerettslige avtalene, er at det etableres gjensidige forpliktelser mellom statene som sådanne. Norges avtaler med EU er til sammenligning å betrakte som overnasjonale, ved at både Stortingets, regjeringens og domstolenes kompetanse i praksis begrenses som følge av plikten til å følge EUs rettsutvikling, selv om Norge formelt sett har adgang til å reservere seg.[6]

Kjernen i avtalen er at EFTA-statene overtar all relevant EU-rett som regulerer det felles markedet, som igjen er basert på reglene om «de fire friheter» – fri bevegelse av varer, tjenester, arbeidskraft og kapital. Et annet kjerneområde er reglene som skal sikre like konkurransevilkår i markedet, gjennom blant annet regler om statsstøtte, offentlige kontrakter og forbud mot ulovlig prissamarbeid og misbruk av markedsmakt. Gjennom årene er reguleringen av det indre markedet i EU spesifisert nærmere for viktige sektorer som energi, samferdsel, bank og forsikring, IKT med mer, og er dermed utvidet til å gjelde en lang rekke områder som grenser opp mot markedet. Videre er markedsreglene supplert med regler som skal kompensere for uheldige sider ved markedet – herunder arbeids- og arbeidsmiljørett, personvern, miljø og klima med mer. I tillegg kommer egne avtaler om politisamarbeid, som Schengen-avtalen med tilleggsavtaler.

10.6.1 EUs regelverk for nettverks- og informasjonssikkerhet (NIS-direktivet)

Den 7. februar 2013 la EU-kommisjonen frem forslag til et direktiv for å sikre et felles nivå for nett- og informasjonssikkerhet i EU. Bakgrunnen er at det i EU per i dag ikke er etablert tilstrekkelige og helhetlige felles sikkerhetstiltak. Medlemslandene har ulik kvalitet på sikkerhetstiltakene de har implementert, noe som skaper en fragmentert tilnærming. EU har frem til nå bare hatt felles sikkerhetsregulering av ekomsektoren, mens felles regler er viktig også for annen infrastruktur og IKT-tjenester.

Aktørene som omfattes av direktivet, er offentlig og privat sektor, det vil si stat, kommuner, fylker og virksomheter innenfor sektorene transport, vannforsyning, helse og omsorg, bank og finans, samt eiere og driftere av samfunnskritisk IKT-infrastruktur. For samfunnskritiske tjenester gjelder forslaget tilbydere som er sterkt avhengige av informasjons- og kommunikasjonsteknologi, som er av avgjørende betydning for å kunne opprettholde viktige økonomiske eller samfunnskritiske funksjoner. I tillegg omfattes e-handelsplattformer, Internett-betalingsportaler, sosiale

[4] NOU 2012: 2 *Utenfor og innenfor – Norges avtaler med EU*, kapittel 5.1.2.

[5] Ibid.

[6] Basert på kapittel 26 i NOU 2012: 2 *Utenfor og innenfor – Norges avtaler med EU.*

nettverk, søkemotorer, skytjenester og applikasjonsbutikker. Softwareutviklere og hardwareprodusenter er ikke omfattet.

Direktivet vil også stille krav om at det utarbeides nasjonale strategier for nett- og informasjonssikkerhet, og at det skal finnes én eller flere nasjonale myndigheter på dette området – et nasjonalt kontaktpunkt og et nasjonalt hendelseshåndteringsorgan (CSIRT). Det skal også etableres nettverk for samarbeid mellom medlemsstatene, blant annet for de nasjonale CSIRT-ene og CERT-EU, som er dedikert EU-institusjoner, og byråer som gir operasjonell støtte til deres IT-team og er kontaktpunkt for andre lands CERT-miljøer. NSM NorCERT mottar jevnlig rapporter og nyhetssammenstillinger fra CERT-EU. I tillegg har de operativt hendelseshåndterings- og informasjonsdelingssamarbeid. CERT-EU er også medlem av EGC. Gjennom nettverk for kompetente nasjonale myndigheter skal medlemsstatene utveksle informasjon og samarbeide på basis av den europeiske planen for samarbeid innenfor dette området for å forebygge, bekjempe og håndtere trusler og hendelser innenfor nett- og informasjonssikkerhetsområdet.

Direktivet vil, gjennom bestemmelsene i artikkel 14–16, bidra til å etablere felleseuropeiske sektorovergripende minimumsstandarder for nettverks- og informasjonssikkerhet. Basert på modellen fra rammedirektivet for elektronisk kommunikasjon tar forslaget sikte på å utvikle en risikostyringskultur og at informasjon deles mellom privat og offentlig sektor. Virksomheter i de særlig kritiske sektorene og offentlige myndigheter vil bli forpliktet til å vurdere risikoen de står overfor, og til å gjennomføre nødvendige og forholdsmessige risikoreduserende tiltak for å ivareta nettverks- og informasjonssikkerheten. Disse enhetene vil bli pålagt å underrette den nasjonale kompetente enheten om enhver hendelse som i alvorlig grad truer deres nettverks- og informasjonssystemer. Direktivet stiller krav om at medlemslandene etablerer regler om sanksjoner hvis aktørene ikke oppfyller sine plikter. Direktivet kan på dette området medføre en endring i forhold til dagens rettstilstand som etter omstendighetene vil kunne berøre og få konsekvenser for et betydelig antall virksomheter.

Når det gjelder virksomhetenes plikter, vises det til rammedirektivet for ekomtjenester (2002/21/EF) og kommunikasjonsdirektivet (2002/58/EF). Etter planen skulle direktivet besluttes i løpet av våren 2015.

10.6.2 Ekom

På europeisk nivå reguleres elektroniske kommunikasjonsnett og -tjenester i hovedsak av den såkalte ekompakken, en samling rettsakter som ble vedtatt i 2002. Den siste større revisjonen ble gjort i 2009. I Norge er disse forpliktelsene inntatt i lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven). Særlig viktig i denne forbindelse er reglene om sikkerhet og beredskap i rammedirektivet (2002/21/EC) og kommunikasjonsverndirektivet (2002/58/EC).

Overordnet sett er den europeiske reguleringen av kommunikasjonsvern, som hovedsakelig regulerer personvern og informasjonssikkerhet, mer moden og utfyllende enn reguleringen av sikkerhet og beredskap. Sistnevnte har tradisjonelt blitt ansett som mer av et ansvar for de enkelte medlemslandene, og har vært mer preget av nasjonale sikkerhetsinteresser.

Gjennom rammedirektivet artikkel 13 a og 13 b er medlemslandene forpliktet til å sikre at det iverksettes tilstrekkelige («appropriate») tekniske og organisatoriske tiltak for å kontrollere sikkerhetsrisikoen i nett og tjenester. Bestemmelsen er inkorporert i ekomloven § 2-10, som går til dels betydelig lenger enn direktivets minimumsregulering. Medlemsstatene skal også varsle EU-organet ENISA ved utfall og forstyrrelser over visse terskelverdier i nett.

Kommunikasjonsverndirektivet legger relativt sterke begrensninger på tilbydernes muligheter til å benytte seg av brukernes kommunikasjon i deres nett og tjenester til andre formål enn å levere tjenesten. Medlemsstatene skal for eksempel forby innholdsanalyse uten samtykke (artikkel 5), samt at trafikk- og lokaliseringsdata er underlagt behandlingsbegrensninger og sletteplikt (artikkel 6 og 9). Disse forpliktelsene er gjennomført i norsk rett gjennom ekomloven §§ 2-7 og 2-9. Også myndighetenes adgang til slik informasjon fra tilbyderne avskjæres tilsynelatende gjennom de materielle begrensningene som er nevnt ovenfor.

Etter kommunikasjonsverndirektivets systematikk er dermed all nasjonal lovgivning om for eksempel kommunikasjonskontroll, innhenting av trafikkdata og strategisk trafikkovervåking å anse som unntak fra direktivet. Slike unntak må oppfylle vilkårene i artikkel 15, som setter krav til at lovgivningen må være forholdsmessig og nødvendig for å ivareta definerte formål. Videre stilles det krav om samsvar med generelle EU-rettslige prinsipper og EUs charter om grunnleggende rettigheter.

Kommunikasjonsverndirektivet artikkel 15 legger med andre ord opp til en vurdering som ligger nær opp til inngrepsvurderingen etter EMK artikkel 8, men der EU-domstolen er øverste tolkningsinstans. Senere rettspraksis fra EU-domstolen, særlig Digital Rights Ireland (C-293/12), gir grunn til å tro at EU-domstolen vil prøve denne typen spørsmål med større intensitet enn EMD tradisjonelt har gjort. Kommisjonen har varslet at kommunikasjonsverndirektivet skal revideres, og arbeidet er antatt å starte etter at personvernforordningen er vedtatt.

10.6.3 Personverndirektivet

Regler for en forsvarlig elektronisk behandling av personopplysninger innenfor EU er en vesentlig forutsetning for digital kommunikasjon innenfor det felles markedet. Gjeldende norsk lovgivning om behandling av personopplysninger, personopplysningsloven, er gjennomført som del av EØS-avtalen ved personverndirektiv 95/46/EF. Reglene er forankret i Den europeiske menneskerettskonvensjonen EMK artikkel 8, som er omtalt i ovenfor under punkt 10.3.1. Europakommisjonen presenterte 25. januar 2012 en reform for modernisering av EUs personvernregler. Kommisjonen har foreslått to nye regelverk: en generell forordning om beskyttelse av personopplysninger og et direktiv for myndighetenes behandling av personopplysninger i politi- og straffesektoren. Personvernforordningen skal erstatte gjeldende direktiv. Det overordnede målet med EU-kommisjonens forslag til reform er å oppdatere og modernisere personvernprinsippene som er nedfelt i 1995-direktivet, i tråd med den digitale utviklingen og de mulighetene dette byr på for realiseringen av ett felles digitalt marked innenfor EU.

Hovedintensjonen med reguleringsforslaget er å sørge for et mer enhetlig regelverk i EU. Derfor benyttes forordning fremfor direktiv, ettersom en forordning vil sikre identiske generelle personvernregler i samtlige EU/EØS-land. Den tidligere reguleringen i form av direktiv gir minimumsregler med større adgang for den enkelte stat til å tilpasse reglene til nasjonal lovgivning. Det har videre vært et mål å styrke enkeltindividets rådighet over egne opplysninger og å bygge opp befolkningens tillit til at virksomheter behandler personopplysninger på en forsvarlig måte.

Kommisjonen legger til grunn at det er nødvendig å ta borgernes mistillit til virksomheter som behandler personopplysninger, på alvor etter en befolkningsundersøkelse om personvern i EU. Undersøkelsen viste at ni av ti (92 prosent) er bekymret for blant annet mobile applikasjoner som samler og bearbeider data uten deres samtykke. Videre gikk det frem at sju av ti europeere er bekymret for virksomhetenes bruk av personopplysninger.

Reformen har derfor som et helt sentralt mål å styrke borgernes personvernrettigheter. Bedre beskyttelse av personopplysninger og større grad av kontroll over egne opplysninger hos den enkelte borger skal gjenoppbygge tilliten til at personopplysninger behandles forsvarlig, herunder når opplysninger formidles via Internett over landegrensene. Viktige endringsforslag er innføringen av en rett til – på nærmere bestemte vilkår – å få slettet personopplysninger om seg selv («rett til å bli glemt»),[7] rett til å få kopi av egne personopplysninger, rett til å overføre egne personopplysninger til alternative tilbydere av en tjeneste («rett til dataportabilitet»), samt styrking av barns personvern. Videre skal borgerne gis økte rettigheter til informasjon om forhold knyttet til behandlingen av egne personopplysninger, som lagringstid og klagerett. Det skal også innføres bestemmelser som skal øke bruken av personvernfremmende teknologi med det mål å sikre at personvernhensyn blir tatt i betraktning på et tidlig stadium ved utvikling og valg av IT-løsninger.

Regelverksutkastet legger opp til en ny institusjonell struktur på personvernområdet. Det er også foreslått å opprette en felles europeisk datatilsynsmyndighet (European Data Protection Board), som skal bestå av representanter fra de ulike medlemsstatenes tilsynsmyndigheter. Forslaget åpner videre for en stor grad av delegert lovgivningsmyndighet til Kommisjonen. For å redusere kostnadene knyttet til å etterleve personvernregelverket ønsker Kommisjonen å innføre en «one stop shop»-ordning. Det vil innebære at virksomheter som etablerer seg innenfor flere EU-land, bare skal forholde seg til én tilsynsmyndighet innenfor EØS-området. Videre gis nasjonale personvernmyndigheter nye verktøy for å

[7] Den 13. mai 2014 avgjorde EU-domstolen at EUs personverndirektiv og nasjonal personvernlovgivning gjelder for søkemotorselskaper som har tilstedeværelse i et EU-land. Dommen slår blant annet fast at slike selskaper har et selvstendig behandlingsansvar for personopplysningene som indekseres, selv om opplysningene først er publisert av andre medier. Søkemotorselskaper må legge til rette for at enkeltpersoner kan be om å få fjernet belastende informasjon, som nettsaker fra aviser eller lignende, som er indeksert av søkemotoren. Informasjon som i utgangspunktet er riktig, kan med tiden vise seg å bli utilstrekkelig, irrelevant eller overdimensjonert, slo domstolen fast. Dermed skal privatpersoner ha rett til å få fjernet opplysninger i søkemotorens treffliste, selv om de ikke kan kreve at den som har publisert informasjonen, trekker den tilbake.

sanksjonere brudd på regelverket, herunder myndighet til å ilegge bøter på inntil 1 000 000 euro, eller, for næringsselskaper, inntil 2 prosent av selskapets omsetning på verdensbasis.

Det rettslige grunnlaget for rettsakten er artikkel 16 i traktaten om Den europeiske unions virkemåte. Forordninger gir som nevnt i mindre grad adgang til å gi regler på nasjonalt nivå enn det direktiver gjør. Fordelen er at EU-landene får et mer enhetlig regelverk, noe som forhindrer uoversiktlig og ulik gjennomføring av personvernregler i de ulike landene. Dette gir også større forutsigbarhet for norske borgere og deres rettigheter i møte med utenlandske aktører. For næringslivet vil det bli enklere å operere internasjonalt fordi det vil foreligge ett europeisk regelsett å forholde seg til.

Medlemslandene synes å være enige om at det er på høy tid å fornye EU-regelverket om behandling av personopplysninger. Det er viktig at regelverket er tilpasset dagens teknologiske virkelighet med mål om en teknologinøytral regulering som tar høyde for å kunne fungere også for fremtidig teknologi. Rettighetene som foreslås for borgerne, er langt på vei i samsvar med dagens norske personvernlovgivning.

10.6.4 Politisamarbeid

I tillegg til EØS-avtalen har Norge inngått en rekke forpliktende avtaler med EU. Justissektoren er et av områdene med størst omfang, og Norge deltar aktivt i EUs politisamarbeid. En del av dette skjer gjennom Schengen-avtalen, som særlig har regler om informasjonsutveksling for politiet. Blant de prioriterte områdene for dette samarbeidet er Internett-kriminalitet. Det er utformet regler og prosedyrer for blant annet felles teknisk infrastruktur, felles strategier og prioriteringer og ikke minst effektiv informasjonsutveksling med en utvikling i retning av direkte søkeadgang i samarbeidende lands databaser.

Politisamarbeidet i EU er bygd på tanken om at dette skal være kompenserende tiltak for å redusere de negative virkningene i form av økt grensekryssende kriminalitet som bortfallet av grensekontroll har hatt. Dette er fortsatt en grunntanke, men den har utviklet seg og omfatter nå også bekjempelse av alvorlig kriminalitet mer generelt. Samarbeidet omfatter en rekke forskjellige elementer. Norges avtaler med EU på dette området er i første rekke:

Europeisk cyberkrimsenter (EC3)

Senteret ble opprettet 01. januar 2013 ved Europol og skal være navet i EUs kamp mot datakriminalitet og bidra til raskere reaksjoner ved lovbrudd på nett. Senteret skal dessuten støtte medlemsstatene og EUs institusjoner i å bygge operativ og analytisk kapasitet for undersøkelser og samarbeid med internasjonale partnere.

The European Union's Judicial Cooperation Unit (EUROJUST)

EUROJUSTs oppgave er å bidra til et effektivt samarbeid mellom medlemsstatene i saker om alvorlig, organisert og grenseoverskridende kriminalitet, samt å få lovovertredere for retten hurtig og effektivt. Innenfor sitt ansvarsområde har EUROJUST vært involvert i en rekke saker knyttet til IKT-kriminalitet, blant annet saker som gjelder spredning av overgrepsbilder på nett. I tillegg er det avtaler på følgende områder:

- den europeiske arrestordren
- gjensidig bistand i straffesaker
- informasjonsutveksling gjennom SIS, SIS II med mer
- Informasjonsutveksling gjennom Prüm-avtalen

Etter anmodning, og etter en omfattende prosess, oppnådde Norge i november 2009 en avtale om tilknytning til EUs forsterkede politisamarbeid etter det såkalte Prüm-regelverket. Formålet med dette er ikke å gi politiet tilgang til nye opplysningskategorier, snarere en forbedring og effektivisering av informasjonsutvekslingen mellom Europas politimyndigheter. Samarbeidet innebærer at de nasjonale politimyndighetene kan søke direkte i hverandres databaser med opplysninger om DNA, fingeravtrykk og kjøretøy. Når det gjelder DNA og fingeravtrykk, medfører søket at man oppnår et treff eller et ikke-treff i databasen man søker i. Dette innebærer at når norske politimyndigheter søker i for eksempel Tysklands DNA-register, vil man få tilgang til referansedata i den tyske DNA-databasen, det vil si DNA-profil og et referansenummer. Disse opplysningene gjør det ikke mulig å identifisere en person, men man kan fra norsk politis side, med den informasjonen man sitter med etter søket som Prüm-regelverket tillater, bruke de kanalene for informasjonsinnhenting som er etablert ved andre EU-regelverk, og andre internasjonale avtaler om gjensidig bistand i straffesaker. Da Prüm-regelverket ble vedtatt i EU, ble det ikke ansett for å være Schengen-relevant. Regelverket ble imidlertid fra norsk side vurdert

som et nyttig verktøy i kampen mot grenseoverskridende kriminalitet, og det var et uttalt mål å knytte seg til det. Norge oppnådde dette gjennom en parallellavtale i november 2009. Avtalen ble endelig godkjent av EU 26. juli 2010, men er ennå ikke operativt i påvente av stortingsbehandling i Norge og installering av nødvendig datasystem hos Kripos.

10.7 EUs strategier, programmer og fora

10.7.1 EUs strategi for sikkerhet i det digitale rom

EU-kommisjonen og utenrikstjenesten presenterte 7. februar 2013 en samlet europeisk cybersikkerhetsstrategi: *Et åpent, sikkert og trygt digitalt rom.* Strategien berører IT-spørsmål i et bredt perspektiv og presenterer unionens visjon og prinsipper for hvordan de sentrale vurderingene og interessene skal gjennomføres og tydeliggjøres i det digitale rom. Strategien berører både interne og eksterne spørsmål om hvordan man skal ivareta Kommisjonens visjon og sentrale prinsipper i det digitale rom, og omfatter IKT-sikkerhet, IKT-kriminalitet, industri- og handelspolitikk og utenriks-, sikkerhets- og forsvarspolitikk.

Implementering og oppfølging av strategien og konklusjoner, samt spørsmål som berører EUs internasjonale cyberpolitikk, håndteres samlet i arbeidsgruppen Friends of the Presidency Group on Cyber Issues, FoP. Arbeidet tar utgangspunkt i grunnleggende verdier som menneskerettigheter, demokrati og rettsstatsprinsipper. Konklusjoner basert på strategien ble vedtatt i 2013, og i 2014 har flere områder i strategien blitt fulgt opp, som for eksempel videre arbeid med forvaltning av Internett.

10.7.2 ENISA

European Agency for Network and Information Security, ENISA, er EUs byrå for nett- og informasjonssikkerhet og ledes av en administrerende direktør. Byrået ble etablert i 2004 og er et ekspert- og kompetanseorgan for informasjonssikkerhetsspørsmål som skal legge til rette for fellesskapets og medlemsstatenes, inkludert næringslivets, evne til å forebygge, håndtere og løse problemer som gjelder nettverks- og informasjonssikkerhet. Byrået arbeid bygger på ulike tiltak som både de enkelte medlemsstatene og EU har iverksatt. ENISA gir råd til Europaparlamentet og EU-kommisjonen. Kort gjengitt er byrået arbeidsoppgaver å analysere endringer i risikobildet, først og fremst på europeisk nivå, samt å bidra til større bevissthet om nett- og informasjonssikkerhet. TF-CSIRT er et initiativ fra ENISA for økt samarbeid mellom europeiske CERT-miljøer, og er i hovedsak en arena for informasjonsutveksling. Det gjøres enkelte utredninger i mindre arbeidsgrupper. NSM NorCERT representerer Norge.

Det er et mål at ENISA skal styrke samarbeidet mellom næringsliv, forskere, leverandører og brukere av produkter og tjenester innenfor informasjonssikkerhetsområdet. Videre skal det legges til rette for samarbeid om å utvikle metoder for å forebygge og håndtere informasjonssikkerhetsproblemer, samt bidra til det internasjonale samarbeidet med tredjeland utenfor EU.

Mer detaljerte beslutninger om ENISAs løpende virksomhet tas av byrået's ledelse, som består av alle medlemsstatene og EU-Kommisjonen Beslutningene utformes som årlige arbeidsprogrammer. Norge deltar som EØS-land uten stemmerett.

ENISA deltar i mye av det arbeidet som initieres eller ledes av Kommisjonen, for eksempel i European Forum for Member States, EFMS, en uformell gruppe for medlemsstatenes nettverks- og informasjonssikkerhetsspørsmål, samt NIS-plattformen, som også kartlegger næringslivets problemstillinger innenfor dette området. I samsvar med Kommisjonens gjennomgang av digital agenda for Europa i 2012 ble behovet for en «cybersikkerhetsstrategi» tatt opp. Dette danner grunnlaget for forslaget til NIS-direktivet.

I EUs digitale agenda for Europa understrekes viktigheten av og behovet for en felles politikk for nett- og informasjonssikkerhet som tydelig skal omfatte elektronisk kommunikasjon, og ENISAs mandat ble besluttet modernisert i 2013. Norge deltar i ENISAs Artikkel 13 a-arbeidsgruppe. Gruppen møtes tre ganger i året og utgir rekommandasjoner for nett- og tjenestesikkerhet.

10.7.3 Digital agenda

EU-kommisjonens digitale agenda for Europa (KOM[2010] 245) er et av hovedinitiativene for Europa 2020 (KOM[2010] 2020), også kalt Europa 2020-strategien. Strategien ble lansert i mars 2010 som et ledd i å få Europa ut av den finansielle krisen og for å forbedre EUs økonomi for den neste tiårsperioden. Strategien beskriver blant annet hvor viktig bruk av informasjons- og kommunikasjonsteknologi er for at Europa skal kunne oppnå strategiens målsettinger.

Forslag til tiltak omfatter sju forskjellige områder:
- et pulserende digitalt indre marked
- interoperabilitet og standardisering
- tillit og sikkerhet
- rask og ultrarask Internett-tilgang
- forskning og innovasjon
- heving av digital kompetanse, digital kunnskap og digital integrasjon

10.7.4 EU-fora for personvern

10.7.4.1 Artikkel 29-gruppen

Gruppen er opprettet i henhold til EUs personverndirektiv (artikkel 29), og er den øverste rådgivende forsamlingen for EU-kommisjonen i spørsmål om personvern og informasjonssikkerhet. Her møter alle lederne for EU-landenes datatilsynsmyndigheter. Norge har observatørstatus som EØS-land, og møter med en representant for ledelsen i Datatilsynet. Artikkel 29-gruppen er først og fremst rådgivende overfor Kommisjonen, og står fritt til å tolke og konkretisere direktivets innhold. Gruppen møtes i Brussel fem–seks ganger per år og arbeider ofte med utgangspunkt i dokumenter fra uformelle arbeidsgrupper der alle medlemslandene kan være med. Uten at det foreligger noe formelt vedtak, er det i praksis akseptert at også observatørland kan tiltre disse gruppene.

10.7.4.2 Technology Subgroup

Technology Subgroup er en arbeidsgruppe som gjør saksforberedelser for Artikkel 29-gruppen. Disse forberedelsene danner grunnlag for mange av Artikkel 29-gruppens uttalelser. I og med at Datatilsynet er observatør i selve Artikkel 29-gruppen, er deltagelse i denne arbeidsgruppen viktig fordi tilsynet her deltar på lik linje med alle andre deltagere fra EU-land.

10.7.4.3 Berlin-gruppen

Dette er en gruppe som arbeider med personvern innen elektronisk kommunikasjon i utvidet forstand. I det vesentlige er det personvernmyndigheter som deltar i her. Gruppen avgir uttalelser (Working Papers) om aktuelle personvernspørsmål. I 2013 påtok Datatilsynet seg ansvar for å skrive gruppens rapport om Big Data. Rapporten ble endelig godkjent våren 2014. Det var første gang det norske Datatilsynet skrev en rapport for denne gruppen.

10.7.4.4 Schengen Coordination Group (SCG)

Gruppen er sammensatt av representanter for alle Schengen-landenes tilsynsmyndigheter og utveksler informasjon om egne saker og felles problemstillinger i praktiseringen av reglene for Schengen Informations System (SIS). Datatilsynet er tilsynsmyndighet for den norske delen av SIS, og deltar i Schengen Coordination Group. En representant fra Datatilsynet deltok i det internasjonale inspeksjonsteamet som våren 2014 førte tilsyn med Sveits' forpliktelser etter Schengen-regelverket.

10.7.4.5 Eurodac/Visumsamarbeid (VIS)

Datatilsynet har i 2014 vært representert med én deltager i møtene, som arrangeres av henholdsvis Eurodac Supervision Coordination Group og Visa Information System Supervision Coordination Group (VIS SCG) i Brussel.

Eurodac er et sentralt europeisk register over fingeravtrykk fra asylsøkere, og brukes primært i asylsaker. I det siste har imidlertid også politimessige formål blitt inkludert i Eurodac-regelverket, og Europol kan under visse vilkår få tilgang til databasen.

VIS er et tilsvarende register som inneholder opplysninger om visumsøkere, og formålet med registeret er å forbedre gjennomføringen av en felles visumpolitikk og konsulært samarbeid i Europa. Det er også et viktig mål å forenkle utvekslingen av opplysninger mellom medlemsstatene om søknader og avgjørelser om visum.

I disse gruppene møter samtlige ansvarlige datatilsynsmyndigheter etter de aktuelle forordningene for å samkjøre oppfølgingen av sine kontrolloppgaver.

10.8 IKT-arbeid i OECD

OECD ble grunnlagt i 1961 og er et samarbeidsorgan for 34 land og lokalisert i Paris. Målet med samarbeidet er å bidra til utvikling, sysselsetting og å heve levestandarden i medlemslandene. Det arbeides for å bidra til en sunn økonomisk utvikling, både i medlemslandene og i omverdenen, samt å bidra til ekspansjon i verdenshandelen.

Samarbeidet foregår ut fra et markedsøkonomisk grunnlag. OECD er et forum for utveksling av idéer og erfaringer samt foretar analyser innenfor flere politikkområder. Et viktig mål er at medlemslandene skal lære av hverandre og diskutere felles problemer og aktuelle internasjonale økono-

miske spørsmål. OECD samler inn statistikk og har en omfattende publikasjonsvirksomhet.

OECD har cirka 200 komiteer og arbeidsgrupper. Her arbeider medlemslandene, partnerland og inviterte organisasjoner sammen med OECDs sekretariat med studier, rekommandasjoner og retningslinjer til støtte for medlemslandenes policyutvikling. OECDs anbefalinger og retningslinjer er ikke juridisk bindende, men veiledende, og har gjennom dette påvirkningskraft og blir fulgt i stor grad. Sekretariatet har cirka 2 500 ansatte, og det årlige budsjettet er på cirka 350 millioner euro. Vedtak fattes med enstemmig konsensus.

OECDs virksomhet er inndelt i direktorater. Direktoratet for vitenskap, teknologi og industri (Directorate for Science Technology and Industry) har fire underkomiteer, og en av disse (Committee on Digital Economy Policy, CDEP) arbeider med den digitale økonomien. CDEP består av tre arbeidsgrupper. En av disse er arbeidsgruppen for informasjonssikkerhet og integritet (Working Party on Information Security and Privacy in the Digital Economy, WPSPDE), som ble etablert i 1992 og er den gruppen som behandler områder som spesielt angår denne utredningen.

Arbeidsgruppen forvalter og reviderer løpende flere rekommandasjoner og retningslinjer som det redegjøres nærmere for nedenfor. For tiden pågår det et arbeid med å etablere indikatorer for måling av informasjonssikkerhet, blant annet via data fra CSIRTs arbeid med ID-forvaltning, samt utvikling av «Privacy Risk Management».

Arbeidsgruppen har, sammen med helsekomitéen, ferdigstilt en rapport om sikkerhet og integritet ved gjenbruk av helseopplysninger. Tidligere arbeider har blant annet handlet om analyse av medlemsstatenes nasjonale strategier for informasjonssikkerhet, informasjonssikkerhetsspørsmål angående «Internet of Things» og Big Data, forberedelse av en rekommandasjon om beskyttelse av barn på Internett («Protection of Children Online»), analyser av nasjonale strategier om informasjonssikkerhet for kritisk infrastruktur, med mer. Arbeidsgruppen foretar også forskjellige analyser innenfor personvernområdet.

10.8.1 OECDs retningslinjer for «cybersecurity»

I 1992 utviklet OECD sine første retningslinjer for å understøtte medlemsstatenes arbeid med informasjonssikkerhetsområdet. De ble revidert i 2002 og på nytt revidert i 2015. Revisjonen fokuserte på informasjonssikkerheten i nettverk og IKT-systemer ut fra økonomiske og sosiale hensyn og velferdshensyn i et åpent, internasjonalt og tilkoblet teknisk miljø. Internett har blitt en stadig viktigere plattform for samfunnets funksjonalitet. De digitale truslene øker med mer sofistikerte aktører.

Nye former for økonomisk og sosial ustabilitet har oppstått. Økt digital mobilitet, skytjenester, sosiale nettverk, tingenes Internett (Internet of Things) med mer er nye parametre for informasjonssystemene. Ambisjonen er at de nye retningslinjene skal ivareta disse og andre utviklingstrekk med utgangspunkt i en helhetlig tilnærming. Utgangspunktet er basert på risikotenkning fordi systemer og nettverk i dag er internasjonale, større og mer komplekse. Både forebyggende tiltak og krisehåndteringsevne forutsettes. Den nye rekommandasjonen er inndelt i tre seksjoner: generelle prinsipper, operasjonelle prinsipper og nasjonale strategier. Rekommandasjonen har også et tillegg med veiledning.

De generelle prinsippene handler om å bevisstgjøre alle berørte om hvilke digitale sikkerhetsrisikoer de utsettes for, og betydningen av å sørge for utdannelse, slik at alle har kunnskap til å kunne bedømme og håndtere slike risikoer. Alle har et felles ansvar ut fra sin egen rolle eller virksomhet. Det må likevel tas i betraktning at et visst risikonivå må aksepteres i et åpent og sammenvevd internasjonalt miljø. Det anbefales å innføre et styringssystem for risikohåndtering («risk management») for å oppnå en felles styring av sikkerhetsarbeidet som er transparent og i samsvar med menneskerettighetene og øvrige grunnleggende verdier. Et globalt Internett krever at alle aktører må samarbeide internasjonalt, på tvers av landegrenser.

De operasjonelle prinsippene handler om systematiske risiko- og sårbarhetsanalyser og håndtering av disse. Risikohåndtering kan resultere i at risiko aksepteres, reduseres, unngås eller kombinasjoner av de forskjellige alternativene. Videre handler den andre seksjonen om sikkerhetstiltak, innovasjon og kontinuitetsplanlegging.

I den tredje seksjonen anbefaler OECD at medlemsstatene utarbeider nasjonale strategier. Hensikten er å redusere digital sikkerhetsrisiko på alle nivåer, innenlands og på tvers av landegrenser, uten unødvendige restriksjoner som påvirker den frie informasjonsutvekslingen eller teknologiutviklingen. Også individene skal beskyttes mot digitale sikkerhetstrusler som for eksempel datainnbrudd, identitetstyveri og øko-

nomisk bedrageri. Statene må også sørge for nasjonal sikkerhet og suverenitet og sikre at menneskerettigheter og grunnleggende verdier blir ivaretatt. Strategiene skal rettes mot alle aktører og tilpasses så vel små og mellomstore virksomheter som individer.

Det anbefales også tiltak som bør gjennomføres på regjeringsnivå. Eksempler på denne typen tiltak er blant annet å utarbeide en helhetlig handlingsplan for den offentlige forvaltningen basert på risiko- og sårbarhetsanalyser, forbedre koordineringen mellom relevante myndigheter, opprette CSIRT, høyne informasjonssikkerhetskravene i offentlige anskaffelser, ansette flere sikkerhetseksperter, stimulere FoU og innovasjon, samt utvikle åpne standarder.

Behovet for internasjonalt samarbeid og assistanse understrekes.

Å delta i internasjonale fora, etablere bilaterale og multilaterale nettverk for utveksling av erfaringer og en best mulig tilpasset teknologi er veien å gå. Internasjonalt samarbeid for å kunne møte og håndtere grenseoverskridende trusler kan for eksempel skje via samarbeid mellom CSIRT og gjennom internasjonal øvingsvirksomhet.

Opparbeiding av tillit i samarbeid mellom aktører tar tid. Informasjonen som det oppfordres til å utveksle, kan i mange tilfeller være sensitiv eller hemmelig og påføre skade hvis den havner hos uvedkommende. Partnerskap og ulike former for samarbeid mellom offentlige og private aktører, formelt eller uformelt, kan stimuleres med det mål å skape arenaer for tillitsfull utveksling av kunnskap og erfaringer.

Andre tiltak som regjeringene kan benytte for å stimulere den digitale sikkerheten, er å støtte frivillige merkeordninger, oppmuntre til sertifisering og rapportere hendelser. Statistikk på området trenger også utvikling gjennom planlegging av nye og internasjonalt sammenlignbare indikatorer.

10.8.2 OECDs retningslinjer for personvern

Beskyttelse av personopplysninger ved overføring og datalagring er et område OECD har arbeidet med i over 35 år. De første retningslinjene ble lansert i 1980. Ulovlig lagring av personopplysninger, oppbevaring av uaktuelle opplysninger og utlevering av sensitive opplysninger er de temaene som behandles i retningslinjene.

Personopplysninger må kunne behandles innenfor viktige sektorer som økonomi, helse og for forskningsformål, samt av myndighetene. Gjenbruk av data er et annet område. Retningslinjene ble utarbeidet for å unngå forskjeller i lovreguleringen mellom landene og med et mål om blant annet å legge til rette for fri utveksling over landegrensene.

Åtte forskjellige prinsipper ble lagt til grunn med rammer og krav knyttet til mengden innsamlede personopplysninger, datakvalitet, formålet med å behandle dataene, behandlingen, det vil si håndtering og bruk, sikkerhet, åpenhet om bruken, individets rettigheter, samt det å definere hvem som har ansvaret for databehandlingen. Disse prinsippene ligger til grunn også for dagens personvern, og er blitt utviklet ytterligere i en revidert versjon som ble fullført i 2013. To tillegg ble innført med de nye retningslinjene. Det ene tillegget gjelder behovet for å innføre et risikobasert styringssystem for å beskytte personopplysninger, det andre er å øke den globale interoperabiliteten for området gjennom internasjonale regelverk.

Nye konsepter er også introdusert, herunder behovet for å utarbeide nasjonale strategier for håndtering av persondata, behovet for å utarbeide et program for ledere av virksomheter, samt krav til hendelsesrapportering ved datalekkasje. Virksomheters ansvar for håndtering av personopplysninger løftes spesielt frem.

10.9 FNs arbeid i fora knyttet til det digitale rom

FNs generalforsamlings første komité

Denne komiteen er tilegnet nedrustning og internasjonal sikkerhet og behandler cybersikkerhet ut fra et internasjonalt sikkerhetsperspektiv. En resolusjon fremmet av Russland har blant annet vært førende siden 1998 og satte utviklingen av informasjons- og telekommunikasjonsteknologier inn i en internasjonal sikkerhetskontekst. Resolusjonen tar blant annet opp risiko og trusler i forbindelse med bruk av teknologiene og behovet for å vedta mulige samarbeidstiltak for å håndtere utviklingen, herunder tiltak i form av normer og tillitsbygging. Resolusjonen, som så langt er vedtatt med konsensus, har gitt mandat til etableringen av en ekspertgruppe for IKT relatert til internasjonal sikkerhet, United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE). Slike grupper er blitt oppnevnt fire ganger, og to av gangene er det oppnådd konsensus om rapporter med gruppens anbefalinger. Spesielt er UNGGE-rapporten som ble antatt i 2013, blitt viet

betydelig oppmerksomhet, ettersom den konstaterte at folkerettens prinsipper for maktanvendelse også gjelder i det digitale rom.

Den fjerde UNGGE-gruppen, med et utvidet antall medlemmer fra 15 til 20 eksperter, ble nedsatt i fjor og leverte sin sluttrapport i forkant av FNs generalforsamling i 2015. Russland, Kina, Tadsjikistan, Usbekistan, Kasakhstan og Kirgisistan fremmet i januar 2015 et forslag til adferdskoder («Code of Conduct») til FNs generalforsamling. Flere vestlige land har møtt dette forslaget med skepsis fordi det ikke anses akseptabelt i et menneskerettighets- og ytringsfrihetsperspektiv. Diskusjonen om cyberspørsmål som et sikkerhetsanliggende innenfor FN har tydeliggjort betydningen av et bredere sikkerhetsperspektiv som også løfter frem menneskerettighetene og betydningen av hvordan Internett forvaltes globalt, der særlig flerpartsmodellen (samarbeid mellom offentlige og private aktører) er tillagt betydning.

En UNGGE rapport fra 22. juli 2015 oppfordrer statene til økt samarbeid og utveksling av informasjon, og hjelp til å straffeforfølge terror og kriminell bruk av IKT. Videre statueres det at statene ikke bør skade informasjonssystemene til de autoriserte responsmiljøene i en annen stat eller bruke disse responsmiljøene til å engasjere seg i ondsinnet internasjonal aktivitet.

FNs generalforsamlings andre komité

FNs generalforsamlings andre komité behandler generelle økonomiske og sosiale spørsmål inkludert utviklings- og bistandsspørsmål. IKT vektlegges som et viktig virkemiddel for økonomisk og sosial utvikling på verdensbasis. Et høynivåmøte som skal holdes i 2015, skal vurdere dette innenfor rammen av World Summit on the Information Society (WSIS).

I FN-kontekst har det eksistert en viktig konflikt omkring WSIS-prosessen, en utviklingsprosess som startet med to toppmøter, i Genève i 2003 og i Tunis i 2005. Den opprinnelige bærende ideen om å styrke FNs arbeid for å forbedre tilgangen til IKT i lav- og middelinntektsland, endte med skarpe motsetninger om kontrollen over Internetts sentrale tekniske ressurser, standarder med mer. Spørsmålet gjaldt om Internett skulle styres i en flerpartsmodell eller ved opprettelse av et nytt FN-organ.

En kompromissløsning førte til etableringen av en åpen, global møteplass i FNs regi – «Internet Governance Forum» – samt et løfte om i løpet av de nærmeste ti årene å etablere «enhanced cooperation», en formulering uten tydelig definisjon som gjorde at Tunisagendaen kunne vedtas. Ti år etter toppmøtet i Tunis er utredningsprosessen avsluttet – der ITU, Den internasjonale teleunionen, og Unesco har spilt en fremtredende rolle. Internet Governance Forum (IGF), er en global arena for dialog mellom myndigheter og private aktører om Internett-utvikling og utfordringer knyttet til styringen av Internett, herunder sårbarhet, sikkerhet og stabilitet for infrastruktur. I tillegg diskuteres folkerettslige problemstillinger knyttet til ytringsfrihet og personvern i det digitale rom. Norske myndigheter deltar aktivt i dialogen i IGF med representasjon fra Nkom, Samferdselsdepartementet og Utenriksdepartementet. Et høynivåmøte innenfor rammen av WSIS-prosessen skal holdes i New York i desember 2015.

FNs generalforsamlings tredje komité

Den tredje komiteen behandler menneskerettighetsspørsmål. Vestlige land og Norge legger til grunn at menneskerettighetene gjelder i det digitale rom på lik linje med samfunnet for øvrig. Diskusjonen om balansen mellom sikkerhet og frihet og mellom privatliv og overvåking er krevende. Brasil og Tyskland fremmet en resolusjon om overvåking og privatliv i 2013 som Norge sluttet seg til. FN har avgitt to resolusjoner om retten til et privatliv i den digitale tidsalder. Resolusjonene er ikke rettslig bindende, men anses for å reflektere visse minstestandarder.

FNs råd for menneskerettigheter

I FNs råd for menneskerettigheter i Genève 2012 ble det vedtatt en resolusjon med konsensus som for første gang bekrefter at de samme rettighetene som finnes offline, også gjelder online. En oppfølgingsresolusjon ble vedtatt i 2014, der også spørsmål om retten til utdanning og styringsspørsmål ble tatt opp. Høykommissærens rapport *The right to privacy in the digital age* ble diskutert i et panel i september og presentert i UNGAs tredje avdeling i oktober. Debatten tok blant annet opp menneskerettighetenes ekstraterritorielle anvendelse.

OSSE

Fra 1993 har OSSE vært en regional organisasjon i FN. Den 3. desember 2013 besluttet medlemsstatene i Organisasjonen for sikkerhet og samarbeid i Europa (OSSE) å vedta en første etablering av til-

litsskapende tiltak innenfor cybersikkerhetsområdet. Målet med tiltakene er å fremme samarbeid, åpenhet, forutsigbarhet og stabilitet for å begrense risikoen for misforståelser og eskalering av konflikter i det digitale rom. I beslutningen understrekes det at iverksetting av tiltakene skal være i samsvar med internasjonal rett og især FNs konvensjon om sivile og politiske rettigheter. Ifølge overenskomsten påtar de deltagende statene seg frivillig å rapportere om nasjonale og transnasjonale trusler som gjelder IKT. I tillegg kan statene på frivillig basis bistå med konsultasjoner for å redusere risiko for misforståelser, konflikt og politisk spenning.

Sårbarheter i det digitale rom er en global utfordring. Det eksisterer ingen internasjonale avtaler som regulerer hvordan nasjonalstatene skal håndtere globale sikkerhetsutfordringer. Den internasjonale debatten rundt sårbarhet, sikkerhet og stabilitet for Internett skjer i stor grad i fora som ikke etablerer rettslige forpliktelser mellom statene. For at norske myndigheter skal kunne være informert og påvirke utviklingen innen sårbarhet, sikkerhet og stabilitet for Internett, er det essensielt at norske myndigheter er representert og deltar i debatten på den internasjonale arenaen.

10.10 NATO

Cyberforsvar er en del av NATOs kjerneoppgave om kollektivt forsvar, som bekreftes av deklarasjonen fra toppmøtet i Wales i 2014. NATO beslutter i det enkelte tilfelle om et cyberangrep mot en medlemsstat skal utløse de gjensidige forsvarsforpliktelsene i artikkel 5. NATOs strategiforslag som ble vedtatt på toppmøtet i Lisboa i 2010, understreker betydningen av at NATO har fokus på cyberforsvarsområdet.

Cooperative Cyber Defence Centre of Exellence (CCD-COE)

Det NATO-akkrediterte cyberforsvarssenteret ble opprettet i Tallinn i Estland for å øke kunnskapen om trusselbilder innenfor cybersikkerhetsområdet. I 2013 presenterte en ekspertgruppe som var tilknyttet senteret, forskjellige perspektiver på hvordan folkeretten kan få anvendelse innenfor cyberområdet. Arbeidet er publisert i rapporten *Manual on the International Law Applicable to Cyber Warfare*, også kalt Tallinmanualen.

NATO Computer Incident Response Capability (NCIRC)

Organisasjonen som har som oppgave å beskytte NATOs egne nettverk. NSM NorCERT mottar rapporter fra NCIRC og deler informasjon via NATO MISP (Malware Information Sharing Platform) som de drifter. NSM NorCERT har også direktekontakt i relevante hendelseshåndteringssaker.

10.11 Interpol

I september 2014 ble Interpol Global Complex for Innovation (IGCI) etablert i Singapore. Dette skal fungere som et forsknings- og utviklingssentrum. Innenfor IGCI ligger Interpols Digital Crime Centre, som skal øke informasjonssikkerheten og bekjempe IKT-relatert kriminalitet. Senteret har et kriminalteknisk laboratorium som støtter etterforskning av IKT-kriminalitet. Her foregår også forsknings- og utviklingsaktiviteter som å teste protokoller, verktøy og tjenester og å utvikle praktiske løsninger i samarbeid med politiet, akademia og øvrig offentlig og privat sektor. Senteret utarbeider i tillegg trendanalyser om IKT-angrep. De tre viktigste initiativene overfor medlemsstatene er harmonisering, å bygge kapasitet, samt gi operativ og kriminalteknisk støtte.

10.12 Andre multilaterale samarbeidsfora

ICANN

Allokering av IP-adresser, domenenavnsystemer (DNS) og toppdomener utgjør tre sentrale funksjoner for sikker og stabil bruk av Internett. Dette håndteres i dag av The Internet Corporation for Assigned Names and Numbers (ICANN), en privat stiftelse i California. Arbeidet er basert på en kontrakt med amerikanske myndigheter.

Norske myndigheter kan gi innspill til ICANN gjennom et myndighetsforum (Government Advisory Committee), men i realiteten har offentlige myndigheter utenfor USA begrenset påvirkning på ICANNs beslutninger. Stabilitet og funksjonalitet for de nasjonale toppdomenene, som «.no», er av stor betydning. Det er så opp til de enkelte lands myndigheter å beslutte nasjonal regulering og iverksette sikkerhetstiltak for nasjonal infrastruktur. Det foregår stor grad av europeisk koordinering i regi av EU-kommisjonen når det gjelder arbeidet innen ICANN.

European Government CERT (EGC)

Dette er et uformelt nettverk av myndighets-CERT-er i Europa. Oppgaver det samarbeides om, er blant annet informasjonsutveksling knyttet til skadevare og sårbarheter og utvikling av tiltak for å håndtere hendelser. EGC er en operativ gruppe med teknisk fokus, og de fastsetter ikke policyer. NSM NorCERT representerer Norge.

Nordic CERT Consortium (NCC)

Dette er en samarbeidsarena for de nordiske nasjonale CERT-organisasjonene. Det blir jevnlig holdt møter, og det er etablert et gradert samband mellom landene. Landene samarbeider også om felles øvelser og kurs.

European Network of Forensic Science Institute (ENFSI)

ENFSI har etablert en gruppe, Forensic Information Technology, som arrangerer årlige møter. Deltagelsen gir Norge tilgang til ressurspersoner og et bredt kontaktnett innen det tekniske fagfeltet og til erfaringer og metoder fra Europa. Gruppen er også en inngangsport til tilsvarende tekniske grupper i Asia og USA.

FIRST (global Forum for Incident Response and Security Teams)

Dette er et forum med over 300 medlemmer globalt, og er et samarbeid mellom en rekke responsmiljøer fra myndigheter, private virksomheter og akademia. Formålet er samarbeid og koordinering for å forebygge hendelser, sikre hurtig respons på hendelser og promotere informasjonsdeling mellom medlemmene og samfunnet for øvrig.

ILETS

Dette er et internasjonalt samarbeid om kommunikasjonskontroll og utnyttelse av elektroniske spor over landegrenser hvor juridiske og teknologiske utfordringer blir diskutert. USA, Australia, Canada, Frankrike, Tyskland, Italia og England deltar aktivt med representanter fra departementer og politiorganisasjoner som har ansvar for politi- og sikkerhetstjenester.

Hardware Forensics

Dette er en liten, eksklusiv internasjonal ekspertgruppe som består av teknologer (ikke politi) med spisskompetanse som møtes for å diskutere metodeutvikling i faget Hardware Forensics, som metoder innen dypsikring av mobiltelefoner, GPS-er, knekking av passordbelagte harddisker/minnepinner, analyse av bilelektronikk, og lignende. Dette er det viktigste forumet Kripos benytter for kompetanseheving og tilgang på verdensledende teknikker innen fagfeltet.

International Watch and Warning Network (IWNN)

Dette er en internasjonal samarbeidsarena som diskuterer trusler, sårbarheter og angrep på Internett. Hensikten er å etablere en felles situasjonsforståelse og evne til å håndtere hendelser. NSM NorCERT representerer Norge.

Den internasjonale personvernkonferansen

Denne internasjonale arenaen samler verdens personvernmyndigheter med et mål om konsensus om overordnede prinsipper og retninger for personvernarbeidet. Det blir utført komité- og gruppearbeid mellom konferansene.

Det norske Datatilsynet, med støtte fra en rekke andre personvernmyndigheter, fremmet utkast til en resolusjon om hvordan personvernmyndighetene bør forholde seg til Big Data. Resolusjonen ble vedtatt. Også resolusjonen *Privacy in the Digital Age* er vedtatt. Dette er en støtteerklæring til FNs pågående arbeid med oppfølging av myndighetenes masseovervåking på tvers av landegrenser.

Global Privacy Enforcement Network, GPEN

GPEN er et samarbeidsforum for personvernmyndigheter. Datatilsynet deltok på et møte i forumet i sammenheng med den internasjonale personvernkonferansen, og deltar i telefonkonferanser gjennom året. GPEN legger til rette for informasjonsutveksling, og det planlegges koordinerte aktiviteter. Det pågår en oppgradering av samhandlingsløsningen for GPEN-medlemmene, og Datatilsynet har bidratt økonomisk ved etableringen av denne. «Internet Sweep Day» er en GPEN-koordinert aktivitet. Sist ble ivaretakelse av personvernet i mobilapper undersøkt.

Del III
Sårbarheter i kritiske samfunnsfunksjoner

Kapittel 11
Elektronisk kommunikasjon

Samhandling og utveksling av informasjon foregår i stadig større grad gjennom elektronisk kommunikasjon. Internett blir brukt til e-post, publisering og innhenting av informasjon og til interaktive e-tjenester som e-forvaltning, e-handel og nettbank. IKT-systemer og nettverk danner basis for prosesstyring og overvåking av installasjoner på norsk kontinentalsokkel, av kraftverk, vannverk og etter hvert de fleste deler av industrien.

Ekom er en innsatsfaktor i all vare- og tjenesteproduksjon og økonomisk virksomhet. Helsevesen, betalingstjenester, stat, kommune og ordensmakt er avhengige av at den elektroniske kommunikasjonen fungerer. Innovasjon og utvikling av nye tjenester som er basert på støtte fra telekommunikasjon, gjør denne avhengigheten enda sterkere.

De verdiene og funksjonene som ekomnett og -tjenester leverer, er en helt sentral forutsetning for at andre samfunnsfunksjoner skal kunne levere det de skal. Samtidig er det en stadig økende forventning i samfunnet om at ekom som innsatsfaktor er stabil og tilgjengelig. 100 prosent oppetid tas mer eller mindre for gitt, og det er meget lav aksept for brudd.

Privatpersoner og organisasjoner har fått sin portal til offentlige myndigheter gjennom norge.no. Så viktig er Internett blitt at også sosialt samkvem i stor grad nå skjer via sosiale medier og online-spill. Mange norske bedrifter bekrefter at noen få dager uten Internett vil være katastrofalt for virksomheten.[1]

Samfunn og næringsliv er i stor grad avhengige av ekom også i krisesituasjoner. Erfaringene fra hendelser der ekom har sviktet, viser at kritiske samfunnsfunksjoner som kriseledelse, nød- og redningstjeneste er avhengige av ekomtjenester som en innsatsfaktor for å ivareta befolkningens behov. Også Forsvaret er avhengig av sivil ekom i samvirket med totalforsvaret og i forbindelse med logistikkstøtte og drift.

11.1 Ekominfrastruktur

Ekom er en forkortelse for «elektronisk kommunikasjon» og defineres i lov om elektronisk kommunikasjon, ekomloven, som «kommunikasjon ved bruk av system for signaltransport som muliggjør overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signaler i fritt rom eller kabel der radioutstyr, svitsjer, annet koplings- og dirigeringsutstyr, tilhørende utstyr eller funksjoner inngår».

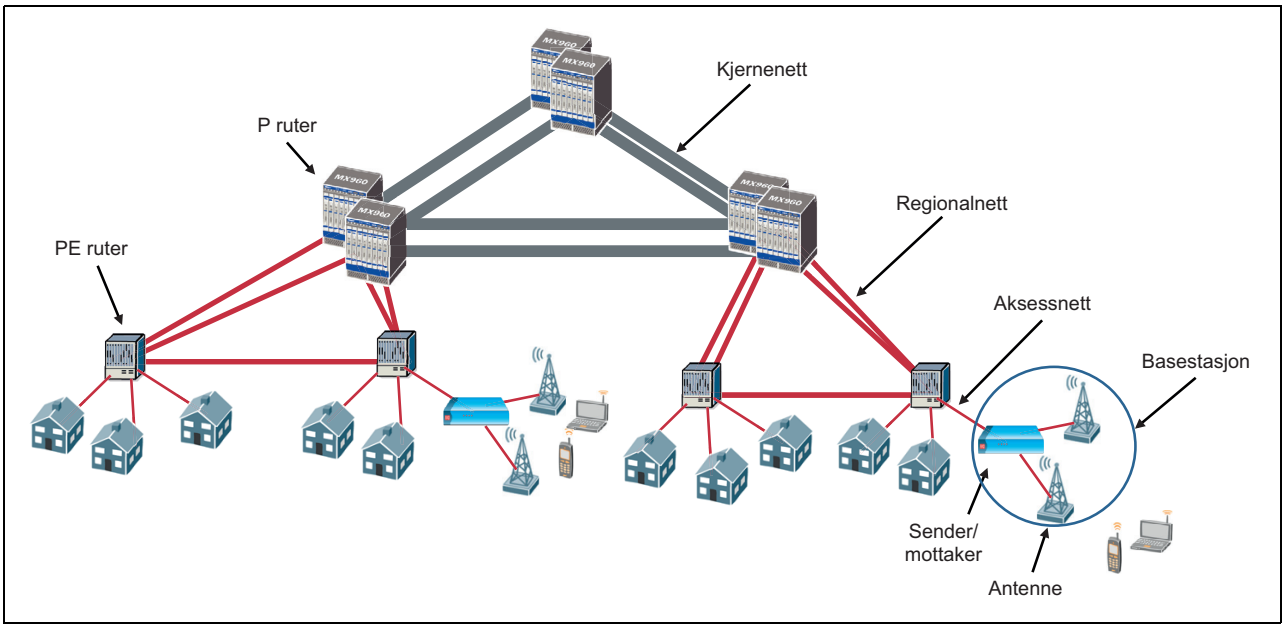
Ekomtjenester er tjenester som formidler signaler i ekomnett, for eksempel TV, taletjenester eller Internett. Som brukere forholder vi oss oftest til taletjenester og ulike distribuerte dataprogrammer som krever kommunikasjon for å fungere. Eksempler på det siste kan være alt fra enkle applikasjoner på mobilen til systemer som kontrollerer kritiske produksjonsprosesser for industrien. Ekomtjenestene må ha en infrastruktur av nettverk og nettverkskomponenter for å fungere.

På Internett kommuniserer alle tilknyttede enheter ved hjelp av en felles protokoll – IP (Internet Protocol). Andre store nettverk (for eksempel de tradisjonelle telenettene) har benyttet andre protokoller, men vi ser at stadig flere systemer migrerer mot IP. Selv om IP er standardisert, er det en kontinuerlig utvikling av utstyret som kobles på Internett, og utskifting av komponenter i selve nettet for å tilfredsstille krav til stabilitet, sikkerhet, kapasitet og effektivitet.

De grunnleggende elementene som til sammen utgjør ekominfrastrukturen, er kjernenett, regionalnett, aksessnett, tjenestenett og drifts- og støttesystemer. Dette er illustrert i figur 11.1.

Selv om vi beskriver ekomnettet i entall, eksisterer det i virkeligheten flere mer eller mindre uavhengige ekomnett. Disse er igjen i større eller

[1] Næringslivets sikkerhetsråd (2014): *Mørketallsundersøkelsen 2014 – Informasjonssikkerhet, personvern og datakriminalitet.*



Figur 11.1 Ekominfrastruktur.

Kilde: Oslo Economics.

mindre grad integrert med hverandre. De ulike nettene vil i varierende grad inneholde alle elementene i figur 11.1.

Figuren illustrerer forbindelsen mellom brukeren og ekomtjenesten. Kjernenettet løser trafikkbehovet mellom større byer og regioner, regionalnettet løser trafikkbehovet innad i større byer og regioner, mens aksessnettet knytter utstyret hos brukeren til regionalnettet. Kjernenettet har nødvendigvis større kapasitet enn regionalnettet og aksessnettet. De ulike begrepene blir brukt ulikt innenfor sektoren, men utvalget har valgt følgende definisjoner i denne rapporten:

Kjernenettet[2] er den landsdekkende «motorveien» for tele- og datakommunikasjon. Kjernenettet består av overføringssystemer med stor kapasitet, fiberkabel og i noen tilfeller radiolinje. Kjernenettet knytter sammen regionalnettene og er forbindelsen mellom de store byene eller knutepunktene.

Regionalnettene[3] er «riksveiene» for tele- og datakommunikasjon. Regionalnettene knytter aksessnettet og kjernenettet sammen gjennom flere sentraler som samler opp trafikk fra aksessnettene. Regionalnettene dekker en region – for eksempel et fylke eller en stor by.

Transportnettet er en kombinasjon av kjernenett og regionalnett.

Aksessnettene knytter forbindelse mellom den enkelte sluttbrukeren og transport- og tjenestenettene. De faste aksessnettene kan være fiber, koaks eller kobber, og sender trafikk mellom sluttbrukeren og nærmeste sentral i regionalnettet. Mobilnettene er en type aksessnett med trådløs forbindelse mellom basestasjoner og brukernes mobiltelefoner. Den enkelte basestasjonen dekker et lite geografisk område, og hver basestasjon er knyttet til den faste delen av ekomnettet med en fast linje eller en radiolinje. Basestasjoner består grovt sett av to elementer: antenner som sender og mottar signalene, og et skap med utstyr som behandler signalene.

For at en tilbyder av mobilnett skal kunne dekke hele landet, kreves det et aksessnett med flere tusen basestasjoner.

Tjenestenett er ikke selvstendige fysiske overføringsnett, men kan benytte ulike typer infrastruktur som også brukes til andre typer tjenester. Disse benytter det samme transportnettet for å formidle informasjon mellom et antall tjenesteoder. Fasttelefonnettet og mobiltelefonnettene er eksempler på tjenestenett. Tjenestenettene består av diverse systemer og utstyr som er nødvendig for å levere de ulike tjenestene.

Transmisjon er den tjenesten som leveres av kjernenett og regionalnett i fellesskap. Et landsdekkende sett av basestasjoner trenger derfor transmisjon for å kunne levere mobiltelefoni.

Drifts- og støttesystemene er IKT-systemer som overvåker og styrer ekomnett og tjenestenett. Drifts- og støttesystemene er en kritisk del av

[2] Kjernenettet kalles i noen sammenhenger transportnettet.
[3] Regionalnettene kalles i noen sammenhenger metronett.

infrastrukturen og er ofte felles for flere funksjoner i nettet. Det er en tendens at funksjonene sentraliseres og styres ved hjelp av elektronisk kommunikasjon. Mange av komponentene er derfor avhengige av at nettene fungerer, for å kunne fungere normalt.

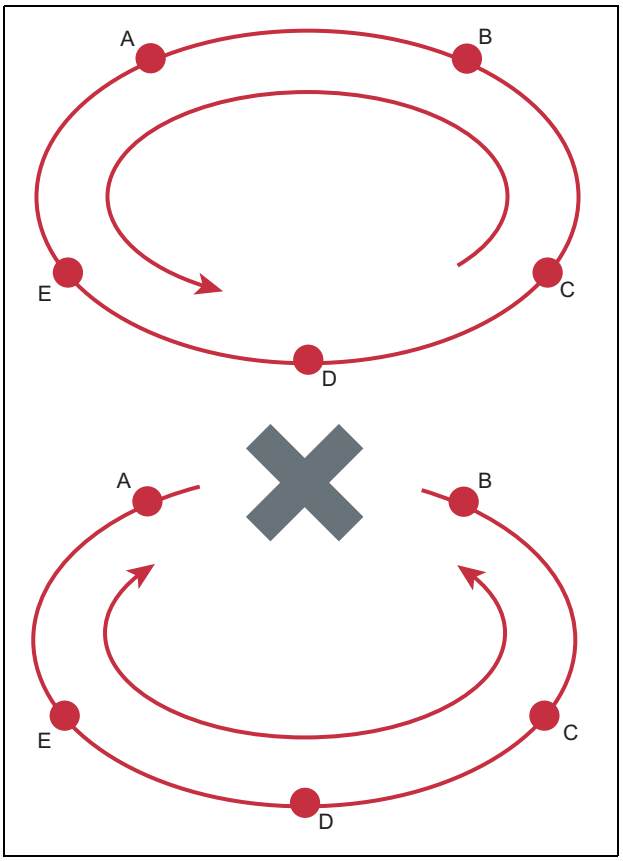
En *node* er i IKT-sammenheng betegnelsen på en enhet i et nettverk. Det kan være for eksempel en ruter, en server eller en svitsj.

En *svitsj* er et apparat som mottar signaler fra en rekke inngående linjer og sender dem videre etter bestemte regler. Klassisk telefoni er et typisk eksempel på et nettverk som er avhengig av svitsjer. Her brukes svitsjer for å koble en midlertidig krets mellom samtalepartnere (linjesvitsjing). I datakommunikasjon deles strømmen av digitale data opp i pakker med avgrenset lengde, som alle inneholder informasjon om opphavet og hvor de skal (pakkesvitsjing). Svitsjer i telefonnettet kalles vanligvis telefonsentraler.

11.1.1 Robusthet i infrastrukturen

Når man snakker om robusthet i ekomnettene, er det særlig to begreper som er sentrale: redundans og fremføringsdiversitet. *Redundans* oppnås ved å ha flere maskiner eller strukturer som kan levere samme tjeneste, i noen tilfeller også ved å ha maskiner på flere lokasjoner. Maskinene kan opereres uavhengig av hverandre og overtar for hverandre dersom det skulle oppstå svikt i én av dem. Dette reduserer faren for utfall av nettet ved tekniske feil eller elektroniske eller fysiske angrep på nettverksutstyr i en node. *Fremføringsdiversitet* er en form for redundans (et «sub-set» av redundans), Med fremføringsdiversitet menes fysisk adskilte føringsveier for infrastrukturen. Dette reduserer faren for utfall av nettet ved naturhendelser, graveskader eller fysiske angrep på infrastrukturen. Fremføringsdiversitet kan enten oppnås gjennom parallelle føringsveier eller gjennom ringstruktur i infrastrukturen. Ringstrukturens funksjon er illustrert i figur 11.2. Kommunikasjonen mellom sentralene A–E går normalt én vei i en ringstruktur i kjernenettet. Ved brudd i ringen kan trafikken legges om slik at den samme kapasiteten benyttes, men nå i begge retninger.

Brudd i kjernenett eller systemfeil i en sentral ruter kan få store konsekvenser for store deler av befolkningen. Brudd i aksessnett eller feil i en CE-ruter vil bare få lokale konsekvenser for et begrenset antall sluttbrukere. Ettersom trafikkonsentrasjonen er størst i denne delen av infrastrukturen, er kjernenettet bygd med høy grad av robusthet, og det er samtidig dimensjonert med



Figur 11.2 Ringstrukturens funksjon.

Kilde: DSB.

høy kapasitet. Robustheten avtar når man beveger seg ut i regionalnettet og aksessnettet mot sluttbrukerne.

11.1.2 Kjerne- og transportnett

Det finnes flere virksomheter i Norge som eier fiberinfrastruktur, men det er kun Telenor og Broadnet som har landsdekkende transportnett på land. Begge disse nettene utgjør en kritisk infrastruktur i ekomsektoren, siden all type trafikk som telefoni, mobiltelefoni, bredbånd, nødnettsamband, fjernsyn og så videre går via disse nettene. En del av infrastrukturen til Telenor og Broadnet er fremført i felles traseer. Dette kan være en faktor som svekker robustheten i nettet.

I kjernenettet til Telenor er redundansen ivaretatt ved at det er to parallelle, fysisk og logisk adskilte nett, samt at deler av nettet har ringstruktur. Ringstrukturen gir en ekstra grad av redundans og robusthet. Dersom ringen brytes, vil trafikken kunne rutes motsatt vei. I tillegg finnes det delvis et reservenett som tas i bruk ved utfall av det ordinære nettet. I regionalnettet er redundansen i infrastrukturen også ivaretatt ved hjelp av ringstrukturer. Foruten redundansen i føringsvei-

ene er kritiske nettverkselementer som rutere/svitsjer duplisert for å øke robustheten i tilfelle feil i maskinvarer. I tillegg er noder (sentraler med rutere/svitsjer/servere) i nettet utstyrt med reservestrømløsninger, enten batteri eller nødstrømsaggregat, for å kunne sikre fortsatt drift ved utfall i strømnettet.

Altibox har etablert sitt eget høykapasitetsnett over langtidsleie av mørk fiber, som så langt dekker 17 av 19 fylker. Mye av infrastrukturen er leid av egne partnere i Altibox. Altibox knytter sammen nettene sine uten å gå via Telenor, men tilbyr foreløpig ikke operatør-transmisjons produkter utover standard lag 2 og 3 bedriftsprodukter. Partnerkonseptet til Altibox innebærer at det bygges fibernett i en rekke regioner hvor lokal partner har ansvar for utbygging og installasjon, i hovedsak lokale elektrisitetsverk. Altibox leverer komplette forretnings- og operasjonelle støttesystemer, teknologisk nettverksdesign og bredbåndsprodukter til partnerne.

Det finnes også et landsdekkende transportnett som benyttes til kringkasting. Nettet eies og drives av Norkring, som er et heleid datterselskap av Telenor. Tradisjonelt har fjernsyns- og radiosignaler utelukkende vært distribuert over kringkastingsnettet, men i dag suppleres dette i økende grad med digital overføring gjennom ekomnettene.

11.1.3 Aksessnett

Et aksessnett knytter sluttbrukeren til transmisjons- og transportnettet og derigjennom til tjenestetilbyderne. Det finnes flere forskjellige typer aksessnett, både faste og trådløse. Gjennom aksessnettet kan en sluttbruker få tilgang til ulike tjenester som telefoni, fjernsyn, radio og Internett.

For faste aksessnett finnes det kobberledninger, koaksialkabler og optisk fiber. Optisk fiber til bruk for aksessnett er i større grad blitt utbygd de senere årene, særlig i tettbebygde og urbane strøk. Dette nettet har betydelig større båndbredde enn aksessnett basert på kobberledninger og koaksialkabler.

Det er planer om å fase ut det linjesvitsjede PSTN-systemet[4], slik at verken analog fasttelefoni eller digital ISDN-telefoni[5] vil være tilgjengelig om noen år. Årsaken til den planlagte utfasingen er redusert etterspørsel etter tjenester basert på PSTN/ISDN-teknologien og at mobiltelefoni og VoIP[6] (telefoni over IP-nettverk) i økende grad har tatt over markedsandeler. En annen viktig årsak er manglende tilgang på reservedeler, support og teknisk personell.

11.1.4 Mobilnett

Trådløse nett er systemer som bruker radiosignaler til kommunikasjon i aksessnettet. Mobilnettene, som er eksempler på trådløse aksessnett, tilbyr mobiltelefoni- og dataoverføringstjenester. Telenor og TeliaSonera (Netcom) er de største aktørene på dette området. Per i dag er GSM (2. generasjon mobilnett) fullt utbygd og har dekning så godt som alle steder der folk bor. UMTS (3. generasjon mobilnett) er også utbygd, men har lavere dekningsgrad enn GSM-nettet. LTE (4. generasjons mobilnett) er fortsatt under utbygging. Foruten å tilby mobiltelefonitjenester blir mobilnettet i dag i økende grad brukt til overføring av datatrafikk. ICE er på vei inn i dette mobiltelefonimarkedet som en tredje aktør. De vil i løpet av 2015 starte utbyggingen av et rent LTE-basert mobilnett.

11.1.5 Satellittkommunikasjon

Satellittbasert kommunikasjon er med sine særskilte egenskaper et svært viktig element i den totale ekominfrastrukturen, spesielt for et land som Norge med tilhørende topografi, geografisk utstrekning og ressursforvaltningsinteresser fra Antarktis til Arktis. Se kapittel 12 «Satellittbaserte tjenester».

11.1.6 Kommunikasjonsinfrastruktur på norsk sokkel

Satellittkommunikasjon var opprinnelig eneste kommunikasjonsmåte offshore og er fortsatt viktig for oljevirksomheten. Ikke minst er den viktig som reserveløsning for å skape redundans. I dag fremstår Tampnet og MCP (Maritime Communications Partner) som viktige infrastrukturleverandører. Kabelutbyggingen er drevet frem av det behovet olje- og gassoperatørene har for stadig mer datakapasitet.

Tampnets infrastruktur leverer høyhastighets båndbredde til offshore olje- og gassinstallasjoner på norsk og britisk side av Nordsjøen. Deres infrastruktur tilbyr raskeste vei ut av Norge til Europa, uten å gå via Sverige. Infrastrukturen består av undersjøiske fiberkabler, radiolinjer og LTE 4G og

[4] Public Switched Telephone Network.
[5] Integrated Services Digital Network.
[6] Voice Over IP.

har fire landingspunkter i Norge og to i Storbritannia. Nettverket er lukket, og det er ikke direkte koblet til Internett.

MCP (Maritime Communications Partner) er en fullverdig mobiloperatør, i motsetning til Tampnet, som til nå har vært aktør med fiberbaserte datatjenester. MCP opererer på alle sju hav, og har båter med sin løsning over hele verden. I 2013 hadde MCP 20 millioner unike brukere i nettet. Tampnet vil tilby mobilaktører å roame i sitt nettverk i Nordsjøen, noe som betyr at flere mobilaktører vil tilby sine tjenester i Nordsjøen, og ikke bare MCP.

11.1.7 Nødnett

Nødnett er det nye digitale radiosambandet for nød- og beredskapsetater. Det er basert på TETRA-standarden og opererer ved 380–400 MHz. Dette frekvensområdet er reservert for nødsamband i hele Europa. Nødnett er primært et talesamband for gruppekommunikasjon, og muliggjør blant annet kryptert kommunikasjon på tvers av nødetater. Ved siden av talekommunikasjon er det mulighet for utveksling av tekstmeldinger (SDS) og dataoverføring med begrenset hastighet. Ved bruk av TEDS-funksjonalitet i TETRA, som tilsvarer GPRS/EDGE i GSM, kan dataoverføringer gjennomføres med realistisk hastighet opp mot cirka 80 kbit/s. Det pågår for tiden uttesting av TEDS. På lengre sikt vil det kanskje være mulig å integrere TETRA og LTE, noe som vil gi en langt bedre dataoverføringshastighet enn dagens løsninger. Digitalt nødnett kjøper transmisjon og transport fra tredjeparter.

Figur 11.3 viser ringstrukturen som nødnettet er bygd med, og som bidrar til en ekstra redundans. Nødnettet skal etter planen være ferdig utbygd innen utgangen av 2015.

11.1.8 Internett

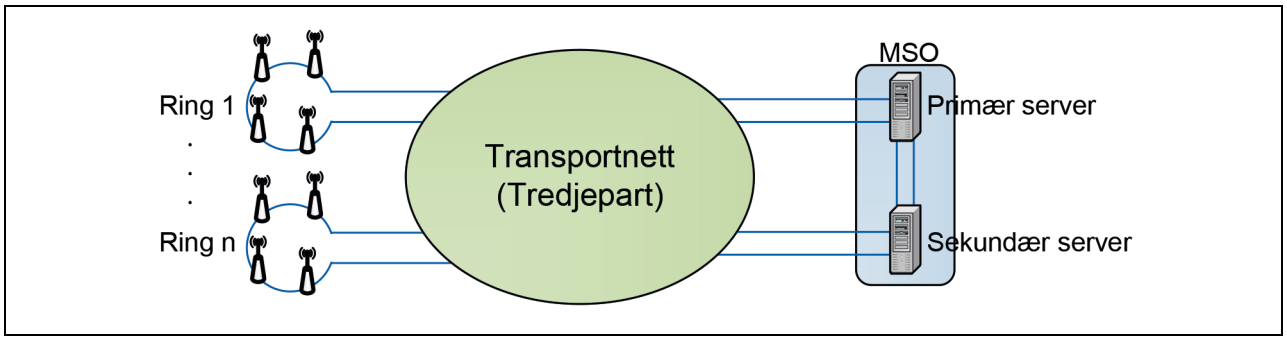
Forløperen til Internett var et forskningsnett som ble kalt ARPANET og opprinnelig var et militært nettverk. Protokoller for utveksling av filer ble utviklet, og med protokollen IP ble det mulig å koble sammen nettverk. I 1972 ble Norge koblet til ARPANET. Norge var dermed det første landet utenom USA som kom til å bruke ARPANET.[7]

Standarder og protokoller utviklet over tid gjorde at geografisk spredte nett vokste frem til det vi i dag kjenner som Internett, et nettverk av nettverk som går på tvers av landegrenser og nasjonale ekominfrastrukturer – uten noen overordnet styring. I dag finnes det tjenester for utveksling av informasjon, informasjonssøk, nedlasting og opplasting av data, og sammenstilling og analyse av informasjon. Datamaskiner kommuniserer med hverandre over Internett, og algoritmer (matematiske regler) bestemmer reaksjonsmønsteret.

Utviklingen har gjort det mulig for globale aktører å utvikle skytjenester der store serverparker kan levere tjenester og prosessorkapasitet til det globale markedet på tvers av nasjonale grenser (se punkt 23.7 «Utkontraktering og skytjenester»). Om vi ser tilbake, er skyen egentlig en videreføring av opprinnelsen til Internett, der ressurstilgang og økonomi la grunnlaget for sammenkobling av datamaskiner. Ringen er dermed på en måte sluttet, og en ny utviklingsspiral trer frem med innovasjon av innholdstjenester basert på Internettet.

Det tidligere tjenesteskillet mellom tale, tekst, bilde og data er i ferd med å forsvinne helt. Alle tjenestene leveres etter hvert på samme vis (over IP) og tilbys som en applikasjon på mobiltelefo-

[7] Bing, J.: «Building cyberspace: a brief history of Internet». In: *Internet Governance, Infrastructure and Institutions.* Eds: Bygrave, L.A. and Bing. J., Oxford University Press: 8–47.



Figur 11.3 Digitalt nødnett.

Kilde: DNK.

nen, nettbrettet, PC-en og så videre. Tjenestene kombineres på helt nye måter, og det blir vanskelig å skille dem fra hverandre. Mange av tjenestene blir i økende grad også tilbudt fra globale innholdsleverandører som Google, YouTube og Facebook. Valgmulighetene blir flere, og det blir enklere for sluttbrukerne å kommunisere på flere måter. Kommunikasjonsform vil i større grad avhenge av kontekst og hensikt, uten at brukerne må gjøre veldig bevisste valg.[8]

11.2 Roller og ansvar

Samferdselsdepartementet (SD) har det overordnede ansvaret for ekomsektoren. SD er nærmere omtalt i kapittel 8 «Organisering av roller og ansvar».

Nasjonal kommunikasjonsmyndighet (Nkom) er underlagt SD og har ansvar for å forvalte ekomloven og føre tilsyn med ekomtilbydere. Nkom har videre ansvar for koordinering og rapportering ved uønskede hendelser som rammer ekomnett eller -tjenester for markedsregulering av tilbydere og frekvensforvaltning. Nkom arbeider også med forebyggende IKT-sikkerhet gjennom nettstedet nettvett.no.

Direktoratet for nødkommunikasjon (DNK) har ansvaret for utbyggingen av et digitalt nødnett i Norge. Direktoratet ble opprettet 1. april 2007 og er underlagt Justis- og beredskapsdepartementet.

Utenriksdepartementet (UD) har en viktig rolle i forbindelse med internasjonale arenaer der blant annet Internetts styring og fremtid blir drøftet.

Sivilt–militært samarbeid

Forsvarets kommunikasjonsinfrastruktur (FKI) er et landsdekkende nett med kommunikasjonstjenester. Den underliggende infrastrukturen som dette bygges på er imidlertid under endring og er delvis eid av private aktører. Dette nettet dekker Forsvarets behov for teletjenester internt i Forsvaret og til noen viktige sivile beredskapsaktører, men for omfattende sivilt–militært samhandling er Forsvaret også avhengig av sivile ekomtjenester. FKI har totalt om lag 50 000 brukere. Forsvaret har tidligere drøftet spørsmålet om å sette bort og selge deler av FKI til andre offentlige etater eller til private selskaper. I anledning effektivisering og modernisering av FKI er det spørsmål om enkelte radiolinjestasjoner, som også støtter sivile behov i dag, fortsatt skal driftes selv om Forsvaret ikke lenger trenger dem i den moderniserte militære infrastrukturen. Fra sivil side er det en bekymring at Forsvaret bygger ned denne infrastrukturen, fordi sivile basestasjoner og utstyr kan være montert på samme radiolinjetårn.

Internasjonalt samarbeid

Innenfor EØS-området er reguleringen av ekommarkedene relativt lik. Krav til sikkerhet og beredskap er imidlertid et nasjonalt anliggende. Norsk regulering på feltet vil i europeisk sammenheng lettest kunne sammenlignes med øvrige nordiske og i en viss grad nordeuropeiske land, der graden av digitalisering er høy og den samfunnsmessige avhengigheten stor. Dette reflekteres generelt i strengere krav til sikkerhet og beredskap. Ellers er aktørbildet innenfor EØS-området kjennetegnet av samme status med en bredspektret blanding av store aktører, gjerne, men ikke nødvendigvis, tidligere monopolister, og en lang rekke mindre og mellomstore utfordrere.

Styring av Internett og Norges påvirkningsmulighet

Internet Assigned Numbers Authority (IANA) er ansvarlig for global koordinering av rotservere for domenenavn, IP-adressering og andre protokollressurser, og er organisert under The Internet Corporation for Assigned Names and Numbers (ICANN). ICANN er en global privat flerinteressentorganisasjon som styrer forvaltningen av de globale Internett-ressursene. Amerikanske myndigheter har et kontraktsforhold med ICANN, men vurderer å avslutte kontrakten for utførelse av IANA-funksjonene. ICANN fasiliterer derfor en prosess der verdenssamfunnet kommer sammen og utarbeider forslag til en ny styringsmodell. Norge ved Nkom deltar i arbeidsgruppen. I tillegg deltar blant annet representanter for .com, .shop og lignende domener. USA har stilt en del betingelser for løsningen man skal komme frem til: Løsningen skal blant annet støtte og forsterke flerinteressentperspektivet, man skal beholde sikkerhet, robusthet og stabilitet i domenenavnsystemet, og man skal imøtekomme krav til åpenhet, forventninger og behov hos de globale kundene.

International Telecommunication Union (ITU) ligger i Sveits og er FNs globale spesialorgan for telekommunikasjon med 193 medlemsland. Norge har vært med helt fra starten. ITU er delt i tre byråer, som arbeider med henholdsvis radio, standardisering og utvikling. ITU er viktig blant

[8] Post- og teletilsynet (2014): *Ekomtjenester, -nett og -utstyr. Utvikling og betydning for PT.*

annet for frekvensforvaltning. Hvert fjerde år holder ITU en fullmaktskonferanse, den nittende ble avholdt i 2014. Fra Norge deltok representanter fra Samferdselsdepartementet, Utenriksdepartementet, Nasjonal kommunikasjonsmyndighet, Telenor og Norid.

Forvaltningen og styringen av Internett debatteres internasjonalt, og diskusjonen er blitt intensivert og aktualisert de siste to–tre årene. Det internasjonale samfunnet har en stor utfordring når det gjelder å enes om prinsipper og veien videre for utvikling og styring av det fremtidige Internettet. Nkom deltar aktivt internasjonalt som forvalter av Internett-ressurser og tilsynsmyndighet for infrastruktur for elektronisk kommunikasjon, for å fremme norske interesser. Sikkerhet og stabilitet for Internett globalt inngår i Nkoms forvaltningsansvar gjennom å være norsk representant i Governmental Advisory Committee (GAC) i ICANN. Nkom er ansvarlig for å ivareta nasjonale interesser innen effektiv ressursforvaltning av Internett-ressurser som domenenavn og IP-adresser, som også innebærer å være pådriver sammen med andre lands myndigheter og andre private interessenter for ivareta sikkerhet og stabilitet for domenenavnsystemet.

Med hjemmel i ekomloven og domeneforskriften § 9 har Nkom tilsynsansvar for Uninett Norid AS (Norid). Norid har ansvar for drift av vår nasjonale del av domenenavnsystemet, landkode-toppdomenet .no. Nkom har vedvarende dialog med Norid vedrørende utvikling og forvaltning av nasjonale domenenavnresurser.

11.3 Hjemmelsgrunnlag og tilsynsvirksomhet

Lov om elektronisk kommunikasjon (ekomloven)[9] regulerer kommersielle ekomtilbydere i Norge, og er grunnlaget for reguleringen av den nasjonale kommunikasjonsinfrastrukturen. Samferdselsdepartementet er sammen med Nkom myndighet etter ekomloven. Nkom har ansvar for tilsyn når det gjelder lovens virkeområde både på fastlandet og på norsk sokkel. Nkom fører tilsyn med tilbydere av elektroniske kommunikasjonsnett og -tjenester (ekomtilbydere), domeneinfrastruktur og utstedere av kvalifiserte sertifikater for esignatur.

Formålet med loven er å sikre brukerne i hele landet gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester gjennom effektiv bruk av samfunnets ressurser ved å legge til rette for bærekraftig konkurranse og stimulere til næringsutvikling og innovasjon.

Loven gjelder virksomhet knyttet til elektronisk kommunikasjon og tilhørende utstyr. Forvaltning og bruk av det elektromagnetiske frekvensspekteret og nummer, navn og adresser er omfattet. Det samme gjelder all utstråling av elektromagnetiske bølger fra elektronisk kommunikasjon og all utilsiktet utstråling av elektromagnetiske bølger som kan forstyrre elektronisk kommunikasjon. Loven gjelder også for norske skip og luftfartøy og for anlegg og innretninger av enhver art som har tilknytning til petroleumsvirksomhet på kontinentalsokkelen, og for utnyttelse av fornybare energiressurser til havs innenfor havenergilovens virkeområde.

Nkom har flere tilsynsområder som følges opp mot forskjellige aktører i ekommarkedet. I tillegg til markedstilsynsrollen kan vi nevne teknisk tilsyn med markedet for radio- og teleterminalutstyr, i tillegg til frekvensbruk, bygging og drifting av nett og i sterkt økende grad forhold knyttet direkte til sikkerhet og beredskap i nett.

NSM fører også tilsyn etter sikkerhetsloven og objektsikkerhetsforskriften. Det direkte tilsynsansvaret med objekter i ekominfrastruktur som er utpekt som skjermingsverdige etter objektsikkerhetsforskriften, ligger hos Nkom.

Sikkerhet og beredskap

Ekomloven § 2-10 gir nærmere bestemmelser om sikkerhet og krav til beredskap. Første ledd inneholder de overordnede kravene, og her angir ordlyden «forsvarlig sikkerhet» den normen som tilbyderne til enhver tid skal oppfylle. Tilbyderne skal selv dekke kostnadene knyttet til å oppfylle krav i dette leddet.

I henhold til andre ledd kan myndigheten treffe enkeltvedtak eller inngå avtale om at tilbyderen skal gjennomføre tiltak for å sikre oppfyllelse av nasjonale behov for sikkerhet, beredskap og funksjonalitet i elektronisk kommunikasjonsnett og -tjeneste utover det som følger av første ledd. Tilbyderens merkostnader ved levering av slike tiltak skal kompenseres av staten.

Nkom kan, som tilsynsmyndighet, utføre tilsyn og pålegge tilbyderne å sette i verk tiltak for å sikre at kravene som er nevnt ovenfor, blir ivaretatt. Tilbyderne kan nektes tilgang til markedet dersom det er nødvendig av hensyn til offentlig sikkerhet, helse eller andre særlige forhold.

[9] *Lov om elektronisk kommunikasjon (ekomloven)*, Samferdselsdepartementet 01.10.2015.

I tillegg er det innført en klassifiseringsordning for nettutstyr i henhold til klassifiseringsforskriften[10] som har til hensikt å sikre nettutstyr i anlegg mot uønsket ytre fysisk påvirkning. Sentralt i klassifiseringsforskriften er bestemmelsen som krever at tilbydere av ekomnett gjennomfører en helhetlig risiko- og sårbarhetsvurdering knyttet til anleggene sine og sørger for at anlegg i de ulike klassene er forsvarlig sikret i samsvar med denne vurderingen.

Basert på både øvelser, hendelser og egne ROS-analyser gjennomfører Nkom i økende grad tilsyn med forhold knyttet til oppfølging av krav til sikkerhet og beredskap. De siste to årene har det vært gjennomført varslet stedlig tilsyn med de to største tilbyderne knyttet til hele spekteret av relevant regelverk. I tillegg har det vært gjennomført særskilte dokumentbaserte tilsyn med de sju største tilbyderne knyttet til varslingsplikten.[11] Avvik og mangler følges opp gjennom vedtak og rapportering.

Kommunikasjonsvern

Etter ekomloven § 2-7 har en tilbyder plikt til å gjennomføre nødvendige sikkerhetstiltak til vern av kommunikasjon i egne elektroniske kommunikasjonsnett og -tjenester. Trafikkdata skal slettes eller anonymiseres så snart de ikke lenger er nødvendige for kommunikasjons- eller faktureringsformål, med mindre noe annet er bestemt i eller i medhold av lov. Annen behandling av trafikkdata krever samtykke fra brukeren.

Taushetsplikt

Etter ekomloven § 2-9 har en tilbyder plikt til å bevare taushet om innholdet av og andres bruk av elektronisk kommunikasjon, herunder opplysninger om tekniske innretninger og fremgangsmåter. Tilbyderen plikter å gjennomføre tiltak for å hindre at andre enn de som opplysningene gjelder, får anledning til selv å skaffe seg kjennskap til slike opplysninger. Opplysningene kan heller ikke benyttes i egen virksomhet eller i tjeneste eller arbeid for andre, med unntak av statistiske opplysninger om nettrafikk som er anonymisert, og som ikke gir informasjon om innretninger eller tekniske løsninger.

Taushetsplikt gjelder også for alle som utfører arbeid eller tjenester for tilbydere av elektroniske kommunikasjonsnett eller -tjenester, installatører, tekniske kontrollorganer eller myndighetene, også etter at vedkommende har avsluttet arbeidet eller tjenesten.

I ekomforskriften er det gitt ytterligere regler for sikkerhet og beredskap, kommunikasjonsvern og taushetsplikt. Enkelte av disse er videre presisert innenfor konteksten av logiske angrep.[12]

Utstyr

Nkoms markedskontroll sjekker at utstyr oppfyller grunnleggende krav til sikkerhet, elektromagnetisk kompatibilitet og bruk av radiospektrum, samt særskilte funksjonelle krav. I enkelte tilfeller testes også utstyrets funksjonalitet.

Nkom velger ut utstyret som skal underlegges markedskontroll, basert på en vurdering av risiko og vesentlighet, etter klage fra brukere eller som en del av felles markedskontrollkampanjer i EU.

Frekvenskontrollen

Nkoms frekvenskontroll utfører planlagt tilsynsarbeid og behandler en rekke henvendelser fra publikum, brukere og operatører av elektronisk kommunikasjon og kringkasting. For å sikre at systemer og utstyr kan funksjonere etter formålet, fører Nkom tilsyn med at tildelte frekvenser er fri for interferens og forstyrrelser, og at det blir brukt i samsvar med tillatelser.

Frekvenskontrollen arbeider typisk med måling av elektromagnetiske felt, håndtering av interferens mellom tjenester, lokalisering av elektromagnetiske forstyrrelser og identifisering av problemer med brukerutstyr.

Kontroll med installasjoner

Nkom fører årlig tilsyn med cirka 50 nett når det gjelder dokumentasjon, elektrisk sikkerhet, teknisk utførelse og kvalitet, samt bruk av autorisert virksomhet for bygging og vedlikehold av installasjon.

---

[10] Nasjonal kommunikasjonsmyndighet (2013): *Forskrift om klassifisering og sikring av anlegg i elektroniske kommunikasjonsnett (klassifiseringsforskriften)*.

[11] «Tilbyder skal varsle Post- og teletilsynet om hendelser som vesentlig kan redusere eller har redusert tilgjengeligheten til elektroniske kommunikasjonstjenester» Ekomforskriften § 8-4.

[12] *Ekomlovens krav vedrørende kommunikasjonsvern, integritet og tilgjengelighet – logiske angrep*. Presiseringsnotat fra Post- og teletilsynet til ekomtilbydere 2.4.2013.

Tilsyn med utstedere av kvalifiserte sertifikater for esignatur

Nkom har tilsynsansvar med utstedere av kvalifiserte sertifikater etter esignaturloven. Bruk av kvalifiserte sertifikater er grunnleggende for å kunne utvikle tillitsbaserte tjenester som blant annet understøtter regjeringens digitale agenda.

11.4 Beredskap og hendelseshåndtering

Hver enkelt privat virksomhet har et eget ansvar og en egeninteresse ut fra kommersielle hensyn til å sørge for tilstrekkelig beredskap. I dette ligger for eksempel det å ha evne til å håndtere angrep som kommer fra Internett. Ekomoperatørene som driver infrastrukturen i Norge, har egne sikkerhetsavdelinger som driver med både forebyggende sikkerhet og hendelseshåndtering. Telenor har sitt eget sikkerhetsovervåkingssenter som driftes 24/7/365.

Tilbyderne har plikt til å varsle Nkom ved ekomutfall. Viktigheten av varsling øker etter hvert som samfunnet blir stadig mer avhengig av elektroniske kommunikasjonstjenester. Informasjon om utfall er viktig for koordinering med og videre varsling til myndighetsorganer med beredskapsansvar for andre sektorer. Nkom har under utvikling en tjeneste for bransjen som skal gi en samlet oversikt over nettutfall (Nettutfall.no).

I 2014 var det 18 hendelser der alvorlighetsgraden krevde ekstra oppmerksomhet eller økt beredskap i Nkom. Varsling fra tilbyderne blir fortløpende vurdert, og Nkom utarbeider en situasjonsrapport når hendelsen blir vurdert som alvorlig. Situasjonsrapportene sendes SD og deles rutinemessig med DSB, NVE og berørte fylkesmenn.

Nkom har etablert beredskapsvakt som en fast ordning 24/7/365. Flere fylkesmenn har etter øvelser eller reelle hendelser påpekt at det er nødvendig med bedre representasjon av ekomsektoren i fylkesberedskapsrådet. Nkom samhandler med fylkesmennene gjennom fylkesberedskapssjefene, og kan selv bistå fylkesberedskapsrådene der det er hensiktsmessig. Nkoms bidrag til fylkesberedskapsrådene kommer i tillegg til Telenors og eventuelt andres deltagelse. Nkom har ved flere tilfeller i 2014 etablert kriseledelse.

Ekomsektoren har et eget beredskapsforum der bransjen møter myndighetene. Slike fora kan bidra til at kriser løses raskere enn dersom private ikke inkluderes i et beredskapssamarbeid med myndighetene. Dette samarbeidet kommer inn under totalforsvaret.

Tilbyderne har som oppgave å tilby elektronisk kommunikasjon til brukerne, uten å måtte ta stilling til hva kommunikasjonen brukes til, og hva slags informasjon som formidles. I et slikt perspektiv kan ekomnettene være innsatsfaktor for kriminelle handlinger i cyberdomenet. Samtidig er ekomnettene svært potente mål i seg selv, enten hensikten er spionasje eller det er å ramme kritiske samfunnsfunksjoner, for eksempel under en sikkerhetspolitisk krise eller i en krigssituasjon.

Ekomsektoren har i dag ikke et felles senter for håndtering av tilsiktede digitale hendelser. Kapasitet for deteksjon og hendelseshåndtering er lokalisert i de enkelte selskapenes egne sikkerhetssentre. Telenor har for øvrig sin egen Telenor Security Operations Centre (TSOC) som overvåker trafikken og sikkerheten i tillegg til en egen CERT-funksjon. Andre teletilbydere har egne operasjonssentre. I tråd med føringene i Nasjonal strategi for informasjonssikkerhet har Nkom fra sommeren 2015 startet oppbyggingen av et eget hendelseshåndteringsmiljø for digitale hendelser, Nkom CSIRT. Denne funksjonen skal videreutvikles i dialog med øvrige myndighetsaktører, sektorvise responsmiljøer og bransjen.

I beredskapssituasjoner kan Forsvaret bidra med enkelte ressurser for å avhjelpe en prekær situasjon. Forsvaret har for eksempel mobile løsninger for kommunikasjon og transportberedskap som har vært benyttet i sivile kriser. Det er Cyberforsvaret som i så fall bidrar via bistandsinstruksen til politiet. Cyberforsvaret samarbeider også med aktører i ekomsektoren i forbindelse med øvelser og læring om hendelseshåndtering og sikkerhet. Cyberforsvaret har imidlertid presisert at deres viktigste rolle er å drifte egen infrastruktur, og at enhver bistand til det sivile samfunnet vil måtte gå på bekostning av den egne militære beredskapen.

11.4.1 Øvelsesfunn

Alle aktører og virksomheter med ansvar for kritiske samfunnsfunksjoner og som er avhengige av fungerende ekomnett og -tjenester, har et eget ansvar for å gjennomføre øvelser på området. I henhold til retningslinjer for departementene og underliggende etater i alle sektorer skal det gjennomføres nødvendig øvelsesaktivitet. Det samme gjelder det regionale og lokale nivået. Ekomforskriften stiller krav til tilbydere om å utarbeide beredskapsplaner og delta i øvelser.

Nkom gjennomfører øvelser i håndtering av IKT-hendelser, både internt i Nkom, innad i sekto-

ren og på tvers av sektorer. Blant annet har Nkom gjennomført en større øvelsesserie sammen med NVE og Vegvesenet i perioden 2008–2013, med vekt på samhandling ved skade på kritisk infrastruktur som følge av ekstremvær. Nkom har startet planleggingen av en nasjonal cyberøvelse i desember 2015 for infrastruktureiere og myndighetene. Samarbeidet med NVE videreføres med cyberøvelsen i 2015. DSB planlegger også en cyberøvelse i 2016, der Nkom vil delta aktivt i planleggingen sammen med DSB.

Det gjennomføres årlig større nasjonale tverrsektorielle øvelser i regi av DSB som har som mål å øve på samordning. Få av disse øvelsene har hatt digitale sårbarheter som hovedtema, men under Øvelse IKT i 2008, Øvelse Orkan i 2012 og Øvelse Østlandet i 2013 ble IKT-hendelser øvd. Hovedfunn i DSBs evalueringer fra disse øvelsene viser at det generelt er manglende egenberedskap hos aktørene (uavhengig av sektor) når det gjelder utfall av digital infrastruktur. Man mangler alternative kommunikasjonsløsninger, det er mangel på kompetanse i bruk av teknisk utstyr, og nødstrøm er en klart begrensende faktor.

Det kreves av hver sektor og hver virksomhet at de skal øve på krisehåndtering og at de tar initiativ til øvelser der det øves på tverrsektorielle avhengigheter. Etter en gjennomgang av øvelsesvirksomhet det siste året er det grunn til å tro at det øves for lite, både på samordning og koordinering på tvers av etater og virksomheter, inkludert private aktører, og på IKT-håndtering av IKT-hendelser i hver enkelt virksomhet. Manglende øvelser kan blant annet bidra til å forsterke uklare rolle- og ansvarsforhold i hendelseshåndtering.

11.5 Sårbarheter i ekominfrastruktur

Hendelser som forårsaker svikt i telekommunikasjon, kan ha mange ulike årsaker. En skiller gjerne mellom tilsiktede og utilsiktede hendelser.

Grovt sett vil truslene mot ekomnettet kunne oppsummeres i tabell 11.1.

Nkom har siden 2010 fulgt opp nær 40 hendelser som kan kategoriseres som alvorlige. De hyppigst forekommende årsakene til disse hendelsene fordeler seg grovt sett slik:

- 35 prosent skyldtes programvarefeil.
- 25 prosent skyldtes fiberbrudd/transmisjonsfeil.
- 20 prosent skyldtes strømbrudd.
- 15 prosent skyldtes feil ved planlagt arbeid (oppgradering).

Siden Nkom bare håndterer de mest alvorlige hendelsene, vil ikke denne feilårsakfordelingen nødvendigvis samsvare med fordelingen av årsaker til feil hos den enkelte tilbyder. For eksempel kan det være en stor andel strømbrudd som bare har lokale konsekvenser, og som Nkom dermed ikke har regnet med. Nkom bemerker på generell basis at det forebyggende arbeidet med sikkerhet og beredskap i nettet har blitt bedre og høyere prioritert i perioden 2010–2015.

11.5.1 Verdikjeder i ekom

Ekomverdikjeden strekker seg fra transport- og transmisjonsnett, via aksessnett til tale- og datatjenester. På toppen av datatjenestene er såkalte Over The Top-tjenester, som gjerne tilbys av aktører som ikke tradisjonelt er regnet som en del av ekombransjen, og som derfor kan være utenfor direkte regulatorisk kontroll. Noen få aktører tilbyr hele verdikjeden opp til tjenestene tale og data. Den mest sentrale er Telenor, den opprinnelige nasjonale teleoperatøren i Norge. Broadnet har et tilnærmet landsdekkende transportnett som i stor grad følger jernbanelinjene. Altibox, som består av en sammenslutning av flere kraftselskaper, er også en totalleverandør med egen infrastruktur. Aktørene handler med hverandre, de leier fiber av hverandre, og kabler legges i samme grøft. Derfor kan en også oppleve svikt

Tabell 11.1 Trusler og farer mot ekomnettet

	Logiske feil	Fysiske feil
Tilsiktede hendelser	– Elektroniske angrep på nettelementer, drifts- og støttesystemer	– Fysiske angrep på infrastruktur
Utilsiktede hendelser	– Tekniske feil – Menneskelig svikt – Overbelastning – Strømbrudd	– Tekniske feil – Naturhendelser (ras, storm, is, flom mv.) – Graveskader

hos flere leverandører for eksempel når kabler blir gravd over ved et uhell.

Aktører som bygger ut aksessnett-infrastruktur, benytter i hovedsak Telenors eller Broadnets kjerne- og regionalnett for transport.

Dette leder frem til noen grunnleggende digitale sårbarheter når det gjelder ekominfrastruktur i Norge:

Felles sambandsinfrastruktur

Telenors kjernenett utgjør ryggraden i infrastrukturen og er et kritisk element ettersom svært mye av trafikken går gjennom dette nettet. Ved utfall av dette nettet vil vesentlige deler av ekom på nasjonalt nivå falle bort. Til sammenligning vil et tilsvarende utfall i et aksessnett bare få lokale konsekvenser for et begrenset antall sluttbrukere. Ettersom trafikkonsentrasjonen er størst i denne delen av infrastrukturen, er transportnettet bygd med høy grad av robusthet og samtidig dimensjonert med høy kapasitet. Det meste av infrastrukturen i kjernenettet er basert på optisk fiber. I noen tilfeller brukes også radiolinje og satellittsamband.

Robustheten avtar når man beveger seg utover mot aksessnettet og sluttbrukerne. Robustheten i infrastrukturen styrkes typisk ved å bygge inn redundans i føringsveier/nettverkselementer og ved å ha reservestrømberedskap i tilfelle utfall.

De ulike tilbyderne av ekomtjenester benytter i stor utstrekning Telenors kjernenett, som også er bærer av IP-infrastruktur. Det betyr at de sårbarhetene som denne infrastrukturen har, er felles for mange tilbydere. Kabler ligger flere steder i felles grøfter, og antenner er i mange tilfeller montert på de samme antennetårnene. Brudd i sentrale sambandsfremføringer og svikt i IP-baserte infrastrukturer kan dermed gi store utfall av ekomtjenester.[13]

Infrastruktursårbarheten har også en geografisk komponent. Infrastrukturen er generelt mindre utbygd og robust i distriktene enn i sentrale, tett befolkede strøk av landet. Det er enkelt forklart et mindre marked og derfor behov for færre basestasjoner for å dekke det daglige behovet. Dessuten har utfall med høy kundekonsentrasjon større konsekvenser enn utfall der færre kunder rammes. Dette er en type begrensninger som kan være en utfordring med tanke på nasjonens evne til å håndtere kriser og forsvare seg mot en rekke trusler. Erfaringer som ble gjort under Dagmar og brannen i Lærdal, viser hvor hardt ekomutfall kan ramme krisehåndteringen.

Sentraliserte nettfunksjoner

Tjenestene i ekomnettene har liten grad av lokal autonomi, men er avhengige av sentraliserte funksjoner. De er implementert på noe ulikt vis hos de ulike tilbyderne. Sentraliserte funksjoner er trolig den mest kosteffektive måten å produsere tjenestene på, og operatøren har mulighet til å bygge mye robusthet inn i løsningene. Hendelser som har relativt lav sannsynlighet, kan imidlertid få svært store konsekvenser dersom disse sentraliserte funksjonene rammes. Eksempler på slike funksjoner er viktige svitsjer/rutere, registre over abonnenter, telefonnumre og simkort, telenett management, overvåkings- og sikkerhetsstyring med mer.[14] Eksempler på sårbarheter som finnes spesifikt i sentraliserte funksjoner, er logiske trusler og programvarefeil. Skadepotensialet og konsekvensene ved feil kan i mange tilfeller øke uforholdsmessig, og kanskje uakseptabelt, om kritiske enkeltkomponenter kommer fra samme leverandør.

Akkumulert sårbarhet

Sårbarheter i ekomnettene akkumuleres gjennom at kabler fra flere leverandører blir lagt i samme grøft, og ved at utstyr monteres på felles mobilmaster eller telesentraler. Sårbarheter akkumuleres og kamufleres gjennom kjøp og salg av tjenester og infrastrukturleie mellom ulike aktører. Omruting av trafikk på grunn av feil eller oppgraderinger gjør også at sårbarhetsbildet er å anse som dynamisk. Dette gjør at det er vanskelig for en aktør å vite om det som fremstår som en redundant løsning, faktisk er det.

Teleoperatøren som leverer tjenestene, har ansvaret for sikkerheten i sine tjenester. Men det er en umulig oppgave å gardere seg helt mot slike sårbarheter, blant annet på grunn av mangel på transparens i systemer som i så sterk grad avhenger av programvare og har så komplekse og lange verdikjeder.

11.5.2 Samfunnets avhengighet av ekominfrastruktur

DSB har vurdert i hvilken grad kritiske samfunnsfunksjoner vil påvirkes av et bortfall av ekomnettet.[15]

[13] Hentet fra blant annet *Sårbarhetsanalyse av mobilnettene i Norge* 2012, Post- og teletilsynet.

[14] Ibid.

Scenarioet som ligger til grunn for vurderingene i DSBs rapport, er at sentrale noder i det landsdekkende transportnettet for ekom blir angrepet, slik at transportnettet settes ut av drift i en femdagersperiode. Dette er et ekstremtilfelle og kan anses som et worst case scenario, men gir et godt bilde av samfunnets avhengighet av elektronisk kommunikasjon.

I tabell 11.2 har vi gjengitt DSBs vurdering av konsekvensene ved bortfall av ekom for de ulike samfunnsfunksjonene som er analysert.

Bortfall av ekomtjenester påvirker mange kritiske samfunnsfunksjoner. Av de ni analyserte samfunnsfunksjonene er transportsektoren, helsesektoren og finanssektoren vurdert å bli sterkest påvirket av ekombortfallet. Et fåtall virksomheter som har egen mørk fiber, vil imidlertid fortsette å fungere når transportnettet ligger nede. Dette inkluderer blant annet Forsvaret, kraftverkene, T-banen i Oslo og helseforetakene i Helse Sør-Øst.

[15] Direktoratet for samfunnssikkerhet og beredskap (2014): *Risikoanalyse av cyberangrep mot ekom-infrastruktur.* Delrapport til Nasjonalt risikobilde 2014.

DSB har vurdert og gjort beregninger av samfunnskonsekvenser av bortfall av ekomnettet med utgangspunkt i scenarioanalysen.

Tabell 11.3 gjengir vurderingene som er gjort av DSB i rapporten.

Det er videre gjort en vurdering av hvilke kostnader de ovennevnte samfunnskonsekvensene vil ha. DSB antar at nettotapet vil overstige 10 milliarder kroner[16] for de fem dagene landet i henhold til scenarioet er uten ekomnett. Det er beregnet at ekomtilbydernes inntektstap vil utgjøre mellom 3 milliarder og 5 milliarder kroner basert på normal omsetning i en femdagersperiode. Med utgangspunkt i disse beregningene vil det påløpe tap på om lag 2 milliarder kroner for hver dag man er uten ekomnett. Dette innebærer at selv relativt

[16] DSB har med utgangspunkt i bruttonasjonalproduktet (BNP) for 2013, som var på om lag 3 000 milliarder kroner, beregnet at samlet produksjon i Norge i løpet av fem dager beløper seg til ca. 40 milliarder kroner. Det er videre antatt at om lag 1/3 av normalproduksjonen (ca. 13 milliarder kroner) vil gå tapt som følge av ekombortfallet. Selv om noe av omsetningssvikten kan innarbeides, antar det at nettotapet vil overstige 10 milliarder for de fem dagene landet i henhold til scenariet er uten ekomnett.

Tabell 11.2 Samfunnsfunksjoners avhengighet av ekomtjenester

Samfunnsfunksjon	Grad av påvirkning ved bortfall av ekom	Forklaring
Kraftforsyningen	*Liten*	Kraftforsyningen påvirkes i liten grad, manglende feilretting ved strømbrudd.
Veitrafikken	*Moderat*	Manglende overvåking av tunneler, ingen varsling fra trafikanter ved hendelser, moderate forsinkelser.
Jernbanetrafikken	*Stor*	Full stans i togtrafikken.
Kystfarten	*Moderat*	Det blir moderate forsinkelser i kystfarten.
Luftfarten	*Stor*	Full stans i kommersiell flytrafikk.
Sentral kriseledelse og krisehåndtering	*Stor*	Mangelfull koordinering og informasjon uten telefon, Internett, radio og TV. Reserveløsninger med begrenset kapasitet.
Vannforsyningen	*Liten*	Vannforsyningen påvirkes i liten grad.
Bank- og finansvirksomheten	*Stor*	Ingen økonomiske transaksjoner, begrenset bruk av betalingsterminaler.
Helse og omsorg	*Stor*	Sykehus og legevakt uten kontakt med omverdenen – redusert effektivitet, utsatt behandling.
Nødsentralene		Ambulanse, politi og brannvesen kan ikke nås på nødnumrene. Mangelfull koordinering av aksjoner.
Nødnett		Nødnettet fungerer bare lokalt.

Kilde: DSB.

Tabell 11.3 Konsekvenser ved utfall av ekomnettet

Samfunnsverdi	Konsekvenstype	Konsekvenser	Usikkerhet	Forklaring
Liv og helse	Dødsfall	Store	*Stor*	50 ekstra døde som følge av manglende mulighet til å ringe ambulanse og varsle nødetatene ved akutte hendelser.
	Alvorlig skadde og syke	Middels/ store	*Stor*	200–300 alvorlig skadde og syke som følge av utsatt behandling eller feilbehandling.
Natur og miljø	Langtidsskader på naturmiljø			Ikke relevant.
	Uopprettelige skader på kulturmiljø			Ikke relevant.
Økonomi	Direkte økonomiske tap	Store	*Moderat*	Reparasjons- og erstatningskostnader knyttet til ødelagte systemkomponenter på mellom 2 milliarder og 10 milliarder kroner.
	Indirekte økonomiske tap	Svært store	*Moderat*	Tap av inntekter, forsinkelseskostnader, produksjonsnedgang og redusert handel til et samlet tap på 10 milliarder kroner.
Samfunnsstabilitet	Sosiale og psykologiske reaksjoner	Svært store	*Stor*	Manglende informasjon fra myndighetene, vanskelig krisehåndtering, ukjent og tilsiktet hendelse skaper uro og bekymring.
	Påkjenninger i dagliglivet	Store	*Stor*	Manglende tilgang til tele- og datatjenester og betalingsmidler. Forsinkelser i vare- og persontransport.
Demokratiske verdier og styringsevne	Tap av demokratiske verdier og nasjonal styringsevne	Store	*Moderat*	Angrep mot svært viktig infrastruktur, som er bærer av samfunnets evne til å styre. Sentrale institusjoners funksjonsevne trues. Krenkelse av demokratiske verdier og individuelle rettigheter.
	Tap av kontroll over territorium			Ikke relevant
Samlet vurdering av konsekvenser		Store/ svært store	*Stor*	Totalt sett store, til dels svært store, konsekvenser.

Kilde: DSB.

korte utfall av kjernenettet vil kunne medføre betydelige kostnader for samfunnet.

I scenarioet i Nasjonalt risikobilde (NRB) er det i tillegg beskrevet at utfall av ekomnettet vil kunne medføre flere følgehendelser som medfører konsekvenser for liv og helse: manglende mulighet for å varsle nødetatene på nødnumrene ved akutte hendelser, ikke mulig å rekvirere ambulanse på vanlig måte, mangelfull kommunikasjon og koordinering mellom nødetatene fordi Nødnett bare fungerer lokalt, samt redusert effektivitet og utsatt pasientbehandling. Som en følge av dette er det beregnet at en konsekvens vil være en øking i dødsfall på 10 prosent per dag, noe som innebærer 10 flere dødsfall daglig i forhold til normalsituasjonen (basert på tall fra 2013).[17]

Overbelastning i nettet

Ekominfrastrukturen er dimensjonert for å håndtere normal trafikk. I situasjoner der behovet øker markant, for eksempel i krisesituasjoner som Utøya-hendelsen, vil visse tjenester kunne svikte ved at brukeren ikke får tilgang til tjenesten. Slik

[17] Direktoratet for samfunnssikkerhet og beredskap (2015): *Risikoanalyse av cyberangrep mot ekom-infrastruktur.* Delrapport til Nasjonalt risikobilde 2014.

overbelastning kan også oppstå ved nektelsesangrep, der en motpart sender falsk trafikk mot servere i ekominfrastrukturen med formål å lamme disse. Trusselen fra nektelsesangrep er av flere operatører fremhevet som en reell trussel som kan ramme både operatøren og operatørens kunder.

Logiske og fysiske feil

Etter som mer og mer av funksjonaliteten i nettene har med programvare å gjøre, vil logiske feil utgjøre en stadig større andel av feilene. Denne typen feil i kjernenettet vil kunne ha konsekvenser for mange brukere og store områder og i verste fall for hele tjenester i hele landet.

Logiske feil som følge av overbelastning av nettene kan også bli et økende problem. Stadig flere får smarttelefoner, som ikke bare brukes til å ringe med, men også til å surfe på nettet, sende e-post og andre mobile tjenester. Samtidig øker bruken av mobilt bredbånd kraftig. Dette medfører omtrent en dobling av datatrafikken hvert år.

Kjernenettene er dimensjonert for å tåle stor belastning, og det er gjerne aksessnettene som setter grensene for mengden trafikk. Dersom det er brudd eller vedlikehold på en strekning (eller gjerne to) i kjernenettet, kan det imidlertid bli problemer med overbelastning på den andre eller tredje strekningen.

Alt ekomutstyr er avhengig av strøm og vil være sårbart for strømbrudd. Sentrale punkter i infrastrukturen er imidlertid som oftest sikret med en betydelig reservestrømkapasitet.

Fysiske skader på infrastrukturen vil i hovedsak være en følge av naturhendelser. Eksempler på hendelser er Dagmar og brannen i Lærdal. Utfordringene i forbindelse med disse hendelsene har imidlertid ikke oppstått som følge av brudd eller problemer med kjernenettene, men i regionalnettet. Kjernenettet har større grad av fremføringsdiversitet og redundans, og brudd som følge av naturhendelser får gjerne liten betydning for befolkningen.

Det finnes imidlertid eksempler på situasjoner der en naturhendelse har ført til brudd på kjernenettet samtidig som det er blitt utført oppgraderinger eller vedlikehold på alternative føringsveier. I slike tilfeller kan naturhendelser utgjøre en trussel mot kjernenettene.

Jordkabler er utsatt for skade i forbindelse med ulike typer gravearbeid. De som utfører gravearbeid, har ofte liten oversikt over hvilke ledninger og kabler som befinner seg hvor, og graveskader forekommer hyppig. I likhet med naturhendelser utgjør dette først og fremst en trussel mot kjernenettet i tilfeller da det enten er flere graveskader samtidig eller utføres vedlikeholdsarbeid eller lignende på alternative føringsveier.

Fysisk skade på infrastrukturen kan også være en konsekvens av tekniske feil. Tekniske feil kan føre til overoppheting av komponenter som følge av svikt i kjøling, feilmontering eller skader på komponenter under vedlikehold. Dette er igjen feil som kan føre til at et helt system slutter å fungere som forventet.

11.5.3 Avhengigheten av kraftforsyning

Ekom kan ikke driftes over lengre tidsrom uten stabil strømforsyning. Statistikk viser at utfall i strømnettet er en av de viktigste årsakene til utfall i ekominfrastrukturen. Det er imidlertid store variasjoner i reservestrømkapasiteten hos de ulike nettleverandørene og i de ulike delene av nettet.[18] Spesielt noder i kjernenettet er utstyrt med god reservestrømkapasitet, men jo lenger man kommer ut mot aksessnettet, er reservestrømberedskapen enten fraværende eller har svært begrenset kapasitet. En medvirkende årsak er at kostnaden med å etablere reservestrømløsninger er lavere i kjernenettet/regionalnettet enn i aksessnettet.

En gjennomgang av driftsstatistikken for Nødnett for 2011 dokumenterte to hovedårsaker til utfall av basestasjoner – for lite reservestrøm på egen basestasjon (inkludert egen transmisjon) og utfall av transmisjon på leide linjer. Om lag 92 prosent av utfallene ville vært unngått gjennom å øke reservestrømberedskapen til 24 timer, og 99 prosent av feilene som er registrert, kunne vært unngått ved å øke reservestrømtiden til 48 timer – dette under forutsetning av at leide linjer også har tilsvarende reservestrøm. Utbyggingen av Nødnett baseres i stor grad på bruk av den eksisterende infrastrukturen for telekommunikasjon, inkludert leide telelinjer. Reservestrømkapasiteten i denne infrastrukturen varierer og er mangelfullt kartlagt. Oppetiden for transmisjon ved strømbrudd er derfor ikke forutsigbar, og det er da ikke mulig å sikre et forutsigbart nødnett ved lengre strømbrudd.[19]

I juni 2014 gjorde Nkom vedtak om minstekrav til reservestrømkapasitet i mobilnett. Vedta-

---

[18] Nexia/Styrmand (2012): *Kost/nyttevurdering av tiltak for styrking av norsk sambands- og IP-infrastruktur.* For Post- og teletilsynet.

[19] Fra *Robusthet i transmisjon. Reservestrøm i transmisjonslinjer i Nødnett*, DNK februar 2014.

Boks 11.1 Ekstremværet Dagmar

Ekstremværet Dagmar i romjulen 2011 avdekket ikke bare fysiske sårbarheter i kritisk ekominfrastruktur, men også hvor avhengig samfunnet har blitt av fungerende mobiltjenester. Denne hendelsen og erkjennelsen av samfunnets stadig økende avhengighet av elektronisk kommunikasjon omtales som et «paradigmeskifte» for arbeidet med sikkerhet i ekominfrastruktur.

Dagmar førte til større bortfall i fasttelefonnettet, med cirka 31 500 abonnenter uten fasttelefon og cirka 12 000 uten Internett/bredbånd. De største regionale utfallene var på Nordvestlandet med cirka 20 000 abonnenter uten fasttelefon og cirka 7 500 uten Internett/bredbånd.[1] Hovedårsaken til utfallene på Nordvestlandet var bortfall av strøm i sentrale noder og i enkelte tilfeller transmisjonsfeil og skader på selve utstyret i nodene. Dagmar førte også til utfall i mobilnettene, spesielt ble Sogn og Fjordane og Møre og Romsdal hardt rammet. Av de 728 basestasjonene som hadde falt ut 27. desember 2011, var 445 lokalisert i de to fylkene på Nordvestlandet. Hovedårsaken til bortfallet var strømbrudd og mangelfulle reservestrømløsninger sett i forhold til varigheten av hendelsen. Strømutfallet som følge av stormen førte også til redusert dekning i deler av Nødnett i Akershus og Buskerud. 45 av 240 basestasjoner hadde kortere eller lengre utfall, og åtte av disse hadde lengre nedetid enn ti timer.

[1] *Foreløpige erfaringer og forslag til tiltak etter ekstremværet Dagmar.* PT-rapport nr. 2 2012.

ket var rettet mot mobilnetteierne Telenor, TeliaSonera (NetCom), Mobile Norway (Tele2) og ICE, og er hjemlet i ekomloven § 2-10 første ledd. I vedtaket stiller Nkom krav om minst to timer reservestrømkapasitet i mobilnettenes dekningsområder der det er fast bosetting eller næringsvirksomhet. I områder utenfor byer med mer enn 20 000 innbyggere skal reservestrømkapasiteten i snitt være på fire timer. Vedtaket ble påklaget av samtlige. SD som klageinstans stadfestet vedtaket.

11.5.4 Sårbarheter knyttet til drift og styring

Svakheter i regimene hos operatørene når det gjelder fysisk og logisk tilgang til anlegg og systemer

Nkom har identifisert sårbarheter knyttet til driften hos de enkelte operatørene. Det er forskjell mellom de ulike operatørene i hvordan de har valgt å styre risiko og sikkerhet. Et generelt funn fra Nkoms sårbarhetsanalyse av mobilnettene var svakheter relatert til fysisk og logisk tilgang til anlegg og systemer.

Problemstillinger knyttet til utstyrets opprinnelsesland

Det har i de senere årene vært mye oppmerksomhet omkring opprinnelsesland for viktig utstyr for kritisk infrastruktur. I Norge har den offentlige diskusjonen i stor grad vært knyttet til Huaweis leveranser til store teletilbydere.

Potensialet til statlige aktører i cyberdomenet er en vesentlig og dimensjonerende faktor for design av gode sikkerhetsløsninger. Opprinnelsesland for leverandør av utstyr er dermed en del av totalbildet. I IKT- og ekomsektoren er imidlertid de fleste leverandører globale aktører som integrerer utstyr fra en rekke ulike underleverandører fra ulike land. Å avgjøre hvilket land utstyret «kommer fra», vil dermed i en del tilfeller bare ha verdi som en teoretisk øvelse.

Komplekse markedsstrukturer og omfattende utstyrsportefølje

Aktørene i markedet må forholde seg til et mangfold av samarbeidspartnere. Noen av disse samarbeidspartnerne vil i andre sammenhenger fremstå som konkurrenter. Å ha full oversikt over dette bildet er en utfordring, særlig når markedet er i stadig endring. Uoversiktlige organisasjoner og mangelfulle arbeidsprosesser er også påvist i sårbarhetsanalysen av norske mobilnett. Enkeltkomponenter kan også ha defekter og feil i maskinvare og programvare.[20]

De større elektroniske kommunikasjonsnettene er satt sammen av en omfattende utstyrsportefølje fra ulike leverandører. Programvare for styring av de enkelte komponentene og for samvirket mellom de ulike komponentene er svært kompleks. Tester kan verifisere at programvare og teknisk utstyr samvirker og utfører de funksjonene de skal. Samtidig vil det for slike systemer være tilnærmet umulig å verifisere at det ikke

[20] Hentet fra blant annet *Sårbarhetsanalyse av mobilnettene i Norge*, Nkom-rapport nr. 1 2012, Post- og teletilsynet.

foreligger alvorlige intenderte eller ikke-intenderte logiske sårbarheter. Forholdet mellom leverandør og kunde av slikt utstyr og programvare må derfor bygge på tillit. Denne tilliten er viktig for leverandørene i et konkurranseutsatt marked, og myndigheters eventuelle inngripen i slikt utstyr for å installere bakdører kan ødelegge for de private leverandørene.[21]

Vedlikehold og endringsledelse av en sammensatt infrastruktur

Elektroniske komponenter, maskinvare, fastvare og programvare som benyttes innen ekom, er i stadig utvikling både når det gjelder forbedring av funksjonalitet, og når det gjelder sikkerhet. Dette er noe av dynamikken teleoperatører må forholde seg til i daglig drift. Etterslep på vedlikehold og oppgradering av systemer, programvare og programvarelisenser representerer mulige digitale sårbarheter. Det er vel kjent at angripere går etter gamle sårbarheter, og ekominfrastruktur består av både nye og eldre systemer. Imidlertid er det ikke uproblematisk å oppgradere all infrastruktur. Feilkonfigurasjon representerer en risiko som kan medføre feilsituasjoner og svikt.

Kompetanse hos nasjonale tilbydere

Tradisjonelle tilbydere utkontrakterer oppgaver til entreprenører og leverandører. Der dette skjer i stor utstrekning, bygges det opp en avhengighet av kompetansen og kapasiteten hos underleverandørene. Dette fører til at erfaring fra hendelser ikke flyter tilbake til tilbyderens organisasjon, og evnen til å improvisere og håndtere situasjoner svekkes over tid. I slike tilfeller kan organisasjonens evne til å lære av hendelsene og forbedre sikkerheten bli redusert.

11.5.5 Driftsmodeller under press fra den globale konkurransen

En av de store utgiftspostene for tilbyderne er drift av og gjentatte reinvesteringer i nett og serverpark. Delvis kan dette gjøres ved effektivisering, men i tillegg er det ønskelig å flytte en del driftsaktiviteter til land med lavere kostnader. Blant de store tilbyderne av ISP- og skytjenester er det et ønske om å utkontraktere drift, både med tanke på stordriftsfordeler og med tanke på de lavere lønnskostnadene man finner utenfor Norden. Ettersom mange av de store tilbyderne eller deres partnere har operasjonssentre over store deler av verden, ligger det store besparelser i å samkjøre drift.

Mange tilbydere har de siste årene redusert sin egen bemanning med teknisk kompetanse og kjøpt inn denne fra underleverandører. Det kan være betydelige kostnadsbesparelser for tilbyderne i å slippe å vedlikeholde den spisskompetansen som kreves. Underleverandørene leverer tjenester til flere tilbydere, systemintegratorer og driftssentre, og kan derfor utnytte kompetansen bedre.

Frafallet av teknisk personell hos tilbyderne betyr også at det er nødvendig med tjenesteavtaler med produsenter av nettverksutstyr. Ved endringer i komponenter, programvare og systemer, periodisk vedlikehold og håndtering av feil i utstyr kan det være nødvendig å gi produsenter og eksternt personell logisk eller fysisk tilgang til kritisk nettverksutstyr.

11.5.6 Nasjonal autonomi og personvernutfordringer

Sikkerhets- og beredskapsregelverket utfordres i markeder der aktører og tjenester opererer på tvers av landegrenser

Mens regelverket som regulerer ekomaktører, i hovedsak er nasjonalt, blir aktørene i økende grad multinasjonale. Utkontraktering av tjenester fra de tradisjonelle operatørene, internasjonal konsolidering i bransjen og nye, Internett-baserte aktører bidrar til et nytt bilde der de nasjonale landegrensene mister relevans. Et eksempel er utenlandske morselskaper, som TeliaSonera, som lokaliserer viktige tjenesteelementer utenfor Norges grenser. Sett fra operatørens ståsted er det av kostnads- og effektivitetshensyn fornuftig å gjøre dette, men fra et norsk ståsted kan det øke risikoen for utfall av tjenester og informasjonslekkasje. Slike driftsmodeller kan føre til at tilsynsmyndighetene ikke har nødvendige virkemidler overfor markedsaktøren.

Samtidig utvikler store internasjonale aktører OTT-tjenester[22] som ikke er underlagt norske myndigheters jurisdiksjon. Hvis slike aktører får operere uten å ta hensyn til nasjonale sikkerhetskrav og beredskapsregelverk, vil det representere en konkurransefordel for disse sammen-

[21] Brev fra John T. Chamber, CEO Cisco System, til president Obama, vedrørende lekkasjer i media om at NSA har brutt opp CISCO-forsendelser og modifisert CISCO-produkter. Datert 15. mai 2014.

[22] Over the top.

lignet med nasjonale aktører som er underlagt nasjonalt lovverk. Dermed kan dette i neste omgang medføre press fra bransjen som opererer i Norge mot mindre streng regulering, eller bety at bransjen må omstilles for å tilpasse seg den nye konkurransesituasjonen.[23]

Personvern

Utviklingen innen global ekom og Internett, der en sammensatt infrastruktur av eierforhold og verdikjeder krysser landegrenser, og der ulike land har ulike regler for innsyn i teletrafikk, utfordrer personvernet. For eksempel har ikke norske tilsynsmyndigheter anledning til å drive tilsyn med OTT-tjenester. De vil være underlagt andre lands regulering. Facebooks kommunikasjonstjeneste og Skype er eksempler på dette.

Norske myndigheter regulerer politiets innsynsrett i Norge. Det følger av ekomloven § 2-9 at tilbydere av elektronisk kommunikasjon har plikt til å bevare taushet om innhold av elektronisk kommunikasjon. Etter straffeprosessloven § 118 første ledd og § 230 første og fjerde ledd kan retten og politiet anmode Nkom om fritak fra den lovpålagte taushetsplikten. I de senere årene har det vært en betydelig økning i antall anmodninger knyttet til signaleringsdata, som vurderes å være en meget personverninngripende metode. Signaleringsdata er informasjon som genereres og lagres selv når telefonene ikke er i bruk. Data som genereres, gir blant annet informasjon om hvor telefonen befinner seg. Når abonnenten har telefonen med seg, er det nærliggende å sammenligne denne typen informasjon med det som kommer fra inngripende og spesifikt regulerte skjulte tvangsmidler som teknisk sporing. Nkom har lagt denne analogien til grunn for sin skjønnsutøvelse ved anmodning om å oppheve tilbyderens taushetsplikt for å få tilgang til signaleringsdata.

Det er en del ulike forespørselstyper med varierende hjemmelsgrunnlag for frigivelse og regimer for håndtering som må holdes fra hverandre. Dette gjelder for eksempel

- forespørsler fra politiet om abonnentinformasjon som ikke trenger myndighetsgodkjenning
- anmodninger om trafikk- og signaleringsdata der Nkom kan innvilge eller avvise å oppheve tilbyderens taushetsplikt om disse
- anmodning om kommunikasjonskontroll (KK) som trenger rettens kjennelse før iverksetting

Når trafikken krysser landegrenser og personopplysninger lagres på servere i andre land, er det andre lands jurisdiksjon som gjelder. Imidlertid har tilbyderne plikt til å informere kunder hvis trafikkdataene går over landegrenser, for eksempel via Sverige. Innen ekom vil typisk både innholdsinformasjon, abonnementsdata, faktureringsopplysninger og trafikkdata representere personopplysninger som enkeltmennesker ikke ønsker skal komme på avveier.

Risiko er knyttet både til lekkasje i forbindelse med det enkelte lands myndigheters tilgang til data til ulike formål og til den generelle trusselsituasjonen i det enkelte landet. Det er på sikt stor risiko for enkeltmennesket dersom stordataanalyse får stor utbredelse og for eksempel trafikkdata og personopplysninger kobles med andre kilder. Personopplysningsloven og EU-lovgivning vil kunne motvirke noe av denne risikoen, men det er likevel slik at både Norge og EU er deltagere i et globalt marked, og det er usikkerhet knyttet til hvem som setter personvernagendaen på sikt (se punkt 23.6 «Næringsutvikling og IKT-sikkerhet»).

Den teknologiske utviklingen setter også personvernet under press. Et eksempel er saken med

[23] Post- og teletilsynet (2014): *Ekomtjenester, -nett og -utstyr. Utvikling og betydning for PT.*

Tabell 11.4 Anmodning om trafikk- og signaliseringsdata. Det er bare strekpunkt 2 over som gjenspeiles i tabellen

	Trafikkdata	Basestasjonssøk	PUK-kode	Trafikkdata/ Basestasjonssøk inkl. signaliseringsdata
2014	1091	208	121	161
2013	1260	234	117	65
2012	1199	250	135	2
2011	1408	332	184	0
2010	1491	316	243	0

Kilde: Nkom.

falske basestasjoner der en mulig angriper kunne fange opp mobiltelefonene til intetanende personer som passerte.[24] Dette er langt fra den eneste måten å få tilgang til teletrafikken fra mobiltelefoner på, det finnes også utviklet skadevare som brukere kan lures til å installere på smarttelefonene sine. Også i forbindelse med programvareoppdateringer kan skadevare som senere spionerer på offeret, bli implementert.

11.6 Fremtidige problemstillinger og trender

Fra «fysiske» til «logiske» nettverk

Ekomtilbyderne benytter IP-nett for produksjon av de fleste av tjenestene sine, og IP-infrastrukturen er i ferd med å bli en felles produksjonsplattform for ekomtjenester. Telenors IP-nett vil de nærmeste årene bære alle Telenors egne faste og mobile telefoni- og bredbåndstjenester, i tillegg til å være det nasjonale transportnettet for mange andre tilbydere. IP-infrastruktur generelt, og Telenors IP-nett spesielt, er og vil fortsette å være svært viktig for produksjon av ekomtjenester på nasjonalt nivå.

Mens ulike produksjonsplattformer tidligere besto av spesialiserte produkter av maskin- og programvare fra enkeltleverandører, blir funksjonaliteten i ekomnett i økende grad realisert gjennom konfigurerbar programvare som er «frikoblet» fra den fysiske infrastrukturen. På den ene siden skaper dette større effektivitet og fleksibilitet ved produksjon av ekomtjenester og gir grunnlag for reduserte kostnader. På den andre siden medfører slike løsninger høy grad av kompleksitet i programvare, integrasjon og konfigurasjon samt avhengighet av underleverandører. I tillegg introduserer de nye sårbarheter knyttet til både utilsiktede hendelser som programvarefeil og konfigurasjonsfeil og tilsiktede hendelser som IKT-angrep. Sentralisering av tjenesteproduksjon fører dessuten til økt skadepotensiale.

Utkontraktering og internasjonalisering

I de senere årene har tilbyderne i økende grad benyttet eksterne leverandører i alle ledd i sin virksomhet, og det er i dag i hovedsak eksterne leverandører som står for installasjon, drift og vedlikehold av tilbydernes nett, samt en del administrative funksjoner. I tillegg plasserer tilbydere i økende grad det fysiske utstyret hos eksterne datasenterleverandører som leverer strøm, kjøling og fysisk sikkerhet. En annen trend er såkalte managed services, der utstyrsleverandører også står for den daglige nettverksdriften.

En trend er også at tilbyderne i økende grad konsoliderer virksomheten sin ved å sentralisere tjenesteproduksjonen til ett land, for så å tilby ekomtjenester på tvers av landegrenser. Dette foregår i dag i stor utstrekning i de nordiske landene. I likhet med ekomtilbyderne er også ekomtilbydernes underleverandører i all hovedsak selskaper som opererer multinasjonalt. Produksjon av norske ekomtjenester vil derfor i økende grad avhenge av innsatsfaktorer fra flere virksomheter i flere land. Fra et sikkerhetsperspektiv er den omfattende utkontrakteringen og internasjonaliseringen utfordrende for forhold som de nasjonale tilbyderes egenkompetanse, evne til risikostyring av virksomheten og kontrollen med trafikkdata og kommunikasjon på tvers av landegrenser. En del sikkerhetsaspekter knyttet til tilbydernes virksomhet vil også kunne ligge utenfor regulerende myndigheters jurisdiksjon.

Bevissthet rundt trusselbilde

Både tilbyderne og myndighetene vil fremover i større grad måtte forholde seg til, og tilpasse seg, et dynamisk trusselbilde og se trusselbildet i lys av samfunnets avhengighet av elektronisk kommunikasjon. I tillegg er det viktig at brukere av elektroniske kommunikasjonstjenester, virksomheter så vel som individer, i nødvendig grad er kjent med trusler mot disse tjenestene og har forståelse for at det kan være nødvendig med egne sikringstiltak tilpasset egen risikoaksept.

11.7 Vurderinger og tiltak

Økningen i samfunnsverdier som legges på toppen av ekominfrastrukturen, mangler historisk sidestykke. For tilbyderne er det svært krevende å ha et forhold til de verdiene de forvalter på vegne av kundene. For kundene er det komplisert å sette seg inn i den risikoen tilbyderne har akseptert, gjerne gjennom en lang verdikjede av tilbydere og tjenesteleverandører. For myndighetene er det komplisert å drive risikostyring på vegne av samfunnet som helhet når verdiopphopningen går så raskt som den gjør i dette tilfellet.

Basert på denne vurderingen av situasjonen fremmer Lysneutvalget følgende forslag til tiltak:

[24] http://www.pst.no/media/pressemeldinger/vedtak-om-henleggelse-falske-basestasjoner/

11.7.1 Redusere kritikaliteten av Telenors kjerneinfrastruktur

Utvalget ser det som en naturlig konsekvens at tiltak må rettes inn mot de sårbarhetene som har et potensial for å gi et massivt ekomutfall, nærmest uavhengig av hvor sannsynlig det er at sårbarheten leder til en hendelse. Vi mener derfor at det må rettes spesiell oppmerksomhet mot Telenors kjerneinfrastruktur. Denne er godt utbygd med tanke på robusthet, den er profesjonelt operert og har historisk sett hatt svært stabil drift. Sannsynligheten for at den skulle svikte, anses som lav. Den vil likevel kunne settes ut av spill ved menneskelige feil, rutinesvikt eller utro tjenere.

Etter utvalgets syn er den totale summen av samfunnsverdier dette nettet er bærer av, uakseptabelt høy, samtidig som verdiene det bærer, bare øker.

Basert på egne vurderinger og en utredning fra Oslo Economics[25] *anbefaler utvalget derfor at SD og Nkom utvikler og gjennomfører tiltak som reduserer kritikaliteten av kjernenettet. Vi anbefaler at disse tiltakene rettes inn mot følgende fremtidige målbilde:*

1. Minst én tilleggsaktør har et landsdekkende kjernenett som er på samme nivå som Telenors med hensyn til dekning, kapasitet, fremføringsdiversitet, redundans og uavhengighet (utredningen til Oslo Economics peker i retning av en samfunnskostnad på om lag 575 millioner kroner. Tallet inkluderer investering og vedlikehold over 10 år).
2. I en normalsituasjon er trafikken spredt mellom de to kjernenettene på en slik måte at samfunnsverdiene de bærer, er fordelt. Spesielt bør det etterstrebes at fullstendig utfall i ett av kjernenettene gir en håndterbar samfunnsmessig situasjon.
3. De to kjernenettene har samtrafikkspunkter som kan omrute trafikk mellom nettene. Denne omrutingen kan knyttes til et begrenset antall prioriterte brukere.

11.7.2 Sikre mangfold blant leverandørene til infrastrukturen

En annen kilde til sårbarheter som kan være felles for flere ekomoperatører, er den som er knyttet til utstyrs- og tjenesteleverandører. Feil og bakdører i utstyr og programvareoppgraderinger fra en leverandør vil samtidig kunne slå ut i nettene til flere operatører. Diskusjonene som har pågått i mange land i den vestlige verden om bruk av utstyr fra kinesiske leverandører, har relevans for samtlige norske infrastruktureiere. Utvalget mener at man bør tilstrebe å ha en kontrollert heterogenitet i utstyrsleverandørbildet i norsk ekominfrastruktur, slik at sårbarheter med opphav hos én enkelt leverandør – uansett opphavsland – kun kan ha begrensede skadeeffekter. Utvalget observerer at det i høringsutkastet til ny sikkerhetslov er lagt inn et forslag om at Kongen i statsråd skal kunne stoppe enkeltinnkjøp til kritisk infrastruktur. Vi mener imidlertid at en slik lovendring er lite egnet til å håndtere den fulle kompleksiteten i sårbarhetsbildet knyttet til utvikling, produksjon, leveranse og drift av ekomutstyr.

Det er et faktum at de leverandørene som er best og billigst, selger mye og dermed overtar svært store deler av markedet. Dette kan være uheldig sett fra et sikkerhets- og avhengighetsperspektiv. En leverandørstyring kan bidra til å spre risiko på flere. Dette er en problemstilling som en ser på flere områder og i flere sektorer, men det er grunn til å tro at sårbarheten er størst på dette området. Konkurranselovgivningen vil i noen grad bidra til å forhindre monopolleverandører, men lovgivningen har ikke i tilstrekkelig grad klart å forhindre at det er en ensidighet i visse utstyrsleverandører. *Nkom bør derfor, i samråd med Konkurransetilsynet, ta initiativ til å utrede hvorvidt vi i dag har tilstrekkelige virkemidler for å ivareta dette forholdet, eller om det er behov for å etablere virkemidler for å sikre diversitet i utstyr. Denne problemstillingen bør også tas med i utformingen av ny sikkerhetslov (del II).*

11.7.3 Opprette en CSIRT i ekomsektoren i regi av Nkom

Det er totalt cirka 175 tilbydere av elektroniske kommunikasjonstjenester i Norge. Av disse er flesteparten svært små, og de færreste eier eget nett. Det er nødvendig med en god overgripende håndtering av hendelser i det digitale rom som favner hele dette spekteret. Det er under planlegging å etablere en CSIRT for sektoren i regi av Nkom, som skal bistå selskapene i håndteringen av digitale angrep. Det er pekt på at det kan være en utfordring tillitsmessig ved at CSIRT-enheten ligger i en tilsynsmyndighet, og dette må det tas hensyn til ved utvikling av funksjonen. En fordel med denne plasseringen er blant annet at Nkom er øverste myndighet til nedstenging som et virkemiddel ved uønskede hendelser, og vil sitte nær

[25] Oslo Economics (2015): *Konsekvensutredning – Alternativer for styrket robusthet i landsdekkende kjernenett.* Utarbeidet for Lysneutvalget.

selve hendelsen. *I dette tilfellet anbefaler vi derfor organisatorisk oppheng hos Nkom. Retningslinjene fra Justis- og beredskapsdepartementet underbygger også en myndighetstilknytning for organet.*[26]

11.7.4 Aktiv myndighetsutøvelse fra Samferdselsdepartementet og Nasjonal kommunikasjonsmyndighet

Det funksjonsbaserte regelverket innenfor ekomsektoren vurderes i utgangspunktet å være godt egnet for å møte stadige endringer i trusselbilde, teknologi og tjenesteproduksjon. Dersom samfunnets behov for forsvarlig sikkerhet i nett og tjeneste skal møtes, krever dette imidlertid en sterk og endringsdyktig ekommyndighet (SD og Nkom). Det vurderes som viktig, som Nkom selv påpeker, at pålegg, avtaler og tiltak innenfor sektoren er forankret i en overordnet ROS-analyse som også adresserer avhengighet av andre sektorer, som eksempelvis kraftforsyningen og justismyndigheten. Det er viktig med en offensiv videreutvikling av regelverket, slik at det til enhver tid er oppdatert i forhold til trusselbildet, den teknologiske og markedsmessige utviklingen og samfunnets behov for ekom. *Ekommyndigheten må styrke innsatsen ytterligere ved å veilede tilbyderne om innholdet i rettslige standarder knyttet til sikkerhet og robusthet. Utvalget vurderer videre at en forsvarlig kobling mellom sentrale ekomaktører og de nasjonale sikkerhetstjenestene er helt nødvendig for å ivareta nasjonale sikkerhetsmessige behov, og anbefaler at dette arbeidet videreutvikles gjennom det etablerte Ekomsikkerhetsforumet.*

Nasjonal ekomplan

Det utarbeides for tiden en ekomplan innenfor Samferdselsdepartementets ansvarsområde knyttet til en ny digital agenda for Norge. Det er positivt at en slik plan etableres. Som nevnt over er imidlertid dette et komplekst felt med flere sentrale sektormyndigheter og aktører som til sammen ivaretar en helhetlig verdikjede. Avhengig av hvordan denne blir seende ut, kan det være ønskelig med en bredere fremtidig plan som også omfatter ekomperspektivet på tvers av sektorer i Norge, inkludert blant annet Nødnett og fremtidige behov for nødkommunikasjon. *En slik helhetlig plan bør ta innover seg hvordan krav til ekomnett og -tjenester gjenspeiler samfunnets økende behov for digitale tjenester. Planen bør inneholde en systematisk oversikt som jevnlig viser hvor ulike forebyggende tiltak bør prioriteres.*

Denne oversikten på ekomområdet bør videre benyttes som et bidrag i Justis- og beredskapsdepartementet større oversiktsbilde over IKT-sårbarhet i Norge.

11.7.5 Etablere tiltak for å regulere utlevering av trafikkdata til politiet

I et samfunn der det teknologiske mulighetsrommet endres så raskt som i dag, vil lovgivningen, som blir til gjennom demokratiske prosesser, alltid ligge etter de teknologiske realitetene. Noe av utfordringene rundt dette er søkt løst ved at lovverket har skjønnsmessige kriterier, mens dette samtidig kan medføre at formålet med bruken av informasjonen endres over tid, såkalt formålsglidning. Her kan vi nevne som eksempel at trafikkdata lagret for faktureringsformål i mange tilfeller brukes til å kartlegge enkeltpersoners bevegelser/aktiviteter knyttet til spesifikke basestasjoner. Man ser også at signaleringsdata lagret for tekniske driftsformål og som genereres uten abonnentens aktive bruk, benyttes til formål som grenser mot teknisk sporing.

Et annet og prinsipielt eksempel er at trafikkdata knyttet til alle personers trafikk ved en spesifikk basestasjon (eller flere) brukes til å kartlegge gruppers tilstedeværelse/bevegelser i et område («basestasjonssøk»). Dette gjøres typisk når det er begått en kriminell handling og man ikke har en konkret mistenkt person. Etterforskerne ønsker informasjon om trafikkdata for å kunne sammenligne med senere vitneuttalelser, avhør med mer. Et slikt basestasjonssøk vil, innenfor en gitt tidsramme, vise hvem som har vært aktive, hvem som har snakket med eller sendt SMS til hvem. Ved basestasjonssøk for signaleringsdata vil man også kunne finne lokasjonen til alle som er tilknyttet basestasjonens område. Dette kan i mange tilfeller gjelde svært mange mennesker.

Slik generell kartlegging av folkemengders kommunikasjon og lokasjon bør vurderes ut fra grunnleggende rettslige rammer, legalitetsprinsippet, og eventuelt reguleres særskilt. Det fremstår som en større formålsglidning at tekniske signaleringsdata (som skjer uten brukerens initiativ) brukes til å identifisere mulige mistenkte, enn at rene trafikkdata (generert ved aktiv bruk av mobil) gjør det.

I denne sammenhengen kan det også være en utfordring for dommere å ha tilstrekkelig teknisk innsikt til å forstå de tekniske begrepene, hvordan

[26] Justis- og beredskapsdepartementet (2014): *Modell for håndtering av IKT-sikkerhetshendelser – anbefalinger og retningslinjer*, brev til departementene.

de aktuelle dataene genereres, hvilket informasjonspotensial dataene har, og hvordan de kan brukes. Det er relevant å se på hvor grundig domstolene vurderer anmodninger om tilgang til data. Lysneutvalget har ikke hatt tidsmessig rom for å gjennomføre noen undersøkelse av dette, men viser til Metodekontrollutvalgets utsagn om at 13,8 prosent av dommerne selv og 58,4 prosent av advokatene mener det ikke blir gjort en tilstrekkelig vurdering av vilkårene for kommunikasjonskontroll, og at dette er bekymringsverdig.[27] Det fremgår samme sted at det er svært sjelden domstolene avslår en begjæring om kommunikasjonskontroll, noe som også er betenkelig.

Lysneutvalget har ikke grunnlag for å fastslå at Metodekontrollutvalgets funn illustrerer et generelt trekk som er overførbart til utvalgets mandat.

Som omtalt i punkt 11.5.6 «Nasjonal autonomi og personvernutfordringer», er omfanget av politiets uthenting av trafikkdata rimelig stabilt, mens andelen forespørsler om opphevelse av taushetsplikt for utlevering av signaleringsdata er sterkt økende. Det er mange spørsmål knyttet til forholdet mellom beslutninger om opphevelse av en taushetsplikt med hjemmel i straffeprosessloven § 118 jf. § 230 og menneskerettsloven § 2 jf. EMK artikkel 8.

Utvalget mener at formålsutglidning av bruk av opplysninger som omtalt over (særlig signaleringsdata) bør utredes. I denne sammenheng bør også dommernes tekniske kompetanse som grunnlag for å ta stilling til innsynsbegjæringer vurderes.

Utvalget mener det er behov for å avklare hjemmelsgrunnlaget for regulering av tilgang til signaleringsdata.

Utvalget er videre av den oppfatning at bruk av signaleringsdata er blitt så utbredt som etterforskningsverktøy at det bør vurderes å lovregulere dette som et særskilt tvangsmiddel.

---

[27] NOU 2009: 15 *Skjult informasjon – åpen kontroll*, side 164, høyre spalte.

Kapittel 12
Satellittbaserte tjenester

I løpet av de siste tiårene har tjenester som utnytter infrastruktur i verdensrommet, blitt en integrert del av hverdagen vår. Antallet samfunnsområder som blir berørt av bruk av rombasert infrastruktur, har økt. Det samme gjelder antallet aktører som er aktivt involvert i den globale romvirksomheten. Satellittsystemer vil i løpet av de neste årene få større strategisk og samfunnsøkonomisk betydning. Satellittbaserte tjenester brukes på de fleste områder – i navigasjons- og kommunikasjonssystemer, til skredovervåking og i avanserte styringssystemer for offshoreoperasjoner. Flere og bedre satellitter, økt dataprosesseringskapasitet, utbredelsen av Internett og fremveksten av mobilt kommunikasjonsutstyr har medvirket til denne utviklingen.

12.1 Romrelatert infrastruktur

En rekke kritiske samfunnsfunksjoner er avhengige av satellittbaserte tjenester for å være operative. Med satellittbaserte tjenester menes i denne sammenheng tjenester for posisjonsbestemmelse, navigasjon og presis tidsangivelse (PNT), kommunikasjonstjenester og jordobservasjonstjenester. Tjenestene leveres via satellitter som går i bane rundt jorda, og tilleggstjenester knyttet til disse for økt ytelse.

Globale satellittsystemer for posisjon, navigasjon og presis tidsangivelse (PNT). USA og Russland opererer i dag hvert sitt globale system, henholdsvis GPS og GLONASS. Begge er militære systemer, men spesielt GPS har fått stor sivil betydning.

Et tredje system, Galileo, er planlagt å være i full operativ drift fra 2020. Galileo er et system under sivil kontroll, eid og drevet av EU. Kina planlegger sitt eget globale satellittnavigasjonssystem (Beidou), som ventes å bli satt i drift rundt 2020. Slike satellittsystemer går under fellesbetegnelsen GNSS (Global Navigation Satellite Systems).

De ulike GNSS-systemene er interoperatible. Det vil si at brukeren kan benytte seg av alle satellitter som er tilgjengelige fra de ulike systemene, hvis brukerutstyret er tilpasset dette.

Støttesystemer til GNSS er utviklet for å gi brukerne bedre ytelse. Disse systemene leverer tjenestene sine enten via satellitt eller fra bakken og betjener brukere langs kysten, offshore, på land og i luften.

Satellittsystemer for kommunikasjon. Kommunikasjonssatellitter er konstruert for overføring av fjernsynsprogrammer, telefonsamtaler, data, bredbåndstjenester og lignende. Satellittkommunikasjon kan spille en viktig rolle for å sikre liv og helse og gjenopprette kritiske funksjoner når bakkebaserte systemer er satt ut av spill, for eksempel i forbindelse med storm, flom eller skred. Det viktigste satellittkommunikasjonssystemet i denne sammenhengen er Inmarsat (UK), som tilbyr data/bredbånds- og telefonitjenester på nær global basis til maritime, landmobile og aeronautiske brukere. Inmarsat er så langt det eneste satellittsystemet for tale og data som er en del av IMOs[1] GMDSS (Global Maritime Distress and Safety System). Systemet er basert på geostasjonære satellitter som står over ekvator, og har gradvis dårligere dekning nord for 72 grader. For mobile brukere i Arktis er i dag lavbane-satellittsystemet Iridium (USA) eneste kommunikasjonsmulighet for telefoni og lavrate datakommunikasjon. Iridium arbeider med å få akseptert systemet i GMDSS. Inmarsat ble i sin tid grunnlagt som en internasjonal ideell organisasjon, men er i dag på lik linje med Iridium et privateid kommersielt selskap.

Telenors Thor-satellitter tilbyr i hovedsak kringkastingstjenester. Dette kan være viktig for bred spredning av informasjon i kritiske situasjoner sammen med annen bakkebasert infrastruktur. Nyeste generasjon Thor-satellitter (fra 2015) vil også adressere maritime markeder for bredbåndskommunikasjon og vil gradvis kunne bli vik-

[1] International Maritime Organization, FN.

tigere her. Telenor og utenlandske aktører med avdelinger i Norge, som Airbus DS, tilbyr også leid kapasitet for punkt-til-punkt-forbindelser via satellitt. Betydelig trafikk, både kringkasting og toveis tale- og datakommunikasjon, håndteres av Telenors jordstasjon i Nittedal og Airbus' jordstasjon på Eik i Rogaland.

I tillegg benyttes systemer som er helt eller delvis eid av utenlandske aktører, for kommunikasjon både på norsk jord og til/fra nordmenn i utlandet og i internasjonalt farvann. Forsvaret har egne jordstasjoner for satellittkommunikasjon. En rekke meteorologiske målestasjoner og oseanografiske bøyer rapporterer også inn sine målinger via satellitt.

Satellittsystemer for jordobservasjon. Værsatellitter er nå den viktigste måletypen i numerisk værvarsling. Norge deltar derfor aktivt i det europeiske værsatellittsamarbeidet EUMETSAT, som opererer satellitter både i geostasjonære og polare baner. EUMETSAT har neste generasjon satellitter under utvikling for innfasing i geostasjonær bane fra 2018/2019 og i polar bane rundt 2021. EUMETSATs hovedbakkestasjon for de polare værsatellittene ligger på Svalbard. Det er Meteorologisk institutt (MET) som ivaretar Norges interesser i EUMETSAT. Også Norsk Romsenter er representert i EUMETSATs råd.

EUMETSAT og den amerikanske værvarslingsorganisasjonen NOAA (National Oceanic and Atmospheric Administration) i USA har et forpliktende samarbeid om bruk av hverandres satellitter. NOAAs satellitter betjenes av Kongsberg Satellite Services (KSAT) bakkestasjon på Svalbard. De amerikanske polare værsatellittene er derfor svært viktige for værvarslingen også i Norge.

Norge har nylig besluttet å bli med i EUs operative jordobservasjonssystem, Copernicus, som i årene fremover skal skyte opp en rekke operative satellitter for miljøovervåking. Også Copernicussystemet vil ha sin polare hovedbakkestasjon på Svalbard.

AIS-satellitter. Automatic Identification System (AIS) ble opprinnelig utviklet som et anti-kollisjonshjelpemiddel for skip. Alle fartøy over 300 bruttotonn er pålagt å ha systemet om bord. Det rapporterer jevnlig om skipets posisjon, kurs, fart og andre skipsdata. AIS brukes i dag også til trafikkovervåking og flåtestyring ved at signalene mottas av bakkestasjoner og satellitter.

AISSat-1 og AISSat-2 er norske småsatellitter som er i drift nå. AISSat-3 er planlagt skutt opp i 2016. Satellittene inngår i AIS-systemet for å gi dekning utover det landbasert AIS gir. Satellittene er å betrakte som teknologidemonstratorer, men har allerede vist seg å være svært nyttige for offentlig forvaltning. Satellittene AISSat-1 og AISSat-2 eies av Norsk Romsenter, mens AISSat-3 eies av Kystverket. Kystverket er ansvarlig for sentral forvaltning av dataene fra satellittene, sammen med data fra den landbaserte kjeden. Bakkestasjoner for kontroll av satellittene og nedlesing av data er etablert på Svalbard og i Vardø, med tilhørende infrastruktur.

Svalbardkabelen er en fiberoptisk kabelforbindelse som går mellom Fastlands-Norge og Svalbard. Den ble primært etablert for å sikre pålitelig dataoverføring for satellittvirksomheten på Svalbard. Forbindelsen består av to kabler som går fra Harstad via Andøya til Longyearbyen. Den ene kabelen er reserve for den andre. Etter landfall i Harstad og i Longyearbyen knyttes fiberkabelen sammen med Telenors kabler og utstyr. Space Norway AS (SPN) eier forbindelsen og noe av det elektroniske linjetermineringsutstyret. Selskapet har inngått kontrakt med Telenor Svalbard (TNS) om linjeleie og om lokaler for linjetermineringsutstyr både på Svalbard og på fastlandet.

Svalbardkabelen brukes av KSAT til overføring av data som hentes ned på Svalbard til ulike kunder og brukere i inn- og utland, av TNS til overføring av teleforbindelser (telefon, TV/radio og Internett) og av UNINETT til overføring av forskningsdata fra Svalbard til Norge og utlandet. SPN har i tillegg leid satellittkapasitet for et enkelt tjeneste-/sikringssamband til bruk for Sysselmannen og KSAT i tilfelle brudd i kabelforbindelsen.

Gjennom avtale mellom SPN og TNS er all overvåking og drift av anleggene og trafikken gjennom kabelen ivaretatt av Telenor. Telenor er også ansvarlig for all kommunikasjon og annen trafikk som går gjennom fiberkabelen til deres kunder, herunder institusjoner, bedrifter og privatpersoner. TNS har knyttet til seg Telenor Norge for å ivareta av deler av dette ansvaret, for eksempel nettovervåking.

TNS har utarbeidet en egen risiko- og sårbarhetsanalyse (ROS) for denne forbindelsen. SPN er nå i ferd med å utarbeide sin egen ROS-analyse ut fra selskapets eieransvar for kabelen. Ved hendelser som innebærer brudd i den ene eller begge kablene, ved planlagte arbeider på kabelforbindelsen, eller i andre situasjoner der kabelforbindelsen utsettes for risiko, vil TNS og SPN kommunisere og samarbeide om situasjonshåndteringen, herunder varsling til brukerne. Ved brudd i begge kablene samtidig vil eneste kommunikasjon være det enkle tjeneste-/sikringssambandet til bruk for Sysselmannen og KSAT, samt Iridium satellitt-telefoni.

12.2 Roller og ansvar

Leveranse av satellittbaserte tjenester er i hovedsak et internasjonalt anliggende, men flere norske etater er premissleverandører og har en myndighetsrolle på området. Det er ingen etat som har det overordnede ansvaret for satellittbaserte tjenester. Nedenfor gir vi en oversikt over de viktigste myndighetsaktørene.

Nærings- og fiskeridepartementet (NFD) er det nasjonale romdepartementet. NFD møter i ESAs ministerråd og i ESA/EU Space Council. NRS (Norsk romsenter) tar hånd om koordineringen av den nasjonale romsatsingen på vegne av NFD. Bevilgningene til ESA og NRS går i sin helhet over NFDs budsjett, og departementet er ansvarlig for de dominerende delene av den offentlige finansieringen av rominfrastrukturen. NFD er også ansvarlig for Galileo og Copernicus, med NRS som sekretariat.

Kunnskapsdepartementet (KD) er gjennom Meteorologisk institutt og deltagelsen i EUMETSAT en viktig aktør innenfor norsk anvendt romvirksomhet.

Samferdselsdepartementet (SD) har ansvar for koordineringen av den sivile radionavigasjonspolitikken, som også omfatter satellittnavigasjon. Kystverket overvåker skipstrafikk og oljesøl via satellitt og er hovedbruker av de norske satellittene for overvåking av skipstrafikken til havs (AIS).

Justis- og beredskapsdepartementet (JD) har gjennom sitt ansvar for samfunnssikkerhet og krisehåndtering direkte eller indirekte behov for satellitt-tjenester. Redningstjenesten bruker romtjenester i forbindelse med redningsoperasjoner, og JD deltar i søk- og redningssamarbeidet COSPAS-SARSAT. Under redningsaksjoner på Svalbard benyttes i økende grad både satellittkommunikasjon, satellittnavigasjon og jordobservasjon. Satellittbasert infrastruktur blir også benyttet av DSB og NSM. Politiet er en aktuell bruker av nye romtjenester som den offentlig regulerte tjenesten i Galileo.

Justis- og beredskapsdepartementet har også det overordnede ansvaret for de norske polare områdene og for embetsstyringen av Sysselmannen på Svalbard.

Forsvarsdepartementet (FD) bidrar gjennom Forsvarets forskningsinstitutt (FFI) til romforskning og jordobservasjon. Forsvaret og Kystvakten er brukere av informasjon fra jordobservasjons-, kommunikasjons- og navigasjonssatellitter. Forsvarets bruk vil de neste årene bli så omfattende og viktig at Forsvaret vil jobbe for sikker tilgang til satellittkapasitet. Gjennom GLOBUS 2-radaren ved Vardø bidrar Forsvaret til overvåking av romsøppel. FD forvalter avtalen med USA om tilgang til den militære delen av GPS.

Utenriksdepartementet (UD) bidrar til forskningsvirksomhet gjennom prosjektmidler til Forskningsrådet. UD har ansvar for at folkerettslige forpliktelser blir ivaretatt i forvaltningen av norsk romvirksomhet, og for eksportkontroll. UD er involvert i internasjonalt samarbeid der også romvirksomhet er et element, som internasjonalt samarbeid om kriser og beredskap, samt skogvernprosjektet. UD ivaretar også utenrikspolitiske problemstillinger knyttet til romvirksomhet på norsk jord.

Norsk Romsenter (NRS) er en etat under Nærings- og fiskeridepartementet (NFD) og er statens strategiske, samordnende og utøvende organ for å sikre en effektiv utnyttelse av verdensrommet til beste for det norske samfunnet. Norsk Romsenter ivaretar norske interesser i ESA og i EUs satellittnavigasjonsprogrammer, Galileo og EGNOS, samt i EUs jordobservasjonsprogram, Copernicus. NRS forvalter også diverse bilaterale avtaler. Nasjonalt forvalter Norsk Romsenter nasjonale følgemidler og er en støttespiller for norske industriaktører. I tillegg utarbeider de strategier for norsk romvirksomhet.

Meteorologisk institutt (MET) er landets største bruker av jordobservasjonsdata fra satellitt, og representerer Norge i den europeiske meteorologiorganisasjonen EUMETSAT. Instituttet har også noen egne antenner for direkte nedlesing av værdata fra satellitt.

Justervesenet har ansvaret for at Norge har en måleteknisk infrastruktur som både har nasjonal og internasjonal tillit. Justervesenet har også det forvaltningsmessige ansvaret for regelverket innenfor måleteknikk, blant annet normaltid. Justervesenet definerer tid som kritisk infrastruktur.

Nasjonal kommunikasjonsmyndighet (Nkom) er underlagt SD og har ansvar for frekvensforvaltning, herunder også for frekvenser som brukes av satellitter, og for tillatelser til etablering og drift av jordstasjoner. Internasjonale innmeldinger og koordinering foregår gjennom FN-byrået ITU (International Telecommunications Union). Sysselmannen på Svalbard fører, i samarbeid med Forsvarets forskningsinstitutt, tilsyn med forhold som omtales i kapittel 3 i jordstasjonsforskriften[2].

Nasjonal sikkerhetsmyndighet (NSM) er tillagt en særlig oppgave knyttet til oppfølgingen av sik-

[2] Samferdselsdepartementet (1999): *Forskrift om etablering, drift og bruk av jordstasjon for satellitt.*

kerhetsarbeidet i de europeiske satellittprogrammene Galileo og EGNOS. NSM har også ansvar for oppfølging av avtaler om utveksling av sikkerhetsgradert informasjon og sikkerhetsmessig godkjenning (akkreditering) av infrastruktur på norsk territorium.

UNINETT utvikler og driver det norske forskningsnettet, som forbinder norske utdannings- og forskningsinstitusjoner, og knytter dem opp mot internasjonale forskningsnett. UNINETT har ansvaret for drift av forskningsnettet på Svalbard.

Norsk romindustri består i dag av rundt 40 store og små selskaper spredt over hele landet. De utvikler og produserer alt fra terminaler for satellittkommunikasjon til blomsterpotter for planteforskning i rommet, og selger tjenester fra Antarktis i sør til Svalbard i nord, blant annet:

Telenor har ansvar for Thor-satellittene og Nittedal jordstasjon.

Airbus DS har ansvar for Eik jordstasjon.

Space Norway AS (SPN) støtter opp under Norsk Romsenters operative funksjoner. Selskapet eier den optiske fiberkabelen mellom Svalbard og fastlandet. Kabelen er et sentralt ledd i Norges infrastruktur i nordområdene. Space Norway har 50 prosent eierandel i Kongsberg Satellite Services (KSAT). Space Norway disponerer satellittbasert kommunikasjonskapasitet som dekker Trollstasjonen i Antarktis. Løsningen om bord i Thor 7-satellitten er utviklet i samarbeid med Telenor. Space Norway er også eier av Statsat AS, et selskap som skal håndtere norske statlige småsatellitter, som for eksempel AISSat.

Kongsberg Satellite Services AS (KSAT) eier og drifter infrastruktur og satellittstasjonene på Svalbard, i Tromsø og i Antarktis. KSAT eies av Space Norway AS (SPN) og Kongsberg Defence & Aerospace AS med 50 prosent hver.

Andøya Space Center (ASC) er et senter som gir forskningsstøtte til forskere som studerer mekanismene i atmosfæren, primært ved oppskyting av raketter og forskningsballonger. Beliggenheten på Andøya er svært gunstig for oppskyting. USA og flere europeiske land samarbeider på ASC.

Samordning mellom myndighetsaktører – det interdepartementale koordineringsutvalget for romvirksomhet

Slik det er i dag, finnes det ikke noe overordnet organ som formelt sett har ansvaret for den helhetlige romvirksomheten. Det er imidlertid opprettet et interdepartementalt koordineringsutvalg for romvirksomhet (IKU) som fungerer som informasjonsutvekslings- og møtearena for myndighetsaktørene som har ansvaret for ulike typer romrelaterte saker.[3] Utvalget ble opprinnelig opprettet for å koordinere Norges deltagelse i Galileo. IKU koordinerer etter hvert alle romrelaterte tverrsektorielle saker, for eksempel AIS-satellittene, BarentsWatch, Copernicus, Radarsat, romrelatert forskning i og utenfor EUs rammeprogram for forskning og oppfølging av rompolitikken som utvikles i EU og ESA. Utvalget blir ledet av Nærings- og fiskeridepartementet med Norsk Romsenter som sekretariat.

Underlag for en nasjonal romsikkerhetsstrategi

Norsk Romsenter (NRS) har tatt initiativ til å utarbeide et underlag for en nasjonal romsikkerhetsstrategi. Underlaget skal blant annet omhandle problemstillinger rundt arbeidet for et sikkert og bærekraftig rommiljø, sikkerhetsutfordringer knyttet til bygging, drift og utnyttelse av rominfrastruktur i rommet, sårbarhet knyttet til samfunnets avhengighet av satellittbaserte tjenester og hvordan rombasert infrastruktur kan styrke sikkerhetsnivået på ulike samfunnsområder. I arbeidet innhenter NRS innspill fra en rekke av de sentrale aktørene som er nevnt ovenfor. Arbeidet er ventet ferdigstilt i desember 2015.

Internasjonalt samarbeid

Rombaserte tjenester består av et utstrakt internasjonalt samarbeid, der departementer, etater og private virksomheter deltar på en rekke ulike områder. I tillegg til områdene som er nevnt over, samarbeider blant annet romfartsnasjonene i Inter-Agency Space Debris Coordination Committee (IADC) for å få kontroll over forurensingen av satellittbanene.[4]

Sivilt–militært samarbeid

Mye av romvirksomheten bærer preg av å ha en flerbruksnatur (dual-use) og omfatter derfor sikkerhetsrelaterte problemstillinger, som for eksempel eksportkontroll. Forsvaret er kunde av tjenester fra Kongsberg Satellite Services, blant annet når det gjelder nedlesing og prosessering av data fra den kanadiske satellitten Radarsat-2.

---

[3] Hjemmelen for opprettelsen av IKU ligger i St.prp. nr. 54 (2008–2009).

[4] Norsk romsenter (2013): *Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur.*

Tabell 12.1 Et utvalg relevante lover og tilhørende ansvarlig myndighet

Lov/Traktat	Angår	Ansvarlig dept./etat
Sikkerhetsloven med forskrifter	Forebyggende sikkerhet	JD/FD (NSM)
Ekomloven med forskrifter	Regulering av beskyttelse og radiofrekvenser + bakkestasjoner	SD (Nkom)
Svalbardtraktaten	Bruk av Svalbard til ikke-militære formål	UD/JD
Romloven	Lov om oppskyting av gjenstander fra norsk territorium ut i verdensrommet	NFD
International Convention on Maritime Search and Rescue	Internasjonal koordinering av SAR	JD
Metarea 19	Værvarsling	KD (met.no, Kystverket)
Galileo/Copernicus-forordningene	Beskyttelse av infrastruktur og tjenester	NFD (NRS)
Romregistreringskonvensjonen	Forvaltning av romregister for norske satellitter	UD (NRS)
ITU-konvensjonen	Frekvensfordeling	SD (Nkom)
Svalbardloven med forskrifter	Etablering, drift og bruk av bakkestasjoner med mer	SD
Havressursloven med forskrifter	Krav til satellittsporingsutstyr om bord på fiskebåter med mer	NFD, Fiskeridirektoratet
Lov om petroleumsvirksomhet med forskrifter	Satellittsporing av seismikkskip	OED
Skipssikkerhetsloven med forskrifter	Krav til kommunikasjonsutstyr med mer	NFD

Kilde: Norsk Romsenter.

Innen satellittkommunikasjon kjøper Forsvaret noen tjenester fra kommersielle aktører.

12.3 Hjemmelsgrunnlag og regulering

Regulering av romvirksomheten er hjemlet i mange ulike lover og forskrifter, og ansvaret for oppfølging tilhører ulike departementer og etater. Lovverket som angår norsk romvirksomhet, er på denne måten relativt komplekst. I tabellen over er det listet opp relevante lover og forskrifter med tilhørende ansvarlig myndighet. Tabellen er ikke utfyllende.

12.4 Sårbarheter i satellittbaserte tjenester

Samfunnets avhengighet av satellittbaserte tjenester fører også til en ny type risiko. Trusler fra eksempelvis sabotører, cyberangrep, kollisjon med romsøppel eller naturfenomener som romvær kan gjøre betydelig skade på samfunnets verdier gjennom å slå ut kritisk satellittinfrastruktur. Håndtering av denne risikoen er blitt en viktig myndighetsoppgave i Norge og blant store internasjonale aktører som EU og USA.

Sårbarheter i infrastruktur for satellittbaserte tjenester kan eksempelvis knyttes til

- selve satellittene og radioforbindelsen til/fra disse
- stasjoner på bakken (jordstasjoner)
- terminalutstyr hos brukerne

Konsekvensene av feil og skader på disse elementene og bevisst eller ubevisst påførte forstyrrelser kan for berørte brukere være av kritisk karakter. Norge har eierskap og operasjonelt ansvar for både satellitter og jordstasjoner.

Tabell 12.2 Trusler som kan påvirke rombasert virksomhet

	Fysisk infrastruktur	System
Tilsiktede	Anslag mot infrastruktur	Interferens Cyberangrep
Utilsiktede	Romvær Romskrot Naturfenomener	Menneskelig svikt Interferens

12.4.1 Trusler mot romrelatert infrastruktur

I 2002 uttrykte USAs riksrevisjon, GAO (General Accounting Office) bekymring over at kommersielle satellitter er sårbare for hackere. Siden 2004 har flere presentasjoner på hackersamlinger som Undercon og Black Hat drøftet muligheten for misbruk av datasamband via satellitt i ulike former for kriminell virksomhet. Eksempelvis påstår en presentasjon på hackersamlingen Black Hat at man med gratis programvare og standardutstyr verdt 50 euro kan misbruke datakommunikasjon over satellitt til ikke-sporbare angrep.

Etableringen av mulige alternative satellittnavigasjonssystemer til GPS, gjennom utbyggingen av Galileo, GLONASS og Beidou, bidrar til å redusere sårbarheten som følger med det å være avhengig av ett enkelt system. Den offentlig regulerte tjenesten Public Regulated Service (PRS) som planlegges for EUs Galileo-program, skal sikre nasjonale beredskapsmyndigheter tilgang til krypterte satellittnavigasjonstjenester. Disse vil være mindre sårbare for forsøk på sabotasje og manipulasjon.

Global informasjonsutveksling og verdensomspennende handel med elektroniske komponenter som oscillatorer, tunere, forsterkere, transistorer og batterier gjør støysendingsutstyr lett tilgjengelig til lave priser. Miniatyriseringen av komponenter bidrar til å gjøre støysendere skjulbare, lett transportable og dermed vanskelige å detektere. Risikoen for tilsiktet forstyrrelse av satellittsignaler er derfor reell.

Etter hvert som satellittsystemer får stadig større betydning for kritiske anvendelser som luftfart, sivil beredskap og aktiviteter relatert til Forsvaret, er det naturlig at disse systemene vil kunne være mål for fiendtlige angrep, både i form av angrep mot fysisk infrastruktur og i form av cyberangrep mot styrings- og driftssystemer.

Interferens, det vil si blokkering av signaler, kan være et resultat av både tilsiktede og utilsiktede hendelser. Tilsiktet interferens kan forårsakes av eksempelvis støysending (jamming), utsending av falske signaler (spoofing) eller retransmisjon av forsinket signal (meaconing).

Satellittnavigasjonssignaler er i utgangspunktet svake og vil lett kunne forstyrres av et sterkere jammesignal. Et jammesignal kan derfor redusere navigasjonsnøyaktigheten og gi feilaktig tidsinformasjon. Risikoen for tilsiktede forstyrrelser er reell, særlig ettersom radioutstyr som kan benyttes til dette, er relativt billig og lett tilgjengelig.

Sannsynligheten for at signalskjerming inntreffer, er avhengig av topografiske forhold og brukernes generelle kunnskap om egenskapene ved satellittsystemer. Risikoen for flerveisinterferens er stor i mange brukeromgivelser, spesielt i byområder og tett ved store konstruksjoner.

12.4.2 Samfunnets avhengighet av satellittbaserte tjenester

I Norge har romvirksomheten blitt en forutsetning for effektiv og sikker samfunnsdrift og for å følge opp prioriterte politiske målsettinger i nordområdene og i klima- og miljøpolitikken.

Satellittkommunikasjon punkt til punkt har til nå vært relativt kostbart sammenlignet med andre alternativer og benyttes derfor primært der annen infrastruktur ikke er tilgjengelig. I tillegg brukes den ofte som reserveforbindelse (backup) for kritiske forbindelser til for eksempel utestasjoner. For omtale av avhengigheter av satellittbaserte tjenester i sjøtransport, se punkt 18.4 «Sjøtransport».

Maskin-til-maskin-kommunikasjon, som fjernovervåking av anlegg og installasjoner og prosesstyring (også kalt SCADA), er et bruksområde i vekst, og avhengigheten av slike systemer er økende. Tabell 12.3 viser en oversikt over samfunnsfunksjoners avhengighet av satellittbaserte tjenester. Tabellen er ikke utfyllende.[5]

[5] Tabellen er basert på tabell i *Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring*. Direktoratet for samfunnssikkerhet og beredskap, 2012.

Tabell 12.3 Samfunnsfunksjoners avhengighet av satellittbaserte tjenester

Kritisk samfunnsfunksjon	PNT, kommunikasjon, jordobservasjon	Merknad
Opprettholde trygghet for liv og helse	Posisjon, navigasjon og tid, kommunikasjon og jordobservasjon	Nødetatene, inkludert Nødnett, er helt avhengige av PNT. Det samme gjelder SAR. Ved landing av fly benyttes GNSS støttesystemer (SBAS/GBAS). Elektroniske kartsystemer (ECDIS) og andre systemer for navigasjon og for rapportering av skipets posisjon er helt avhengige av satellittnavigasjonssystemet om bord. Kommunikasjon via satellitt er i enkelte områder eller når bakkenett er satt ut av drift, eneste mulighet for kommunikasjon eller kringkasting av informasjon. Værvarsling, skredvarsling og flomvarsling er avhengig av jordobservasjonstjenester fra satellitter.
Opprettholde lov og orden	Posisjon, navigasjon og tid	Nødetatene er helt avhengige av PNT. Tollvesenet er avhengig av PNT.
Opprettholde finansiell stabilitet	Tid	Finansnæringen er helt avhengig av tidssignaler i transaksjoner.
Opprettholde befolkningens behov for varme	Tid	Styring av kraftnett er helt avhengig av presis tid og frekvens.
Ivareta styring og kriseledelse	Posisjon, navigasjon og tid, kommunikasjon og jordobservasjon	PNT, satellittkommunikasjon og data fra jordobservasjonssatellitter sammen med geodata kan i noen kriser vært svært viktige verktøy.
Ivareta nasjonal sikkerhet	Jordobservasjon, PNT og kommunikasjon	Militære operasjoner er helt avhengige av PNT, og satellittkommunikasjon og data fra jordobservasjonssatellitter kan være vesentlig i enkelte sammenhenger. Suverenitetshevdelse og overvåking, spesielt av Norges store havområder, er avhengig av data fra jordobservasjonssatellitter.
Beskyttelse av natur og miljø	Jordobservasjon, satellittkommunikasjon, posisjon, navigasjon og tid	Detektering av oljesøl i havområder er helt avhengig av jordobservasjonssatellitter. For å unngå utslipp fra skip ved kollisjon eller grunnstøting er man avhengig av navigasjon, kommunikasjon og jordobservasjonssatellitter.
Vare- og persontransport	Posisjon, navigasjon og tid	Særlig luft- og sjøfart, men også veitransport og sikring av verdifull og farlig last, er avhengig av PNT.
Ekomtjenester	Satellittkommunikasjon	Kommunikasjon via satellitt er i enkelte områder eller når bakkenett er satt ut av drift, eneste mulighet for kommunikasjon eller kringkasting av informasjon.
Elforsyning	Tid og satellittkommunikasjon	Styring av kraftnett er helt avhengig av presis tid og frekvens. Det samme gjelder fjernstyring av kritisk infrastruktur der bakkebasert kommunikasjon ikke er tilgjengelig, for eksempel damanlegg.
Meteorologiske tjenester	Jordobservasjon, PNT	Værvarsling er helt avhengig av jordobservasjonssatellitter og bidrag fra navigasjonssatellitter.
Olje og gass	Posisjon, navigasjon og tid	Dynamisk posisjonering.

Kilde: DSB.

12.4.3 Romvær og romskrot

Romskrot er biprodukter av ulike typer romvirksomhet og består hovedsakelig av gamle satellitter som er tatt ut av drift, fragmenter av satellitter, utbrente deler av bæreraketter, fragmenter etter kollisjoner, samt objekter som er mistet i forbindelse med at astronauter har oppholdt seg utenfor romfartøyer. Når det gjelder den generelle risikoen for kollisjon med romskrot, er den størst i den lave jordbanen, der de operative observasjons- og kommunikasjonssatellittene befinner seg, sammen med ikke-aktive satellitter, rakettrester og annet romskrot.

Den tekniske kompetansen og evnen til å bruke våpensystemer mot satellitter er det i dag et begrenset antall stater, primært USA, Russland og Kina, som har. Et angrep i en krigssituasjon vil foruten eskalerende effekter ha store konsekvenser også for en angripers egen bruk av rommet, da et angrep med fysisk ødeleggelse vil skape enda mer søppel, som også vil komme til å utgjøre en trussel mot angriperens egne romsystemer.

Trusler mot brukernes utstyr i denne sammenhengen består i blokkering av signaler på grunn av radiostøy, ionosfæriske fenomener eller tilsiktet interferens, samt villedning gjennom utsendelse av falske signaler. Mangelfull brukerinnsikt kan derfor øke risikoen for at feilnavigering kan føre til ulykker.

Av utilsiktede hendelser vil romvær kunne slå ut kommunikasjon og føre til unøyaktig satellittnavigasjon, noe som igjen kan skape kritiske situasjoner. Romvær kan også forstyrre retningsstyrt oljeboring og leting etter olje og gass der det brukes magnetiske sensorer.

Norge er mer sårbart for romvær ettersom vi opererer teknologi lenger nord enn de fleste andre land. Det er derfor viktig at samfunnet er klar over disse effektene og settes i stand til å takle kraftig uvær i rommet.

Tilsvarende vil naturhendelser på jorden kunne utgjøre en trussel mot den bakkebaserte romvirksomheten.

Bruk av ett system (GPS) i nordområdene i perioder med kraftig ionosfærisk aktivitet kan innebære risiko for bortfall av signaler i korte tidsrom. Tilgang til flere satellitter vil gi bedre spredning av satellitter på himmelen, noe som igjen vil kunne gi bedre ytelse og økt signaltilgjengelighet i slike situasjoner. Faren for signalsvekkelse eller -tap på grunn av stor ionosfærisk aktivitet er reell i perioder med høy solaktivitet. Disse forholdene gjør det nødvendig med tiltak på brukersiden. Under meteoroideskurer velger derfor satellittoperatører å redusere den eksponerte flaten ved å reposisjonere satellittenes solpaneler.

Boks 12.1 Romvær

Kraftige solstormer kan gi stråling mot jorden, noe som kan ødelegge elektronikken i satellitter. De kan også gi forstyrrelser i ionosfæren og i magnetfeltet som kan påvirke kvaliteten på trådløs kommunikasjon og navigasjon. I forbindelse med solflekkmaksimum i 2013/2014 har solstorm med påfølgende geomagnetisk storm her på jorden vært et av momentene i det nasjonale risikobildet hos DSB de siste årene.

Kartverket har en sanntidstjeneste for varsling av brukerne av presisjonsnavigasjon når det registreres geomagnetiske stormer. På samme måte varsles mange oljeselskaper fra Romværsenteret ved Tromsø Geofysiske Observatorium når det er geomagnetiske forstyrrelser som kan påvirke horisontale boreoperasjoner offshore.

12.4.4 Menneskelig svikt

Menneskelig svikt kan også utgjøre en trussel mot drifts- og støttesystemer. Skader og ulykker kan eksempelvis inntreffe ved operatørfeil eller når brukere har mangelfull innsikt i begrensninger og muligheter ved bruk av satellittmottakerutstyr.

Interferens kan, som nevnt ovenfor, forekomme som følge av både tilsiktede og utilsiktede hendelser. Utilsiktet interferens kan eksempelvis inntreffe når signaler fra andre radiotjenester forstyrrer eller blokkerer mottak av satellittsignaler. Slike forstyrrelser kan oppstå dersom annet radioutstyr sender på de samme eller nær frekvensene som benyttes for satellittsignalene.[6]

12.4.5 Restsårbarhet og redundans

Selv om det stadig arbeides med å øke sikkerheten i systemene, i tjenester og i brukerutstyret, er det et sterkt behov for økt bevissthet og kjennskap til risikofaktorene hos brukere når det gjelder avhengighet og sårbarhet. Sektorbaserte og bedriftsinterne risikoanalyser for å iverksette relevante og kosteffektive sårbarhetsreduserende tiltak, er relevant i så måte.

Satellittbaserte systemer vil i flere sammenhenger kunne benyttes for å gi redundans til bakkebaserte løsninger. Samtidig vil det være tilfeller der det motsatte er aktuelt.

Når det gjelder satellittnavigasjonssystemer, vil ulike bakkebaserte metoder kunne gi redundans. De ulike metodene har forskjellige sterke og svake sider, og det kan være en utfordring å finne en bakkebasert løsning som dekker behovene i alle brukersegmenter. Dessuten eksisterer det også sårbarheter knyttet til de bakkebaserte løsningene.

---

6 Norsk romsenter (2013): *Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur.*

Eksempler på systemer som kan benyttes som redundans for forskjellige typer PNT-tjenester som nå leveres over satellitt, er radarsystemer, VHF Omnidirectional range (VOR) and distance measuring equipment (DME), Wide Area Multilateration (WAM), eLoran og digitalt bakkenett kombinert med atomklokker. Det digitale bakkenettet med tilhørende sendere er godt utbygd og meget godt egnet for å distribuere tid fra atomklokker. Å utnytte dette nettverket kan være kostnadseffektivt for å få opp en redundans i forhold til tidsanvendelser i kraftnett og nødnett, og for finansielle transaksjoner og andre anvendelser som har behov for presis tid.

Loran-C og eLoran

Med sin rekkevidde på 1 000–1 200 km over vann dekker Loran-C (Long Range Navigation System) store deler av norske havområder. I disse farvannene kan fartøyer som er utstyrt med Loran-C-mottakere, bruke systemet som et redundant radionavigasjonssystem. Imidlertid er bare et lite antall skip i dag utstyrt med Loran-C-mottaker. Regjeringen besluttet i 2013 at det ikke skulle bevilges midler til oppgradering til eLoran. Samtidig ble det klart at man ville legge ned Loran-C som tjeneste fra 1. januar 2016. Det er imidlertid flere som påpeker nødvendigheten av at systemet blir beholdt som en backup til satellittnavigasjonssystemer. Selv om det etter hvert kommer flere satellittbaserte PNT-plattformer, lider de prinsipielt av noen av de samme digitale sårbarhetene som eksempelvis sårbarhet for elektronisk jamming eller bruk av narresignaler (spoofing) som kan mislede brukeren. Et system som eLoran ville absolutt kunne representere et jammeresistent alternativ til GPS i områder med dekning, men det krever at det er brukere av systemet, og at det produseres mottakerutstyr i volumer som bygger opp under bruk. Avgjørelsen om nedleggelse av Loran-C uten oppgradering til eLoran er et godt eksempel på en avgjørelse som krever at interesser fra flere brukergrupper og sektorer blir belyst og tatt inn i en overordnet kost–nytte-analyse som er forankret i et realistisk trusselbilde. Lysneutvalget har ikke hatt grunnlag til å følge opp denne typen problemstillinger.

12.4.6 Bevissthet rundt sårbarhet og risiko

Det har vært en betydelig økning i bruken av rombaserte tjenester på en rekke samfunnsområder. Utviklingen har gått raskt, og det har i intervjuene kommet frem bekymringer knyttet til at aktørene som benytter seg av rombaserte tjenester, i for liten grad er bevisste på den avhengigheten og sårbarheten dette medfører.

Aktørene som er avhengige av rombaserte tjenester, gjennomfører i varierende grad egne sårbarhetsanalyser. Det synes å være stor forskjell på i hvilket omfang forskjellige sektorer har tatt innover seg dette nye risikobildet, både med hensyn til hvor omfattende bruken av rombaserte tjenester er, hvor avhengig man er av satellittnavigasjon, og i hvilken grad de skal forholde seg til bortfall og forstyrrelser.[7]

Dette understøttes av innspill som er kommet frem i intervjuer med sentrale aktører, der det blant annet etterlyses at myndighetsansvaret knyttet til blant annet følgende punkter bør tydeliggjøres:

- å vurdere risiko og sårbarhet
- å utarbeide tilstandsrapporter, initiere og gjennomføre nødvendige utredninger og foreslå tiltak
- å føre tilsyn med virksomheter opp mot gjeldende lovverk eller yte romfaglig bistand til eksisterende tilsynsmyndigheter
- å identifisere avhengigheter
- å sørge for kontakt mellom myndigheter – sektorovergripende «uavhengig» dialog
- å gi virkemidler til å regulere romvirksomheten
- å stille krav knyttet til bruk av rombaserte tjenester
- å etablere en helhetlig nasjonal romsikkerhetsstrategi

12.4.7 Sårbarheter knyttet til verdikjeder

Det finnes ingen overordnet myndighet som regulerer norsk romvirksomhet og de satellittbaserte tjenestene som samfunnet er avhengig av. At ansvaret er fordelt på flere ulike myndigheter, innebærer ikke nødvendigvis gråsoner uten ansvar eller sårbarheter knyttet til dette. Innenfor romvirksomheter er det imidlertid mange som påpeker at det fragmenterte ansvarsforholdet kan innebære en sårbarhet – ikke minst i tiden fremover, da satellittbaserte tjenester som innsatsfaktor for kritiske samfunnsfunksjoner blir enda mer sentralt.

Et eksempel er knyttet til å ivareta Svalbardkabelens funksjonalitet og sikkerhet. Samarbeidet med NASA og NOAA var utslagsgivende for at det ble lagt fiberkabel til Svalbard i 2004. I tillegg til operativ værvarsling og overvåking av atmosfæ-

[7] Ibid.

rens og havets tilstand driver NOAA en utstrakt forskningsvirksomhet. Blant annet har organisasjonen ansvaret for flere meteorologiske satellitter og måledata som kommer fra disse.

Kabelen må anses som en særdeles viktig del av den norske rominfrastrukturen. Den har i dag mange andre oppgaver for befolkningen på Svalbard og er kritisk for Svalbards kommunikasjonsløsninger med fastlandet. Svalbardkabelen er også kritisk med tanke på norske internasjonale forpliktelser.

Den tekniske sårbarheten i kabelforbindelsen knytter seg primært til feil i det digitale endeutstyret eller signalforsterkerne, svikt i kraftforsyningen og svikt i spenningsmatingen til signalforsterkerne. Den fysiske sårbarheten knytter seg primært til brann i lokaler som huser fiberrelatert utstyr, sabotasje, overgraving av kabelen på land og brudd i kabelen til sjøs som følge av fiskeriaktivitet, ras på sjøbunnen eller lignende.

Den samfunnsmessige sårbarheten knytter seg til det faktum at det ikke er andre muligheter for bredbåndet telekommunikasjon til Svalbard, bortsett fra meget begrensede og kostbare satellittforbindelser. I tillegg til de drøyt to tusen innbyggerne i Longyearbyen, Svea og Ny-Ålesund vil viktige institusjoner som Sysselmannen, Avinor og Longyearbyen sykehus bli sterkt skadelidende om kabelforbindelsen blir brutt. Norges internasjonale forpliktelser overfor for eksempel EU (Galileo) vil ikke kunne overholdes om kabelforbindelsen faller ut.

Deler av satellittinfrastrukturen på Svalbard er underlagt krav og tilsyn med hjemmel i sikkerhetsloven noe som innebærer at det skal beskyttes i henhold til de føringene som NSM gir. Space Norway påpeker imidlertid en stor utfordring knyttet til at det i dette regimet kun gis føringer for å vurdere beskyttelse mot tilsiktede hendelser, mens de største utfordringene og den største risikoen for forbindelsen er knyttet til utilsiktede hendelser. Det er videre en utfordring at objektsikkerhetsregimet bare ser på deler av en verdikjede, noe som gjør at sikkerhetstiltak som blir etablert, ikke vil ha tilstrekkelig effekt, siden kjeden ikke blir sikrere enn det svakeste leddet. De fysiske beskyttelsestiltakene som SPN kan iverksette for eksempel på Svalbardkabelen, er primært knyttet til ilandføring på Svalbard og i Harstad, og tar ikke høyde for sikkerheten videre. Fra enden av kabelen på Svalbard og videre inn til bebyggelsen er det andre aktører som har et ansvar, og det samme gjelder på fastlandet. Linjetermineringsutstyret som SPN eier, er plassert i lokaler som leies av andre aktører, og der andre har sikkerhetsansvaret.

Svalbardkabelen representerer et svært sentralt eksempel på verdikjeder innen satellittbaserte tjenester og hvordan ulike aktører og virksomheter er avhengige av hverandre. Utvalget ser det som en utfordring at det er flere andre eiere «utenfor kabelen» og i liten grad et ende-til-ende-fokus. En konsekvens av dette er at det ikke nødvendigvis stilles krav til sikkerhet som ivaretar et helhetlig sårbarhetsperspektiv.

Samtidig er det ingen overordnet myndighet som har et helhetsbilde av hvilke samfunnstjenester som er avhengige av kabelens funksjonalitet eller sørger for at alle hensyn blir ivaretatt ved for eksempel oppgradering, sikkerhetstiltak eller vedlikehold.

Hendelser som fører til brudd i kabelforbindelsen, berører ikke bare det nasjonale, også de internasjonale forpliktelsene Norge har, blir berørt ved en mulig svikt.

Kabelens levetid er anslått til 25 år – til 2029. Det er uklart om SPN som kabeleier vil ha eller kan ta ansvar for fornyelse av kabelforbindelsen eller ha økonomisk løftekraft til å gjøre det uten myndighetenes medvirkning.

Boks 12.2 Svalbardkabelen

I løpet av de siste fem årene har kabelforbindelsen blitt brutt to ganger: cirka 4,5 timer i juni 2014 og cirka 10 minutter i september 2014. Begge gangene skjedde det i forbindelse med oppgradering av endeutstyret i kabelen, og begge gangene som følge av svikt hos underleverandører som utførte selve oppgraderingsarbeidet. Det første bruddet fikk store konsekvenser for brukerne, blant annet måtte Svalbard lufthavn stanse all flytrafikk.

12.5 Vurderinger og tiltak

12.5.1 Tydeliggjøre myndighetsansvar for norsk romvirksomhet

De fleste samfunnsområder er i dag mer eller mindre avhengige av satellittbaserte tjenester, enten det er PNT, kommunikasjon, jordobservasjon eller annet. Myndighetsbildet knyttet til området er komplekst. Regulering av romvirksomheten er hjemlet i mange ulike lover og forskrifter, og ansvaret for oppfølging av romsektoren er desentralisert.

Det er grunn til å tro at ikke alle sårbarheter i et verdikjedeperspektiv er kjent og innkalkulert i eksisterende ROS-vurderinger og i forebyggende og beredskapsmessige tiltak som skal redusere sårbarheten i den enkelte sektor. Videre er det slik at den akkumulerte sårbarheten, knyttet enten direkte eller indirekte til bruk av satellittbaserte tjenester, ikke nødvendigvis samsvarer med summen av alle delbidragene. Uavhengig av om total avhengighet ikke samsvarer med summen av alle delbidragene, vil summen av sikringstiltak etter sin natur sjelden samsvare med et nødvendig sikringsnivå. Det synes derfor naturlig å vurdere om det bør være et myndighetsorgan som får særskilt ansvar for å følge opp satellittbaserte tjenester på nasjonalt, tverrsektorielt nivå. De fleste av aktørene som Lysneutvalget har vært i dialog med relatert til romvirksomhet, etterlyser større oppmerksomhet fra myndighetssiden på området – både når det gjelder overordnet regulering og krav til et sikkerhetsarbeid som evner å se helheten og bredden i dette komplekse feltet.

Videre er det tverrsektorielle avhengigheter som medfører et behov for samordning mellom sektorene. Problemdefinisjoner, virkemidler og tilskuddsordninger som er utviklet i én sektor, kan eksempelvis skape utilsiktede konsekvenser for måloppnåelsen i en annen sektor. Samtidig kan enkelte sektorer være avhengige av at andre sektorer medvirker, for å kunne nå sine mål. Koordineringen mellom myndighetsaktørene er imidlertid i liten grad formalisert. Det interdepartementale koordineringsutvalget har ikke selv beslutningsmyndighet, og utvalget synes også å kunne være sårbart overfor utskifting av nøkkelpersonell i de ulike departementene og etatene.

Utvalget anbefaler derfor at det blir tydeliggjort et myndighetsansvar for norsk romvirksomhet.

Behovet for tydeliggjøring av myndighetsansvaret for norsk romvirksomhet oppsummeres i følgende tre punkter:

Man bør
- øke bevisstheten rundt de ulike samfunnsområdenes sårbarheter og risiko knyttet til romvirksomhet
- identifisere avhengigheter og det samlede sårbarhetsbildet knyttet til romvirksomheten
- stille krav til og føre tilsyn med romvirksomheten

For å kunne utføre disse oppgavene må myndigheten som får ansvaret, tilføres kompetanse til å kunne utføre oppgavene. Myndigheten som får det overordnede ansvaret, trenger derfor en grunnleggende forståelse av romvirksomhet og generell innsikt på området, men ikke nødvendigvis på et teknisk nivå. Fokuset bør trolig være på sårbarhetsaspektet og hvordan sårbarheter kan reduseres. I tillegg vil det kunne være relevant med kompetanse på hvordan samfunnet skal håndtere en situasjon der rombaserte tjenester svikter. Til dette kreves kompetanse innen samfunnssikkerhet og beredskap.

Lysneutvalget ser det som formålstjenlig at det i første rekke opprettes en mindre enhet, bestående av fem stillinger, som får som oppgave å vurdere videre hva som per i dag eksisterer av retningslinjer, lover, regler og så videre for satellittbaserte tjenester, og deretter utleder hva som må etableres av nytt regelverk, retningslinjer, tilsynsbehov og andre reguleringsmekanismer. Kostnader knyttet til tiltaket vil utgjøre om lag 5,5 millioner kroner årlig.[8]

Basert på egne vurderinger og en utredning fra Oslo Economics anbefaler utvalget at ansvaret enten legges til Nkom eller til DSB. Utvalget mener det kreves en egen vurdering for å kunne beslutte hvilken av disse enhetene som skal ivareta dette ansvaret.

---

[8] For beregning av kostnader se *Konsekvensutredning – Tydeliggjøring av myndighetsansvar for norsk romvirksomhet.* Utarbeidet for Lysneutvalget, september 2015 Oslo Economics.

Kapittel 13
Energiforsyning

Svikt i forsyningen av elektrisk kraft får konsekvenser for alle samfunnssektorer og digitale systemer som samfunnet er avhengig av. I Norge er det høy leveringssikkerhet for elektrisk kraft. Samtidig er det umulig å garantere 100 prosent leveringssikkerhet.

Selskapene i energiforsyningen har i mange år benyttet IKT-systemer for å understøtte drift og for å overvåke og fjernstyre anleggene i energiforsyningen. Dette er i dag svært komplekse systemer, som omfatter selve driftskontrollsystemet (SCADA)[1], datanettverk for å føre signaler til og fra SCADA-systemet og ut til anleggene, stasjonsdatamaskiner og utstyr som oversetter digitale signaler til fysisk handling i stasjonene, samt nettverksutstyr som binder driftskontrollsystemet sammen. Inkludert i driftskontrollsystemet er også driftssentralene, der operatørene får sanntidsinformasjon om tilstanden i kraftsystemet og kan fjernstyre anleggene. Tidligere var dette helt særegne systemer som var helt uavhengige av andre IKT-systemer som virksomhetene benyttet. Systemene ble bygd for maksimal tilgjengelighet og integritet. Ivaretakelsen av konfidensialiteten var ikke prioritert, da systemene ikke hadde kontakt med omverdenen. I dag er situasjonen en helt annen.

IKT er i dag en integrert og svært viktig del av energiforsyningen for å kunne tilfredsstille samfunnets krav til effektiv drifts- og forsyningssikkerhet. For å oppnå dette har driftskontrollsystemene blitt knyttet stadig tettere opp mot tilgrensende systemer som for eksempel systemer for måling, avregning og fakturering, kundeinformasjonssystemer (KIS), nettinformasjonssystemer (NIS), geografiske informasjonssystemer (GIS) og kontorstøttesystemer.

Innføring av automatisk måling og avregning (AMS), som innebærer at alle strømkunder får installert en strømmåler med toveiskommunikasjon til nettselskapet, vil øke innslaget av IKT i virksomhetene betydelig. AMS vil gi nettselskapene langt bedre informasjon om status og tilstand i overføringsnettet og flere og mer effektive styringsverktøy. Samtidig er utrullingen av AMS med på å forsterke avhengigheten mellom energiforsyningen og ekomsektoren, som er sterk fra før. Selskapene benytter i stor grad tjenester fra kommersielle ekomtilbydere for å overføre signaler fra AMS-målerne og inn til nettselskapene.

Denne utviklingen har gjort at høy driftssikkerhet i energiforsyningen, herunder god IKT-sikkerhet, er blitt sentralt for samfunnet og bransjen.

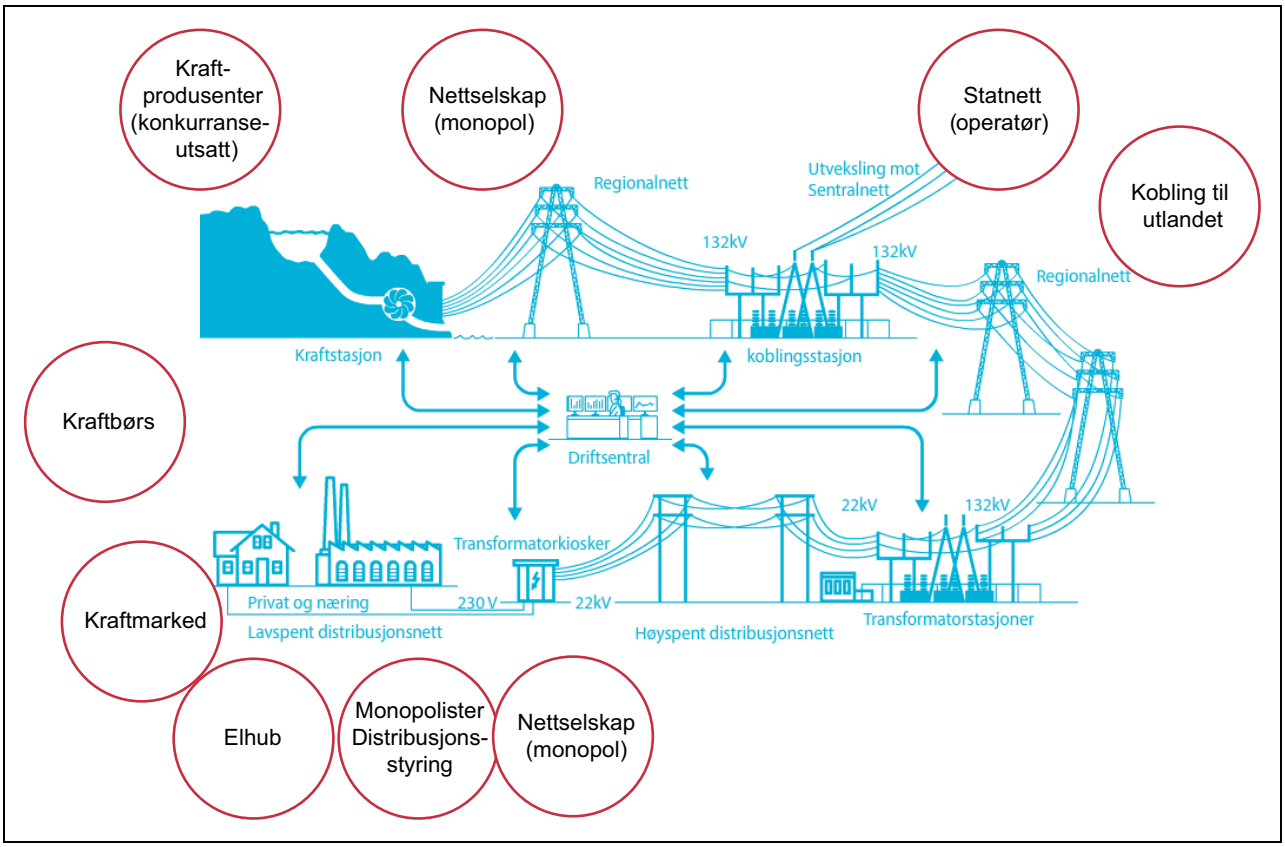
13.1 Kraftsystemet

Cirka 98,5 prosent av den norske elektrisitetsproduksjonen kommer fra vannkraftverk, hvorav den største delen er regulerbar. Levering av fjernvarme har økt vesentlig i omfang de senere årene. For helseinstitusjoner er dette av spesielt stor betydning gjennom hele året.

Kraftsystemet er et sammenhengende og komplekst system, og både utbygging og drift av de enkelte elementene må koordineres for at systemet skal fungere tilfredsstillende. Kraftsystemet er i stor grad redundant, og betydningen av det enkelte anlegget vil variere med revisjoner, nedbør, temperatur, årstid og tidspunkt på døgnet.

Kraftnettet deles inn i tre nettnivåer: sentral-, regional- og distribusjonsnett. Sentralnettet består i hovedsak av kraftledninger med 300 eller 420 kV spenning og knytter sammen forbrukere, produsenter og overføringsledninger til utlandet. Sentralnettet består i enkelte deler av landet også av kraftledninger med 132 kV spenning. Regionalnettene er bindeledd mellom sentralnettet og distribusjonsnettene. De mest utbredte spenningsnivåene i regionalnettene er 132 kV og 66 kV. Distribusjonsnettene sørger normalt for distribusjon av kraft til sluttbrukerne, som husholdninger, tjenesteytere og annen næringsvirksomhet. Store industrivirksomheter og kraftkrevende industri er

[1] For generell omtale av SCADA-systemer, se punkt 5.7 «Sikkerhet i prosesskontrollsystemer».



Figur 13.1 Kraftsystemet.

Kilde: Basert på Skagerak Energi.

koblet direkte på 132 kV- og 420 kV-nettet. Distribusjonsnettene har normalt en spenning på opptil 22 kV, men spenningen transformeres ned til 230 volt før den leveres til vanlige strømforbrukere.

Sentralnettet drives som en enhet med Statnett SF som operatør og dominerende eier (om lag 90 prosent). Det øvrige sentralnettet er fordelt mellom 20 eiere. Hafslund Nett AS, BKK Nett AS og SKL Nett AS har de største eierandelene. Underliggende nett har en variert eiersammensetning. Det er mange nettselskaper, og enkelte selskaper eier både deler av sentralnettet og regionalnett. Noen få av dem eier også distribusjonsnett.

Innkjøp av komponenter og teknologi til bruk i det norske kraftsystemet baseres på internasjonale standarder, for eksempel CENELEC og IEC, der utstyret godkjennes av nasjonale standardiserings- og kontrollorganer (NEK, Nemko). I tillegg er sentrale komponenter og utstyr som blir brukt i kraftsystemet, underlagt NVEs beredskapskrav, Justervesenets kvalitetskrav og DSBs forskriftskrav.

13.2 Roller og ansvar

Olje- og energidepartementet (OED) har det overordnede ansvaret for energiforsyningen. Samordningsinstruksen pålegger OED å ha oversikt over risiko og sårbarhet i egen sektor, herunder IKT-sikkerhet.

Norges vassdrags- og energidirektorat (NVE) har ansvar for å forvalte Norges vann- og energiressurser, og er beredskapsmyndighet for kraftforsyningen. NVE fører tilsyn med sikkerhet og beredskap med utgangspunkt i beredskapsforskriftens krav. Forvaltningen skjer gjennom regelverk og regelverksutvikling, veiledning og tilsyn, men også gjennom FoU.

Enhetene i Kraftforsyningens beredskapsorganisasjon (KBO) har en varslings- og rapporteringsplikt til NVE ved hendelser som truer sikkerheten. Alle selskaper som har konsesjon til å eie eller drive nett, kraftproduksjon eller fjernvarme, inngår automatisk i KBO. NVE følger i denne sammenheng opp de 200 KBO-enhetene innen nett, produksjon og fjernvarme. I tillegg utøves NVEs forvaltningsrolle gjennom ulike samvirkearenaer med bransjen og gjennom samarbeid med

andre myndigheter. NVE etablerte i 2013 Samvirke for infrastruktur, som er et beredskapsforum for myndigheter som har et fag- og/eller tilsynsansvar for infrastrukturer i Norge. Målsettingen er et effektivt samvirke mellom etater som ledd i en god og robust samfunnsberedskap. Beredskapsforumet er organisert som et likeverdig kollegium, og NVE ivaretar sekretariatrollen.

Statnett ivaretar både rollen som systemansvarlig og rollen som anleggseier. Som systemansvarlig for kraftsystemet har Statnett ansvar for å opprettholde den nordiske balansen mellom produksjon og forbruk og ivareta driftssikkerheten i kraftsystemet. Rollen som anleggseier av hoveddelen av sentralnettet innebærer å drifte om lag 1 000 km med høyspentlinjer og 150 stasjoner over hele landet. Driften overvåkes av én landsentral og tre regionsentraler.[2] Statnett har også ansvar for forbindelser til Sverige, Finland, Russland, Danmark og Nederland. Statnett er et statsforetak (SF) opprettet i henhold til statsforetaksloven og er eid av staten ved Olje- og energidepartementet.

Nord Pool er en kraftbørs som driver handel med og «clearing»[3] av fysiske og finansielle kraftkontrakter i Norden. Det er bare store aktører i kraftmarkedet som handler direkte på kraftbørsen Nord Pool eller gjennom bilaterale kraftkontrakter. Disse aktørene omfatter kraftprodusenter, kraftleverandører, tradere, meglere, større industribedrifter og andre større virksomheter.

Statkraft AS er den største kraftprodusenten i Norge og står for cirka 50 prosent av produksjonen. Statkraft er et ledende selskap innen vannkraft internasjonalt og Europas største produsent av fornybar kraft. Konsernet produserer vannkraft, vindkraft, gasskraft og fjernvarme og er en global markedsaktør innen energihandel. Statkraft AS er heleid av Statkraft SF, som igjen er heleid av staten ved Nærings- og fiskeridepartementet.

Flere nettselskaper har inngått kompetanse- og innkjøpssamarbeid, som skal ivareta eiernes interesser gjennom å etablere konkurransedyktige og attraktive fellestjenester. En undersøkelse gjort av NVE viser at 78 prosent av selskapene har inngått samarbeidsavtaler med andre nettselskaper om planlegging, innkjøp og installasjon av AMS-utstyr.[4] Behovet for samarbeid er også tidligere påpekt av Reiten-utvalget.[5]

Interesseorganisasjoner

Energi Norge er en interesse- og arbeidsgiverorganisasjon for norsk kraftnæring, og representerer 280 bedrifter innenfor området kraftproduksjon, kraftoverføring og salg av strøm og varme. Energi Norge har blant annet fokus på forsyningssikkerhet, nett, kraftmarkedet, kompetanse og andre problemstillinger av høy relevans for medlemmene. *KS Bedrift* organiserer over 500 kommunalt eide bedrifter i en rekke bransjer, deriblant kraftbransjen. *Distriktenes energiforening (Defo)* er opptatt av distriktspolitikk og kraftselskapenes rammebetingelser.

Forum for informasjonssikkerhet i kraftforsyningen (FSK) har 21 medlemsbedrifter blant de største kraftprodusentene og nettselskapene i Norge og skal arbeide med aktiviteter relatert til informasjonssikkerhet i kraftforsyningen slik dette er definert i NVEs beredskapsforskrift. FSK arrangerer faglige samlinger, utarbeider utredninger og felles veiledninger og rammeverk for informasjonssikkerhetsarbeid der slikt ikke finnes, og avklarer/påvirker myndighetskrav innen informasjonssikkerhet.

Kontaktutvalget for telesaker i Kraftforsyningen (KOTE) er et koordinerende organ for alle aktører innen ikke-kommersiell televirksomhet i elforsyningen i Norge. NVE har ikke fast plass i FSK og KOTE, men blir invitert til å holde innlegg eller diskutere særskilte tema innenfor IKT-sikkerhet.

Sivilt–militært samarbeid

Forsvaret er avhengig av pålitelig kraftforsyning for drift av administrative systemer spesielt. Innenfor beredskapsområdet er kraftforsyningsanlegg registrert på lister over objekter som skal beskyttes særskilt dersom en alvorlig krise / krig truer. Utover dette foregår det samarbeid gjennom Fylkesberedskapsrådet.

Forskning og utvikling

Energi Norge deltar i og koordinerer FoU-virksomhet innenfor kraftsektoren, eksempelvis pro-

---

2 Fra 1.9.2016 legges regionsentralen på Sunndalsøra ned, mens regionsentralene i Oslo og Alta består. Beslutningen ble tatt som en del av Statnetts arbeid med å styrke beredskapen og forsyningssikkerheten i kraftsystemet.

3 «Clearing» betyr at en tredjepart håndterer transaksjonen, og sikrer at kjøpers og selgers forpliktelser blir ivaretatt.

4 Norges vassdrags- og energidirektorat (2015): *Smarte målere (AMS). Status og planer for installasjon og oppstart per 1. kvartal 2015.*

5 Olje- og energidepartementet (2014): *Et bedre organisert strømnett* fra 2014.

sjekter knyttet til leveringskvalitet, driftssikkerhet og smartnett-løsninger. Gjennom NVEs økonomiske regulering av nettselskapene får selskapene mulighet til økte inntektsrammer ved å få godkjent egne FoU-prosjekter innen for eksempel IKT-sikkerhet. Flere prosjekter og søknader blant Energi Norges medlemmer er finansiert og igangsatt gjennom denne ordningen. NVE er i ferd med å vurdere et samarbeid med FFI om FoU-prosjekter innenfor temaet EMP-beskyttelse. Bransjen samarbeider allerede med akademia på en rekke områder, blant annet innenfor AMS, risikoanalyser og sårbarhetsindikatorer.

Internasjonalt samarbeid

NVE deltar blant annet i det nordiske samarbeidsorganet NordBER, der energimyndighetene og systemansvarlige selskaper i Norden samarbeider om beredskap og krisehåndtering innen elforsyningen. Kraftnettene i de nordiske landene er knyttet sammen og drives som ett sammenhengende system. Samarbeidet har bakgrunn i et uttrykt ønske fra nordiske energiministre om et forpliktende og samordnet arbeid for å sikre forsyningssikkerheten i Norden. I tilknytning til NordBER er det opprettet en undergruppe med representanter for myndighetene og systemansvarlige i Norden som samles for å diskutere felles utfordringer innen IKT-sikkerhet. NVE er med som observatør i EU-organet Agency for the Cooperation of Energy Regulators (ACER). Etter EU-kommisjonens syn foreligger det et regulatorisk hull blant annet i spørsmål om grensekryssende handel.

13.3 Hjemmelsgrunnlag, konsesjoner og tilsynsvirksomhet

Kraftforsyningen er regulert gjennom energiloven. Pålitelig forsyning av elektrisitet med riktig kvalitet (spenning og avbruddsfri forsyning) er regulert i forskriftsform. I tillegg er det etablert økonomiske incentiver som skal sørge for at nettselskaper inkluderer samfunnsøkonomiske kostnader ved redusert leveringspålitelighet i sine bedriftsøkonomiske beslutninger.

Forsyningssikkerhet for strøm er definert som «kraftsystemets evne til kontinuerlig å levere elektrisk kraft av en gitt kvalitet til sluttbrukere». Forsyningssikkerhet omfatter både energisikkerhet, effektsikkerhet og driftssikkerhet.[6]

Energiloven og beredskapsforskriften regulerer sikkerhet og beredskap innenfor kraftsystemet, herunder informasjonssikkerhet. Olje- og energidepartementet har revidert kapittelet om beredskap i energiloven.[7] NVE forvalter forskrifter som inneholder bestemmelser om beskyttelse av informasjon, IKT-sikkerhet og krav til kompetanse. Bestemmelsene omfatter både forebyggende, skadebegrensende og beredskapsmessige tiltak. Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften) skal sikre at energiforsyningen opprettholdes, og at normal forsyning gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner for å redusere de samfunnsmessige konsekvensene av strømutfall. I beredskapsforskriften stilles det blant annet strenge krav til risikovurderinger, tilgangskontroll og tilgang til systemene fra leverandører. I tillegg er kravene i forskriften differensiert, slik at de viktigste selskapene er underlagt de strengeste sikkerhetskravene.

Energiloven § 9-3 og kapittel 6 i beredskapsforskriften omfatter informasjonssikkerhet. Dette omfatter identifisering og håndtering av kraftsensitiv informasjon og opplysninger om energiforsyningen som kan brukes til å skade anlegg eller påvirke funksjoner som har betydning for energiforsyningen. Kapittel 7 i beredskapsforskriften omfatter krav til sikring av selskapenes driftskontrollsystemer, som er kritiske for å overvåke og styre energiforsyningen. Beredskapsforskriften har en omfattende veileder som gir selskapene ytterligere informasjon om hva som forventes for at kravene i forskriften skal være oppfylt.

NVE har ikke kjennskap til noen myndighet i noen andre land som har tilsvarende regelverk for beskyttelse av driftskontrollsystemer, men innen Norden ser de at særlig Finland er spesielt kompetent på IKT-sikkerhet i flere sektorer, også energiforsyningen.

Beredskapsforskriften pålegger enhetene i KBO en rekke krav for å beskytte sensitiv informasjon om kraftsystemet. Med sensitiv informa-

---

6 *Energisikkerhet* er definert som «kraftsystemets evne til å dekke energiforbruket». Energiknapphet eller svikt i energisikkerhet karakteriseres ved redusert produksjon av elektrisk energi som følge av mangel på primærenergi (vann, gass, kull etc.). *Effektsikkerhet* defineres som «kraftsystemets evne til å dekke momentan belastning» og karakteriseres ved tilgjengelig kapasitet i installert kraftproduksjon eller i kraftnettet. *Driftssikkerhet* defineres som «kraftsystemets evne til å motstå driftsforstyrrelser uten at gitte grenser blir overskredet».

7 Se Prop. 112 L (2010–2011) om endringer i energiloven. Dagens kapittel 9 i energiloven omhandler beredskap, og § 9-3 omhandler informasjonssikkerhet. Her sies det at enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen.

sjon menes informasjon som kan benyttes til å skade energiforsyningen. Hva som er sensitiv informasjon, er klargjort i § 6-2.

Enheter i KBO som setter ut oppdrag til leverandører og andre, skal påse at disse etterlever bestemmelsene om informasjonssikkerhet og taushetsplikt for sensitiv informasjon. Det skal også opplyses i avtale at beredskapsmyndigheten kan føre tilsyn med etterlevelsen av disse bestemmelsene, jf. beredskapsforskriften § 6-5.

Et annet krav i beredskapsforskriften er beskyttelse og beredskap mot elektromagnetisk puls (EMP). EMP kan i ytterste fall slå ut elektronikk over et stort område, men også et avgrenset område, for eksempel i et enkelt anlegg. Norge er det eneste landet som har krav til EMP-beskyttelse i energiforsyningen.

Forskrift om leveringskvalitet regulerer kvaliteten og stabiliteten på levert energi og effekt til sluttkundene. Forskriften skal bidra til å sikre en tilfredsstillende leveringskvalitet i det norske kraftsystemet og en samfunnsmessig rasjonell drift, utbygging og utvikling av kraftsystemet. Leveringskvalitetsforskriften presiserer blant annet nettselskapenes plikt til å gjenopprette elektrisitetsforsyningen til nettkundene så raskt som mulig etter et avbrudd, og det er gitt konkrete grenseverdier for enkelte parametre på spenningskvalitet i kraftsystemet.

I kontrollforskriften inngår et element som skal sørge for at nettselskapene tar hensyn til samfunnets kostnader knyttet til leveringspåliteligheten i kraftnettet, KILE (kvalitetsjusterte inntektsrammer ved ikke levert energi). KILE-ordningen er en incentivregulering som skal gi nettselskapene økonomisk motivasjon til riktig ressursallokering innenfor de rammene og vilkårene som ellers er gitt av myndighetene. KILE inngår i selskapets inntektsramme som en del av selskapets kostnadsgrunnlag og normkostnad på samme måte som andre kostnader. Faktisk KILE i et gitt år kommer til fratrekk i selskapets inntektsramme, slik at selskapets tillatte inntekt reduseres som følge av avbrudd (ikke levert energi).

Avregningsforskriften pålegger aktører i kraftsektoren en rekke plikter for å legge til rette for et effektivt kraftmarked. Flere av disse pliktene gjelder for nettselskap og er innført på grunn av at nettselskapene ellers ikke ville utført dem, da de ikke er bedriftsøkonomisk lønnsomme. I denne forskriften er det også krav til måling av innmating og uttak fra nettet, herunder kravene til AMS.

13.3.1 Konsesjoner

Utbygging av nettanlegg med høyt spenningsnivå, det vil si regional- og sentralnett, trenger anleggskonsesjon etter energiloven. Søknader om bygging og drift av kraftledninger, transformatorstasjoner og andre elektriske anlegg i sentral- og regionalnettet behandles av NVE. Driftskontrollsystemer er ikke underlagt konsesjonsplikt, men selskapene som etablerer eller i vesentlig grad endrer omfanget av driftskontrollsystemet, har ifølge beredskapsforskriften § 5-9 plikt til å melde fra om dette. NVE fastsetter gjennom enkeltvedtak sikringsklasse på driftskontrollsystemet i de høyeste klassene. NVE kan også i særskilte tilfeller forby bruk av utstyr i driftskontrollsystemer, jf. beredskapsforskriften § 7-6.

NVE hadde tidligere et sterkt virkemiddel i kompetanseforskriften som stilte krav til egenbemanning. Reiten-utvalget konkluderte med at dette kravet kunne være konkurransevridende, og kompetanseforskriften er nå opphevet, slik at det i større grad skal være mulighet for samarbeid og bortsetting av tjenester til tredjepart. Krav til kompetanse vil nå bli lagt inn i energilovforskriften.

13.3.2 Tilsyn

NVE fører tilsyn med kraftforsyningsanlegg, og det gjennomføres både stedlige og skriftlige tilsyn. NVE har i tillegg hjemmel til å føre uanmeldte tilsyn, men dette benyttes ikke ofte. I 2015 har NVE planlagt 90 tilsyn, inkludert skriftlige tilsyn. Av NVEs tilsyn i 2014 ble ett gjennomført i samarbeid med Nkom.

Tilsynsobjektene blir valgt ut blant annet på grunnlag av hvilken betydning de har for kraftsystemet, og tidligere gjennomførte tilsyn. De siste årene har NVE i stadig større grad prioritert tilsyn med selskapenes driftskontrollsystemer. Bakgrunnen for dette er den økte trusselsituasjonen. Tilsyn med selskapenes driftskontrollsystemer er de mest omfattende og gjennomføres som regel over to dager. Ettersom evnen til å håndtere IKT-hendelser er vesentlig, gjennomførte NVE i 2015 et større skriftlig tilsyn der kravene til overvåking og logging av datatrafikk var tema.

Av NVEs egen database går det frem at omtrent alle selskaper der det ble ført tilsyn med informasjonssikkerhet, fikk avvik. Tabell 13.1 viser avvik i forhold til beredskapsforskriften § 6 om informasjonssikkerhet og § 7 om beskyttelse av driftskontrollsystemer.

Tabell 13.1 NVEs tilsynsfunn

År	Antall selskap	Avvik beredskaps-forskriften kap. 6	Avvik beredskaps-forskriften kap. 7
2013	28	6	18
2014	22	12	12

De fleste funnene etter tilsynene omhandler mangler ved ROS-analyser og hvordan disse kobles mot beredskapsplanverket. Dokumentasjonen, særlig av kobling mellom nettverk i driftskontrollsystemer og andre nettverk, er ofte mangelfull. Det er også mangelfull dokumentasjon av avtaler og retningslinjer rundt kontroll med fjerntilgang til systemene i driftskontrollsystemene. Videre har NVE påpekt at det må øves mer på å håndtere IKT-hendelser.

NVE har ikke hjemmel i lovverket til å føre direkte tilsyn med leverandører til virksomheter, men lovverket pålegger enhetene i KBO å kontraktfeste at beredskapsmyndigheten kan føre tilsyn med leverandøren (jf. beredskapsforskriften § 6-5). I tillegg stilles det krav om at det skal inngås sikkerhetsavtale mellom leverandøren og NVE eller en enhet i KBO for at leverandøren skal få tilgang til sensitiv informasjon (jf. beredskapsforskriften § 4-3). NVE kan imidlertid vedta at virksomheter som leverer varer eller utfører tjenester, eller andre som kan ha betydning for kraftforsyningens drift og sikkerhet, skal inngå i KBO (beredskapsforskriften § 2-2).

Hendelsesbaserte tilsyn benyttes også som virkemiddel av NVE. Disse utløses av selskapenes innrapporterte hendelser, jf. rapporteringsplikten. Et eksempel er tilsyn etter at et selskap meldte fra om en hendelse der årsaken var manglende endringshåndtering.

13.4 Beredskap og hendelseshåndtering

NVE er delegert beredskapsmyndighet av OED. NVE har ansvaret for å samordne energiforsyningens beredskapsplanlegging og skal lede landets energiforsyning ved nasjonal beredskap og i store ekstraordinære hendelser. For dette formålet er det etablert en landsomfattende organisasjon – Kraftforsyningens beredskapsorganisasjon (KBO), som består av NVE og de virksomhetene som står for kraftforsyningen.

Statnett har fullmakt til å sette i verk tiltak for å balansere forbruk og tilbud på effekt. Ved større utfall som skaper effektknapphet, kan Statnett koble ut forbruk for å opprettholde balansen i kraftsystemet. Ved langvarig energiknapphet kan OED iverksette tiltak etter råd fra NVE.

Det viktigste grunnlaget for god evne til å håndtere hendelser ligger hos selskapene. Alle selskapene i energiforsyningen har en selvstendig plikt til å sørge for effektiv sikring og beredskap og til å iverksette tiltak for å forebygge, begrense og håndtere virkningene av ekstraordinære situasjoner. Alle kriser skal i utgangspunktet håndteres på lavest mulig nivå. Dette følger av ansvarsprinsippet. Selskapene i energiforsyningen har imidlertid en varslings- og rapporteringsplikt til NVE ved hendelser som truer sikkerheten.

Etter hvert som truslene mot IKT-systemene har økt, har NVE prioritert arbeidet med IKT-sikkerhet. Eksempler på dette er den siste revisjonen av beredskapsforskriften, flere tilsyn med driftskontrollsystemer, dialog og veiledning. På lik linje med krav om å kunne håndtere utfall ved uvær eller teknisk svikt skal KBO-enhetene ha evne til å håndtere IKT-hendelser. Beredskapsforskriften stiller for eksempel krav om at selskapene skal ha en ordning for hendelseshåndtering av sikkerhetstruende hendelser i driftskontrollsystemet. Undersøkelser gjort i en doktorgradsstudie ved NTNU viste imidlertid at selskapene som var med i studien, ikke hadde tilstrekkelige deteksjonsmekanismer, og at det av ressursmessige årsaker ikke er en systematisk tilnærming til oppfølging av logger og varsler.[8]

KraftCERT

Med økningen i IKT-trusselnivået og IKT-kompleksiteten innså NVE og bransjen at det var behov for å etablere et kompetansemiljø som kunne gi råd og bistå selskapene ved større IKT-hendelser. KraftCERT AS ble da etablert med Statnett, Statkraft og Hafslund Nett som eiere i november 2014. Selskapet skal bistå medlemmer innenfor kraftbransjen i Norge med håndtering og forebygging av angrep på selskapenes IKT-

[8] Line, Maria Bartnes (2015): *Understanding Information Security Incident Management Practices – A case study in the electric power industry.* NTNU.

systemer. KraftCERT hadde medio 2015 13 store medlemmer, inkludert Hafslund, Statnett og Statkraft, og har samlet mange av de mindre kraftselskapene under NC-Spectrum og via KS-bedrift. Noen av de små selskapene leverer tjenester innen vann og avløp, men bruker de samme IKT-leverandørene som kraftbransjen. De har derfor funnet det hensiktsmessig også å være med i KraftCERT-samarbeidet.

KraftCERT ser at det kan bli en utfordring å få kraftselskapene med, blant annet fordi enkelte synes medlemsavgiften er høy. KraftCERT samarbeider med sektor-CERT-er og andre relevante aktører både nasjonalt og internasjonalt, deriblant ICS-CERT og JPCERT (ICS). I Japan, USA, Østerrike, Sverige og Finland har energisektorens miljøer for hendelseshåndtering tung statlig støtte i form av midler og tilknytning til de nasjonale ressursene.

Energi Norge mener det er viktig å støtte opp om og videreutvikle det initiativet som er tatt ved etableringen av KraftCERT. Dette bør skje i nær dialog med NVEs forvaltning av beredskap i kraftforsyningen og øvrige sentrale sikkerhetsmyndigheter.

Naturhendelser er fortsatt det som fører til flest avbrudd og blackout, og dette gir seg utslag i statistikken. Eksempelvis gjenfinner vi omfattende avbrudd som følge av ekstremvær som Dagmar i 2011 i avbruddsstatistikken. For nærmere omtale av Dagmar, se kapittel 11 «Elektronisk kommunikasjon».

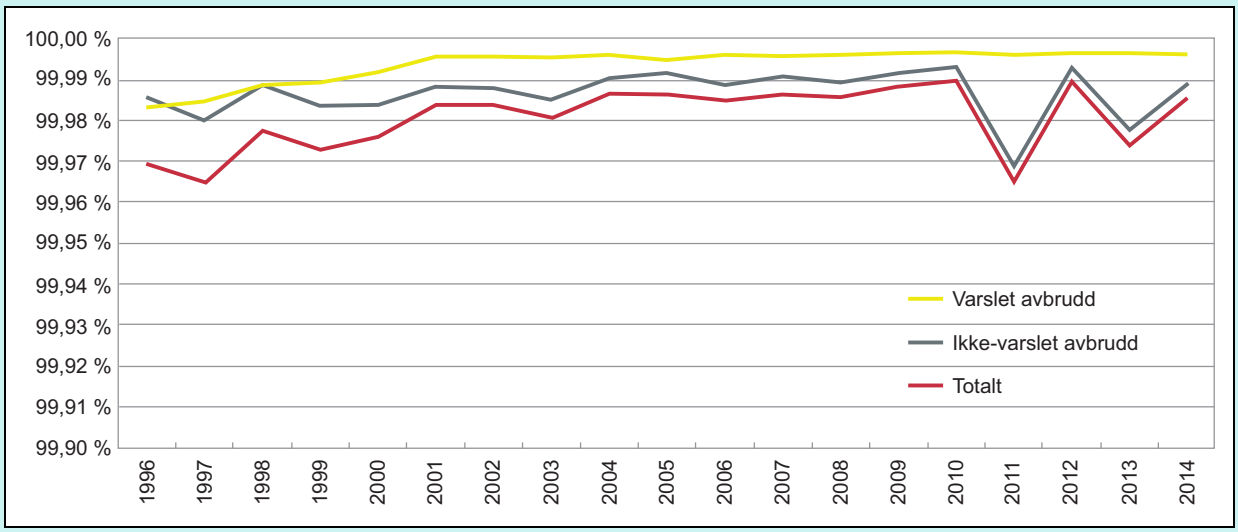
IKT-hendelser i energiforsyningen

NVE har god statistikk over avbrudd der årsaken er teknisk svikt eller uvær. Det finnes ikke noen tilsvarende nasjonal statistikk over tid når det gjelder IKT-sikkerhetsrelaterte hendelser. Det er ventet at dette bildet blir bedre med etableringen av KraftCERT. I USA viser statistikken til den amerikanske ICS-CERT at hele 87 prosent av de identifiserte sårbarhetene i driftskontrollsystemer kunne utnyttes via fjerntilgang, mens de resterende trengte lokal tilgang. Nesten 65 prosent av sårbarhetene ble av eierne av systemene klassifisert som høyprioritetssårbarheter. To kjente driftskontrollangrep som kan karakteriseres som digital sabotasje, er Stuxnet og angrepet mot et tysk stålverk i 2015. Angrep som Havex og Dragonfly viser også at det foregår spionasje og etterretningskampanjer mot energisektoren.

Energi Norge påpeker at NVE har hatt økende oppmerksomhet på IKT-sikkerhet og på utfordringer knyttet til skytjenester, oppdagelse og logging

Boks 13.1 Uvær forårsaker fortsatt mest utfall

NVEs avbruddsstatistikk gir et samlet bilde av forsyningssikkerheten på elkraft. I Norge skyldes mer enn 50 prosent av avbruddene været. Leveringspåliteligheten i 2014 for hele landet var 99,985 prosent.



Figur 13.2 Leveringspålitelighet 1996–2014.

Kilde: NVE.

Boks 13.2 Havex utnyttet menneskelig sårbarhet

Skadevaren Havex, som ble rapportert av ICS-CERT i juni 2014, er en fjernstyringstrojaner som angriper leverandører via phishing-angrep (e-post), omdirigering til infiserte nettsider og ved å infisere gjennom regulære programvareoppdateringer. Den siste måten å angripe på, via programvareoppdateringer, er bekymringsfull, da oppdatering av programvare er et av de viktige sikkerhetstiltakene og angrep mot dette kan undergrave tilliten til oppdateringer.

Havex kommuniserer med en kommando- og kontrollserver. Havex samler inn informasjon om systemet og nettverket den har infisert, og kan sende data tilbake inn i det infiserte systemet, noe som har medført at systemer har brutt sammen.

Analyse av angrep og skadevare hadde ikke vært mulig uten logger som dokumenterer hendelser i systemet. NVE vil fremover se på prinsipper for logging – oppbevaringstid, hvordan man kan gå frem for å søke i logger, med videre. Det kan bli vurdert å utvide krav om logging for selskaper med driftskontrollsystemer i klasse 1.

av unormal og uønsket datatrafikk. Bransjen er blitt bedre til å stille krav til leverandører, til å varsle om hendelser til NVE og til å samarbeide på tvers av selskaper for å bedre IKT-sikkerheten. Til det siste punktet kommer også forskningssamarbeid innenfor hendelsesidentifikasjon og -håndtering.

Øvelser

Øvelser gir gode muligheter for å avdekke sårbarheter, og de bedrer grunnlaget for å håndtere reelle hendelser. Selskapene i energiforsyningen har gjennomført beredskapsøvelser i en årrekke, men i liten grad inkludert IKT-hendelser. De viktigste forbedringspunktene etter øvelsene har i stor grad gått ut på å forbedre beredskapsplanverket, prosedyrer og rutiner, samt internt samarbeid mellom ulike funksjoner.

Etter hendelsene sommeren 2014, der NSM offentlig advarte om et storstilt angrep mot norsk energisektor, har bransjen etter påtrykk fra NVE i større grad gjennomført beredskapsøvelser som inkluderer IKT-hendelser. Frem til nå har ingen norske selskaper vært utsatt for målrettede angrep mot sine driftskontrollsystemer, derfor er denne typen øvelser nyttig for selskapene for å avdekke svakheter i beredskapen og forbedre denne.

13.5 Digitale sårbarheter i kraftforsyningen

Den økte digitaliseringen i energiforsyningen og den stadig tettere sammenkoblingen av systemer og nettverk har medført at de totale systemene blir mer komplekse, og det kan være vanskelig å ha full oversikt. Dette kan igjen medføre at man ikke har god nok kunnskap om hvordan samhandlingen mellom systemene fungerer, noe som kan føre til feil bruk.

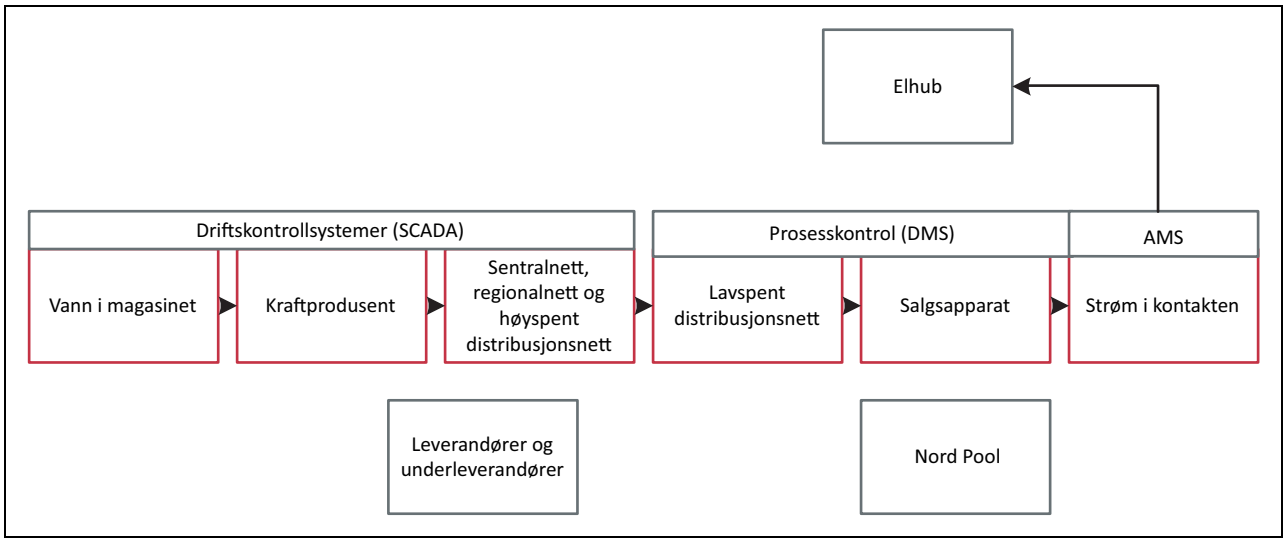
Dette øker risikoen for teknisk feil, menneskelig svikt og også for uautorisert inntrenging i systemene.

Nasjonale kraftsystemer og markeder integreres dessuten i økende grad på tvers av landegrensene. Stadig flere strømkabler knytter Norge tettere sammen med resten av Europa, og kraftmarkedene vil etter hvert smelte sammen til ett stort europeisk marked. Sentrale problemstillinger som diskuteres internasjonalt er krav til SCADA- og AMS-sikkerhet, krav til godkjenning av systemer og krav til sertifisering.

13.5.1 Verdikjeden i norsk kraftforsyning

Produksjon og forbruk av elektrisitet må til enhver tid være synkronisert for å unngå teknisk ubalanse i kraftnettet. IKT-systemer understøtter denne balansen, og digitale sårbarheter kan oppstå i alle ledd i verdikjeden, herunder hos underleverandører og kraftbørsen Nord Pool Spot. Alvorlig svikt vil derfor kunne påvirke forsyningssikkerheten negativt. NVE har oversikt over forsyningssikkerheten i regional- og sentralnett gjennom ordningen med kraftsystemutredninger og ga i 2014 ut en rapport som sammenstiller data fra alle de regionale kraftsystemutredningene. Det er 467 punkter i regionalnettet og 312 i sentralnettet som har redusert forsyningssikkerhet i henhold til å tåle en feiltilstand.

Verdikjeden i kraftforsyningen har frem til nå blitt overvåket og styrt av driftskontrollsystemer for henholdsvis produksjonsanlegg, sentralnettnivå, regionalnettnivå og høyspent distribusjonsnivå. Etter utrullingen av smarte målere vil mange selskaper også vurdere å etablere overvåking og styring på lavere distribusjonsnettnivå.



Figur 13.3 Verdikjeden i norsk kraftforsyning.

Figur 13.3 er en forenklet fremstilling av verdikjeden i norsk kraftforsyning, fra vann i magasinet til strøm i kontakten.

13.5.2 Sårbarheter i driftskontrollsystemer

Driftskontrollsystemer har som tidligere beskrevet omfattende krav til sikring. De fleste nettselskaper har et eget driftskontrollsystem med reserveløsning i en eller annen form, og flere selskaper samarbeider også om felles løsninger og beredskap.

SCADA-systemer og administrative IKT-systemer har generelt ulike sikkerhetsbehov.[9] ENISA har pekt på utfordringene med å lage et felles sikkerhetsregime og en felles sikkerhetsarkitektur når SCADA-systemer kobles sammen med administrative IKT-systemer.[10]

De viktigste selskapene i Norge har krav til redundant kommunikasjon i driftskontrollsystemet, slik at feil i én kommunikasjonslinje ikke medfører funksjonssvikt.

Økt tilgang fra Internett – også fra utlandet

For driftskontrollsystemene er tilgjengelighet og integritet det mest sentrale. De største driftskontrollsystemene er omfattende og i stor grad spesialtilpasset det enkelte selskapets behov, og det kan være flere leverandører som leverer ulike deler av det totale driftskontrollsystemet.

Den økte kompleksiteten og økte krav til forsyningssikkerhet har gjort at selskapene har blitt mer avhengige av leverandører til vedlikehold og feilretting via fjernaksess. Selskapene har i større grad også tilrettelagt for overvåking og styring av anleggene via fjernaksess.

Driftskontrollsystemene var opprinnelig ikke utviklet med tanke på sikkerhet, noe som har ført til et omfattende og kostbart arbeid med å sikre systemene mot uautorisert tilgang etter hvert som systemene i stadig større grad har blitt koblet til andre IKT-systemer og mot Internett. Dette innebærer også å etablere en moderne arkitektur i nettverket i driftskontrollsystemet som bidrar til større kontroll med trafikken i nettverket.

Et annet eksempel på utfordringer er bruk av antivirusprogramvare eller systemer for overvåking av datatrafikk på SCADA-systemer. I eldre systemer er bruken av disse problematisk fordi risikoen er stor for at disse systemene forstyrrer, forsinker eller stopper lovlig og nødvendig datatrafikk.

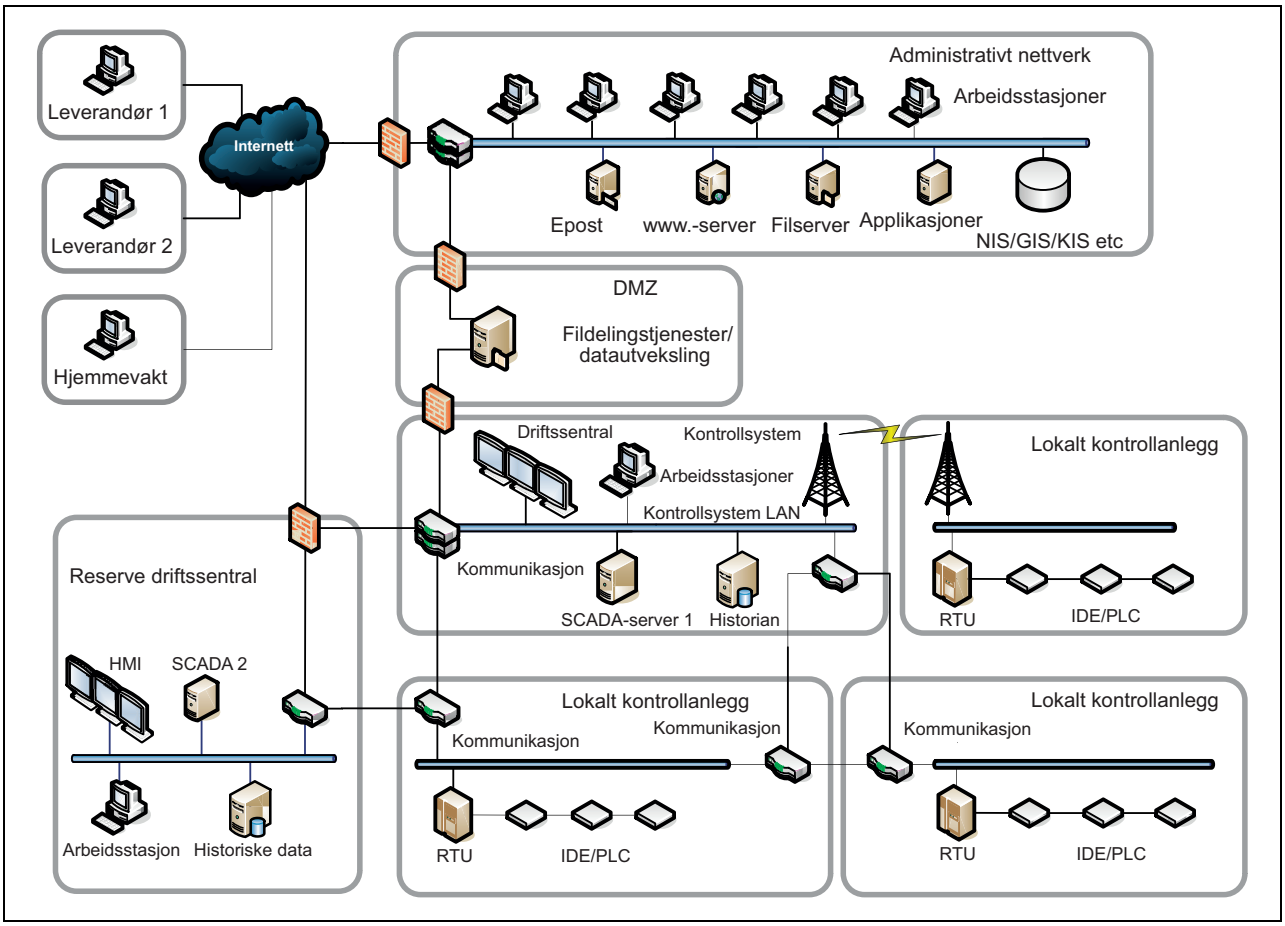
I tillegg er kravet til tilgjengelighet så stort at det krever omfattende arbeid og forberedelser når det skal installeres oppdateringer, for å sikre seg mot at oppdateringene ikke fører til nedetid i systemene. Det økte trusselbildet har også utfordret selskapene med hensyn til sikkerhetskompetanse.

Alt dette kan medføre at selskapene blir mer avhengige av leverandørene for raskest mulig gjenoppretting ved omfattende systemfeil. Samtidig er trenden at flere store leverandører i større grad satser på å utføre supporttjenester fra utlandet. Det kan by på utfordringer i forhold til bered-

---

9 Weiss, Joseph (2010): *Protecting Industrial Control Systems from Electronic Threats.* Momentum Press. New York.

10 ENISA (2012): *Smart Grid Security – Annex I General Concepts and Dependencies with ICT.*



Figur 13.4 Forenklet illustrasjon som viser hvordan driftskontrollsystem og administrativt nett er tilknyttet Internett.

Kilde: NVE.

skapsforskriftens krav til beskyttelse av sensitiv informasjon og kontroll med egne data. NVEs regulering krever at fjernaksesstjenester leveres i kontrollerte former.

Konsentrasjonsrisiko i leverandørleddet

Enkeltleverandører av SCADA-systemer har store markedsandeler i Norge. Det kan føre til at feil i kjernesystemet fra én stor leverandør påvirker flere selskaper i energiforsyningen. Dette er også en problemstilling som drøftes i kapittel 11 «Elektronisk kommunikasjon».

Det er viktig å hindre at uvedkommende får tilgang til sensitive opplysninger om kraftforsyningen i landet, og å sørge for oppetid for systemer som ivaretar viktige driftskontrollfunksjoner. Sensitiv informasjon om kraftforsyningen vil være informasjon som, i gale hender, kan brukes til å skade eller hindre funksjoner i kraftforsyningen.

Analysen av Stuxnet-angrepet viser at tradisjonelle beskyttelsestiltak som holdningskampanjer, sikkerhetsoppdateringer og antivirusbeskyttelse har liten effekt på denne typen sofistikerte angrep. Data fra Open Source Vulnerability Database (OSVDB) viser at Stuxnet førte til økt oppmerksomhet rundt sårbarheter i industrikontrollsystemer. Av det totale antallet kjente sårbarheter ble i følge ICS-CERT hele 80 prosent oppdaget i tiden etter Stuxnet.

Kostbart å oppgradere

Dagens SCADA-system og stasjonsdatamaskiner utvikles på moderne programvareplattformer der også sikkerhetsmekanismer er mer integrert i systemene. Men å modernisere SCADA-systemer og implementere moderne nettverksteknologi er svært kostbart og arbeidskrevende, og det tar gjerne fra ett til tre år å gjennomføre, avhengig av hvor omfattende driftskontrollsystemet er. Selskapet gjør da dette stegvis, og det betyr at det fremdeles er en god del eldre systemer og komponenter i driftskontrollsystemene i energiforsyningen. Dette innebærer at proprietære og sårbare protokoller fremdeles benyttes, og at det finnes utstyr

Boks 13.3 Stuxnet

Stuxnet fikk i 2007 det iranske atomprogrammet til å stoppe midlertidig ved at et prosesskontrollsystem i et atomanlegg i Natanz (Iran) ble angrepet av skadevare. Dataviruset skal ha ødelagt omtrent 1 000 av Irans 6 000 uransentrifuger.[1]

Iransk atomindustri hadde en gammel, upålitelig prosessteknologi og hadde implementert systemer som bidro til høyere feiltoleranse enn det som var vanlig for slike anlegg. Operatørene var dermed vant til feilsituasjoner. Teknologien i anlegget stammet fra pakistansk atomindustri på 1970–1980-tallet.

En teknisk analyse av Stuxnet-angrepet (Lagner, 2013) viser at begge angrepene mot anlegget i Natanz hadde som mål å ødelegge sentrifugene. Men taktikken var forskjellig. Det første angrepet, som skjedde skjult, hadde som mål å øke overtrykket i sentrifugene. Det andre angrepet hadde som mål å manipulere hastigheten på sentrifugerotorene og på den måten få dem til å spinne med for høy hastighet og ødelegge dem. Skadevare ble fraktet inn i anlegget og la seg som et «man-in-the-middle-angrep». Det overstyrte dermed operatørene. Dataviruset skapte i egenskap av trusselen bekymring også i norsk kraftindustri.

[1] Lagner, Ralph (2014): *To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve.*

ute i anleggene som ikke har innebygd sikkerhetsfunksjonalitet.

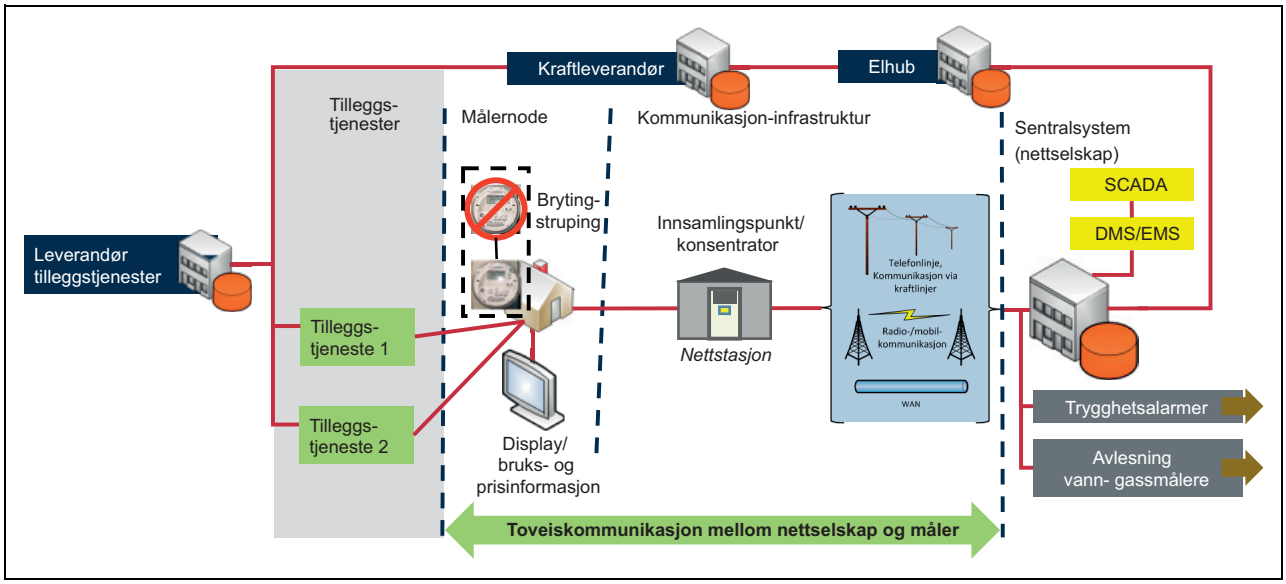
13.5.3 Sårbarheter i tilknytning til smarte nett

NVE har pålagt alle nettselskapene å innføre strømmålere med toveiskommunikasjon (AMS) innen 1. januar 2019 for sluttbrukere. Dette vil gjøre strømforsyningen sikrere og mer stabil, eksempelvis ved å lokalisere og reparere feil raskere enn før, men det vil også kunne øke den digitale sårbarheten.

Måleren er nettselskapets eiendom, og det er selskapets ansvar å beskytte den. Målerne er plassert i private bygg, og etter den nye NEK-normen[11] skal målere til nye bygg plasseres utendørs på vegg og i felles skap med ekom.

Gjennom innføringen av AMS vil strømkunder i Norge få registrert strømforbruket sitt med en oppløsning på en time eller mindre. Datainnsamling og styring av målere skjer gjennom løsninger som er designet for automatiserte prosesser samt overvåking av drift og feilsituasjoner i strømnettet. Utover ren innsamling av måleverdier samler systemet inn data rundt hendelser i strømmålerne, kommunikasjonen eller elnettet. Gjennom dette vil nettselskapene ha mulighet til å motta data av sterkt forbedret kvalitet, noe som vil gi et

[11] Norsk elektroteknisk norm – NEK 399-1 2014 *Tilknytningspunkt for el- og ekomnett.* Normen omhandler etablering og utforming av felles grensesnitt (skap) for blant annet elnett, elmåler og ekomnett.



Figur 13.5 Eksempel på AMS-system.

Kilde: NVE.

stort forbedringspotensial for planlegging, drift og vedlikehold av lavspentnettet.

Med innføring av AMS øker antallet flater som kan angripes, med antall husholdninger og virksomheter som skal tilknyttes AMS-systemet. Utfordringene er knyttet til økt avhengighet av offentlig telekommunikasjon og økt behov for tilkobling, personvern og sikkerhetsstyring. Innføringen av AMS vil gjøre kraftsystemet mer eksponert for programvarefeil og trusler som kommer gjennom Internett. Dette følger naturlig av bruken av kommersielle systemer og tilkoblingene til Internett for å overføre data fra AMS til Elhub (sentralisert KWh-server). For eksempel bygger SORIA-prosjektet en sky med IPv6 som gjør at man kan fase inn andre funksjoner i nettet, eksempelvis gatelys. AMS blir da en del av et Smart City/Smart Grid.

Beslutningen om å implementere AMS har skjedd uten stor debatt i Norge og Norden, i motsetning til i enkelte andre land, særlig Nederland og USA. NVE har imidlertid tydeliggjort overfor bransjen viktigheten av å gjennomføre risikoanalyser ved innføringen av AMS og at nettselskapene er ansvarlige for å sørge for tilstrekkelig sikkerhet i AMS-løsningen.

Strategisk sårbarhet som følge av bryterfunksjonaliteten

I Norge er det et krav til AMS-målerne som installeres, at de støtter bryter- og strupefunksjonalitet. Per i dag har nettselskapene bare adgang til å fjernutkoble én kunde om gangen. Det kan bli aktuelt på sikt, etter testing og utredning, å tilrettelegge for masseutkobling eller massestruping på et gitt effektnivå i forbindelse med en beredskapssituasjon eller ved rasjonering, typisk ved effektknapphet. Ved inntrenging i systemene som administrerer AMS-bryterfunksjonaliteten for å foreta uautorisert utkobling, kan man risikere at mange strømkunder mister strømmen.

Sikkerhet rundt bruk av bryterfunksjonalitet i AMS er en aktuell problemstilling som diskuteres internasjonalt. EUs funksjonskrav for AMS inneholder bryterfunksjonalitet. Det eneste landet som har valgt å gå imot anbefalingene og ikke inkludere bryterfunksjonalitet, er Nederland.

Uautorisert tilgang

Det er allerede vist at smarte målere kan hackes, at radioantenner kan avlyttes, at signaler kan stoppes, eller at måleren fysisk modifiseres når den ikke er godt fysisk beskyttet. Dette synet er støttet av internasjonale sikkerhetseksperter som advarer mot sårbarheter og fare for misbruk i AMS.

Uautorisert tilgang til sentralsystemet for AMS kan gjøre det mulig å manipulere brytere. Samme konsekvens kan oppnås dersom SCADA-systemet ikke er tilstrekkelig sikret mot uautorisert tilgang, eller at tilkoblingen til andre typer systemer er tilsvarende sikret. Dessuten vil en slik sammenkobling kunne gi muligheter for manipulering av data.

I tillegg til dette kommer innsidetrusselen. Dersom en utro tjener i eget selskap eller hos leverandøren får uautorisert tilgang, kan vedkommende tappe systemet for informasjon og i verste fall overta styringen av systemet. Alle landets måleverdier vil bli lagret i Elhub, som også inneholder noe informasjon om de enkelte kundene. Potensielt kan informasjon komme på avveie hvis en ansatt med tilstrekkelig tilgang tapper informasjon fra systemene.

Håndtering av endringer, konfigurasjoner og grensesnitt

AMS-systemet er komplekst og kjennetegnes av mange grensesnitt og gjensidige avhengigheter mellom ulike komponenter, men også avhengigheter til eksterne systemer som elektroniske kommunikasjonssystemer og satellittbaserte tjenester som gir nøyaktig tid.

Det er krevende å holde oversikt over og få verifisert at alle målerne er oppdatert og riktig konfigurert. Leverandørene sender konfigurasjonsdata til nettselskapene, som selv gjennomfører oppdateringer. Driftsselskapene kan også stå for oppdateringer, slik det for eksempel er tenkt i SORIA-samarbeidet. Det er en risiko for at feil kan få utilsiktede konsekvenser et annet sted i verdikjeden, for eksempel dersom systemet blir infisert av skadevare i forbindelse med oppdateringer.

Logging og analyse

Systemkompleksiteten gjør at det blir viktig å være i stand til å oppdage unormal og utilsiktet trafikk. Eierskap til AMS-infrastrukturen vil variere fra selskap til selskap. Enkelte nettselskaper vil eie en god del infrastruktur selv, mens andre vil leie mye av infrastrukturen, som for eksempel mobildatakommunikasjon. Leverandører har hevdet at trafikk fra målere er lett å gjenkjenne ved at det danner seg et mønster. Ved å logge datatrafikk og være i stand til å analysere disse loggene kan leverandøren skille uvesentlige feil fra feil en bør

reagere på. Ved å se på adferden til sensorene kan en se om en måler er fysisk manipulert eller ikke. Så langt har NVE standardisert at det ut mot kundene av nettselskapene bare skal være ett lesegrensesnitt, og at kunden skal kunne kryptere eller skru av dette.

Sårbarheter ved bruk av datasentre eller utkontraktering av drift

Noen leverandører tilbyr driftsløsninger til kraftselskapene. Dersom en utkontrakterer drift av AMS, kan det oppstå andre sårbarheter. Ifølge SINTEF drifter 70 prosent av nettselskapene sin egen driftssentral, men dette bildet kan endres i fremtiden.[12] Flere nettselskaper har påpekt at det er stor variasjon i modenheten hos leverandører av sikkerhetsløsninger for AMS. Blant annet som følge av lav modenhet hos nettselskapene og leverandørene på enkelte områder ble enkelte krav, som for eksempel PKI og kryptering, «bør-krav» og ikke «må-krav». Alle nettselskapene stilte imidlertid krav om at sikkerhetsløsningen på sikt bør kunne tilpasses et endret trusselbilde.

Bruken av datasentre og skytjenester knyttet til AMS er i dag liten. Flere selskaper har ut fra effektivitetshensyn satt i gang et arbeid for innsamling av måle- og avregningsdata gjennom å etablere regionale datahuber. Når AMS er gjennomført i 2019, vil timesdata av alt forbruk fra cirka 2,9 millioner målere bli innsamlet via regionale datasentraler og videreformidlet til den nasjonale datahuben (Elhub). Dette tilsier at sikring av informasjon i datasentre/skytjenester vil bli spesielt viktig i prosessen frem til oppstart av systemene.

Personvernutfordringer i smarte nett

Personopplysningsloven stiller krav til hvordan nettselskapene kan bruke opplysningene som samles inn.

Strømforbruk kan spores til enkeltpersoner. Opplysninger om strømforbruk er i utgangspunktet knyttet til et målernummer på en bestemt adresse, ikke til en person. Men når måleren igjen knyttes til en huseier, kan opplysningene om strømforbruket spores tilbake til en bestemt person. Dette kan være abonnenten selv eller en annen person, for eksempel en leietaker.

Ved å analysere detaljerte data om strømforbruk kan det i fremtiden være mulig å anta eller forutsi når personene i hjemmet er på ferie eller på jobb, når de sover, når de er våkne, og andre bruksmønstre.

Bruksmønstrene kan være nyttige ved at man kan analysere strømforbruket vårt med tanke på for eksempel strømsparing. Men bruksmønstrene kan også bli brukt til andre ting, som markedsføring og reklame. Politiet, skattemyndighetene, forsikringsselskaper, utleiere, arbeidsgivere og andre tredjeparter kan også være interessert i informasjon om personlig strømforbruk.

Fare for misbruk av personopplysninger. Det er definerte rammer for hvordan de personopplysningene som samles inn ved hjelp av automatiske målesystemer, kan brukes. Det europeiske personvernombudet, The European Data Protection Supervisor (EDPS), advarer likevel om at denne informasjonen kan misbrukes hvis den ikke sikres forsvarlig. EDPS anbefaler at selskapene må innhente samtykke fra forbrukerne før nettselskapet bruker informasjonen fra slike målere til andre formål enn det som er nødvendig for å utøve virksomheten.

NVE har pålagt nettselskapene å innhente data for fakturering (fra Elhub). Kunden eier sine egne strømdata og må selv aktivt samtykke i at kommersielle aktører skal få tilgang til disse dataene.

13.5.4 Avhengighet av ekom og satellittbaserte tjenester

På sentralnett- og regionalnettnivå eier og drifter selskapene sine egne telekommunikasjonssystemer. Dette sikrer selskapene tilgang til telekommunikasjonstjenester også på områder der dekningen fra ekomleverandører ikke er god nok. Selskapene gjør seg mer avhengige av driftskontrollsystemene for å ha mest mulig effektiv drift og detektere feil raskere. En gradvis effektivisering over tid, der personell blir erstattet med informasjons- og kommunikasjonssystemer, forsterker avhengigheten av telekommunikasjon. Myndighetene og bransjen selv er klar over avhengigheten.

De største selskapenes driftssentraler er derfor, etter krav fra NVE, knyttet med dublert samband til underliggende stasjoner av sikkerhetsklasse 2 og 3. Selv om det er dublerte samband på viktige installasjoner, kan sekundærforbindelsen ha lavere kapasitet enn hovedforbindelsen, noe som kan hemme effektiviteten i driften dersom hovedsambandet faller ut. Det er imidlertid et

[12] Sæle, H., Sagosen, Ø., Bjørndalen, J. (2014): *Norsk driftssentralstruktur Funksjon, kostnadsforhold og fremtidig utvikling.* SINTEF Energi.

krav at kommunikasjonslinjer som faller ut, raskt skal gjenopprettes.

Det er et krav at selskapene har et mobilt radiosamband som skal fungere uavhengig av offentlige teletilbydere. Det er dette som skal benyttes når mannskap skal påkalles, og når arbeid i felten skal koordineres. Reparasjon og vedlikehold krever imidlertid samvirke med mange aktører og underleverandører. Kommunikasjon med andre aktører enn de rent driftsrelaterte innen bransjen går via teletjenester kjøpt i markedet. Bortfall av mobilnettet vil dermed kunne redusere effektiviteten i samvirke og håndtering av kriser og hendelser i sektoren. NVE har uttrykt at selskapene står fritt til å velge teknologi såfremt de oppfyller kravene i beredskapsforskriften. Bruk av Nødnett til kraftforsyningens behov er ikke avklart. For å opprettholde nødvendig beredskap skal kraftforsyningen etter behov vedlikeholde, anskaffe og bygge radionett for mobilkommunikasjon (driftsradio) uavhengig av utbyggingen av Nødnett.[13]

Ekstremværet Dagmar medførte store utfordringer for kraftbransjen. Mange hovedveier og mindre veier ble stengt, ferjer var ute av drift og hele eller deler av jernbanestrekninger ble stengt. Dette medførte ekstra utfordringer både for nettselskapenes opprydning og feilretting og for kommunenes håndtering av hendelsen. At kommunikasjonsmuligheter i stor grad var fraværende eller sterkt redusert, medførte store utfordringer for krisehåndteringen – både i kommunene, hos nødetatene og hos mannskapene som skulle gjenopprette feil og ødeleggelser. Hendelsen viste imidlertid at kraftforsyningens kommunikasjon med reparasjonsmannskapene i stor grad ble ivaretatt, ettersom de benyttet egne driftsradiosystemer. Hendelsene i forbindelse med Dagmar har bidratt til en rekke tiltak knyttet til sikkerhet og beredskap. For nærmere omtale, se kapittel 11 «Elektronisk kommunikasjon».

Akkumulert sårbarhet fra elektronisk kommunikasjon

Kompleksiteten i kraftforsyningen er ventet å øke med den planlagte innføringen av AMS. AMS fører til behov for ny IKT-infrastruktur. AMS vil legge til rette for større styringsevne når det gjelder ut- og innkobling av forbruk på distribusjonsnettnivå, og også gi kundene raskere og riktigere innhenting av måleverdier, bedre grunnlag for faktura og muligheter for å effektivisere strømforbruket. På sikt vil dette systemet gi grunnlag for smarte byer (se punkt 6.2.2 «Tingenes Internett») der også husholdninger og virksomheter kan selge energi og effekt fra egenproduksjon (eksempelvis vindmølle på taket / solcellepanel / batteri). Systemdriften blir trolig mer sammensatt fremover som følge av økt innmating fra ikkeregulerbar produksjon. Dette gjelder også i distribusjonsnettet. Forbruket endres i form av økt fleksibilitet og større variasjoner (økt effektuttak). Smarte nett og AMS gir nye muligheter for å håndtere systemdriften, men øker i følge Reitenutvalget samtidig behovet for investeringer og kompetanseutvikling.

AMS gjør seg nytte av elektronisk kommunikasjon, som GPRS. Selv om det er krav i avregningsforskriften om sikker kommunikasjon i AMS-løsningen, er denne typen teknologi sårbar for avlytting. Derfor vil ifølge NVE alle enten bruke et krypteringslag på toppen eller bruke løsninger som i seg selv beskytter informasjonen mot innsyn under transport. Det er krav til lokal lagring av måledata i AMS-målerne, slik at AMS' primære funksjon ikke faller ut ved kommunikasjonsutfall.

Avhengighet av satellittbaserte tjenester – tid

Både driftskontrollsystemer og AMS blir stadig mer avhengige av korrekt tid. Internasjonalt utarbeides det nye standarder for kontrollanlegg (IEC 61850) som innebærer synkroniseringskrav på mikrosekundnivå. Det anses derfor som sannsynlig at strengere tidssynkroniseringskrav på sikt kan bli relevant også i Norge.[14] Dette kan igjen få konsekvenser for sårbarheten i systemet som helhet.

13.6 Fremtidige problemstillinger og trender

Samfunnet har lenge vært og blir stadig mer avhengig av stabil kraftforsyning med høy kvalitet. Kraftforsyningen står overfor store teknologiskifter som blant annet vil kunne medføre at selskapene i større grad også blir leverandører av IKT-tjenester. Fremtidige sårbarheter er knyttet til fortsatt automatisering, herunder utrullingen av AMS og fremtidig bruk av skyløsninger i kraftforsyningen.

[13] Energi Norge og Telenor (2013): *Sikkerhet og beredskap mot ekstremvær i telesektoren.*

[14] Norsk romsenter (2013): *Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur.*

Boks 13.4 Mulighetsrommet ved avanserte målere

Avanserte målere gir muligheter for å utvikle tjenester knyttet til smarte hus og pleie- og omsorgstjenester. Et eksempel er Lyse energi, som leverer tjenester både til smarte hjem og til velferdstjenester, der kunden skal kunne styre hele boligen med én fjernkontroll. Smartly AS utvikler løsninger for smart styring av varme, lys, innbrudds- og brannalarm. Smartly tilbyr også velferdsteknologiprodukter som skal hjelpe eldre og andre med spesielle behov til å klare seg lenger hjemme. Disse produktene kan styres fra nettbrett og smarttelefoner.

Ny teknologi innenfor desentral produksjon (småskala vindkraft, småkraft og solkraft) og endringer i forbruksmønstre (flere effektkrevende apparater, hurtiglading av elbiler og så videre) endrer tradisjonell kraftflyt og gir nye utfordringer for nettselskapene og produsentene. Det er usikkerhet knyttet til hva den nye teknologien gjør for stabiliteten i nettet når flere kunder blir pluss-kunder og leverer overskuddsstrøm tilbake til kraftsystemet. Ny teknologi åpner også for nye forretningsområder og markedsorientert sluttbrukerstyring, samt løsninger for energieffektivisering.

Utviklingen går i retning av smarte målere, smarte nett og smarte byer, noe som betyr økt kompleksitet, tettere koblinger og økt risiko for mer vidtrekkende konsekvenser ved feil. I fremtiden vil strømleverandørene kunne bli IKT-selskaper som analyserer data og leverer informasjon og tjenester til forbrukernes smarttelefoner og nettbrett. Målesystemer som gir detaljerte opplysninger om hva enkeltpersoner gjør i hjemmet, kan legge til rette for velferdsteknologi og trygghetspakker for eldre. Nettselskapene har pekt på at det er ønskelig at NVE gjør det tydelig hvilke andre bruksmuligheter AMS åpner for.

IKT og kraftsystemet smelter mer og mer sammen. Det trengs sikre IKT-systemer og tilstrekkelig kompetanse der problemene oppstår. Det finnes enormt med data, men det blir en utfordring å administrere og analysere disse. Mer overvåking basert på IKT og økning i fornybare energikilder blir mulig. Det er et aktuelt tema i Europa. Det ventes også en økning i cybertrusler og i sabotasje og fysisk ødeleggelse av kommunikasjonssystemer. Elektroniske komponenter blir stadig mindre, samtidig blir de mer sensitive for elektromagnetisk interferens. Dette representerer også en sårbarhet i et stadig mer automatisert system.

Kravene til kontinuerlig risikoanalyse og endringsledelse vil øke som følge av denne utviklingen.

13.7 Vurderinger og tiltak

Infrastrukturer og samfunnsfunksjoner er avhengige av stabil kraftforsyning med god kvalitet. Den økte digitaliseringen gjør avhengigheten enda større, og sårbarheter innen kraftforsyningen akkumuleres til andre områder i samfunnet. Det gjør at det stilles særlige krav til denne bransjen og til hvilke tiltak som må gjennomføres for å redusere sårbarheten. Utvalget har observert at det er uenighet mellom Olje- og energidepartementet og Forsvarsdepartementet knyttet til utpeking av skjermingsverdige objekter i energiforsyningen etter sikkerhetsloven. Utvalgets synspunkter på slike problemstillinger er beskrevet i kapittel 23 «Tverrsektorielle sårbarhetsreduserende tiltak». Gitt kraftforsyningens kritikalitet i samfunnet og økte digitale sårbarhet vil utvalget anbefale følgende:

13.7.1 Styrke tilsyn og veiledning i IKT-sikkerhet

NVE har ansvaret for beredskapen i norsk kraftforsyning og regulerer dette gjennom forskrifter og veiledning av bransjen. Den økte digitaliseringen medfører et behov for tett oppfølging fremover og for mer spissede tilsyn innenfor enkelte områder. NVE har begrenset kapasitet til å følge opp med tilsyn innen IKT-sikkerhet og sårbarhet. *Disse forholdene legges til grunn for utvalgets forslag om å styrke NVE betraktelig på området tilsyn og veiledning.*

Det er et generelt utviklingstrekk at det legges opp til stadig tettere koblinger mellom driftskontrollsystemer og forretningssystemer. Dette er en betydelig utfordring fordi driftskontrollsystemene i utgangspunktet er bygd for et langt liv i et beskyttet miljø med store krav til stabilitet og driftssikkerhet. Det står i et misforhold til behovet for stadige oppdateringer og tilpasninger som er imperativt for systemer som fungerer i den åpne verden. Utvalget mener ikke det er veien å gå å jobbe mot denne utviklingen, til det er de forretningsmessige og styringsmessige gevinstene for store og åpenbare. *Utvalget mener at dette er en*

utfordring som må møtes med gode og gjennomgripende tiltak knyttet til teknisk arkitektur, transaksjonskontroller og hensiktsmessig soneinndeling. På dette området mener utvalget at NVE bør kunne spille en viktig rolle i å formidle beste praksis og for øvrig veilede berørte virksomheter i sikker implementering.

Utvalget observerer at det i kraftbransjen, som i andre bransjer, er en økt trend mot tjenesteutsetting. Denne trenden har innvirkning på IKT-sikkerheten. Tjenesteutsetting omfatter også oppfølging av leverandører. Virksomhetene må sørge for at relevante IKT-sikkerhetskrav inngår i avtaler med leverandøren, og at kravene følges opp. Den enkelte virksomheten vil ikke alltid evne å se de samfunnsmessige konsekvensene av utilstrekkelige IKT-krav. *Derfor mener utvalget at NVE i fellesskap med interesseorganisasjoner og bransjen bør utarbeide veiledere og krav til tjenesteutsetting i kraftbransjen. Utvalget anbefaler sektoren å se på internasjonale standarder.*

13.7.2 Stimulere til større og mer ressurssterke fagmiljøer innen IKT-sikkerhet

Flere KBO-enheter er små med få ansatte, og det er en kompetanseutfordring å etablere og opprettholde nødvendige fagmiljøer. *Utvalget mener at NVE i samarbeid med interesseorganisasjonene bør stimulere til større og mer ressurssterke fagmiljøer på IKT-sikkerhet i KBO-enhetene.* Dette kan gjøres på flere måter, eksempelvis gjennom økt samarbeid mellom KBO-enheter eller gjennom strukturendring.

Bransjeorganisasjonene har et veletablert system for kurs og opplæring. Utvalget foreslår at dette videreutvikles til å dekke de nye utfordringene vi står overfor innenfor IKT-sikkerhet. *Bransjeorganisasjonene bør kunne bidra med å organisere kurs innenfor IKT-sikkerhet, gjerne i samarbeid med andre organisasjoner, eller henvise til NVE, andre myndigheter eller undervisningsinstitusjoner der det er hensiktsmessig. Det bør også utvikles kurs og studieretninger innenfor prosesstyring, systemintegrasjon og IKT, noe som kan bidra til at bransjen får den kompetansen som trengs for å drifte systemene i fremtiden.*

Kraftbransjen har lang tradisjon for å gjennomføre øvelser. Utvalget er gjort kjent med at kompetansen knyttet til IKT-sikkerhet er varierende blant virksomheter i bransjen, og mener derfor det er behov for å gjennomføre flere øvelser innenfor IKT-sikkerhet, der leverandører inviteres med. Gjennom ulike typer øvelser kan organisasjoner og samarbeidspartnere øve på planverk og nye utfordringer. *Utvalget anbefaler at NVE gjennom sin veiledningsrolle er pådriver for flere øvelser på IKT-sikkerhetsområdet både i sektoren og opp mot andre sektorer det er naturlig å samarbeide med.*

13.7.3 Bygge et sterkt operativt fagmiljø for IKT-hendelseshåndtering

Leveringssikkerheten i kraftbransjen er høy. Likevel gir naturhendelser og teknisk svikt tidsbegrensede kraftbortfall. Sektorens kritiske rolle tilsier at bransjen må ha god beredskap mot alle typer hendelser, også tilsiktede IKT-hendelser som vi ennå ikke har sett så mange av. IKT er tett integrert i kraftforsyningen og avgjørende for å sikre en effektiv og sikker drift av systemet. Virksomhetene må selv ha evne til å håndtere hendelser. I den sammenheng er det viktig med åpenhet og rask informasjonsutveksling om trusler, erfarte hendelser og mulige avbøtende tiltak.

Kraftforsyningen er en viktig infrastruktur for resten av samfunnet. Bransjen bør ha et kompetent felles miljø for hendelseshåndtering som både kan koordinere hendelser internt i sektoren og være kontaktpunkt ut mot andre sektorer. *Utvalget støtter ideen om å videreutvikle KraftCERT som et sterkt fagmiljø innen operativ hendelseshåndtering. NVE må tydeliggjøre krav om tilknytning til et operativt fagmiljø for hendelseshåndtering, enten mot KraftCERT eller mot andre miljøer.* Virksomhetene bør ha en tydelig begrunnelse for hvilket alternativ de velger. Det er viktig med avklarte roller mellom responsmiljøene, slik at kraftbransjen opptrer enhetlig overfor andre sektorer.

13.7.4 Vurdere de sikkerhetsmessige forhold ved å behandle og lagre kraftsensitiv informasjon i utlandet

Noen typer informasjon er kritisk for drift av kraftforsyningen i ordinære og ekstraordinære situasjoner. Hva som er kraftsensitiv informasjon, og som skal beskyttes særskilt, går frem av beredskapsforskriften. Samtidig observerer utvalget at teknologiutviklingen, økt systemintegrasjon og organisasjonsendringer hos leverandører endrer mulighetsrommet for tjenesteutvikling. Med dette blir tradisjonelle sikkerhetstiltak og begrensninger for informasjonsdeling utfordret, se nærmere omtale i punkt 23.7 «Utkontraktering og skytjenester».

Norsk kraftforsyning må kunne driftes selv i situasjoner der ekom mot utlandet svikter. Dette

har konsekvenser for hvilken informasjon som kan lagres utenfor Norges grenser. Utvalget observerer at dagens regelverk gir utfordringer for tjenesteutvikling og effektiv drift av kraftforsyningen, og vil derfor anbefale at NVE gjør en vurdering av hvilken informasjon som, gitt de endrede teknologiske og organisatoriske rammene, er så kritisk at den ikke bør lagres og behandles utenfor Norges grenser. *Utvalget anbefaler at NVE ser på hele verdikjeden og identifiserer hvilken informasjon i denne som må være under nasjonal kontroll.*

13.7.5 Gjennomføre risiko- og sårbarhetsanalyse for utvidet bruk av AMS

Vedtak om *innføring* av AMS skjedde uten en forutgående risiko- og sårbarhetsanalyse.[15] Utrullingen av AMS innebærer et stort potensial for økt nettnytte, innovasjon og effektivisering i sektoren. Utvalget stiller seg positivt til at denne effekten må tas ut, men mener det må gjøres med en grad av forsiktighet. Ukritisk implementering av funksjonalitet som for eksempel knytter AMS tettere sammen mot driftskontrollsystemer, vil medføre en sårbarhetsoppbygging med et betydelig skadepotensial. Utvalget mener det er viktig med en god og bredt dekkende risiko- og sårbarhetsanalyse i forkant av teknologiskifter, ved bruksendringer og ved system- og organisasjonsendringer. *Utvalget anbefaler at NVE gjennomfører nødvendige risiko- og sårbarhetsanalyser for utvidet bruk av AMS inn mot driftskontrollsystemene.*

13.7.6 Utarbeide en oppdatert analyse av kraftforsyningens avhengighet av ekom

Utvalget har merket seg NVEs uttalelser om at kraftbransjens avhengighet av ekom er lav, og at dette i hovedsak skyldes gjeldende krav i regelverket om å kunne drifte kraftsystemet selv når kommersiell ekom er nede. Utvalget er kjent med at kraftforsyningen har et eget samband, men stiller spørsmål ved om denne vurderingen fullt ut tar innover seg kompleksiteten og samhandlingen på tvers av aktører i og utenfor bransjen. Utvalget konstaterer videre en generell trend for alle andre samfunnsaktører om økt avhengighet av IKT og kommersiell ekom. Dette henger sammen med et bredere aktørbilde og økt kompleksitet i verdikjeden.

Utvalget vil peke på at selv om kraftbransjen så langt har klart å håndtere kritiske situasjoner uten kommersiell ekom, kan evnen utfordres i fremtiden når enda mer IKT blir lagt til og integrert i kraftinfrastrukturen. *Utvalget anbefaler derfor NVE og bransjen å foreta en ny gjennomgang for å etterprøve om dagens krav gir den «uavhengigheten» som regelverket krever.*

[15] En rekke ROS-analyser er imidlertid gjennomført etter vedtaket, se eksempelvis Proactima og Energi Norge (2015), Overordnet risiko- og sårbarhetsanalyse for innføring av AMS.

Kapittel 14
Olje og gass

Enhver aktivitet i olje- og gassektoren er forbundet med risiko forårsaket av trusler og sårbarheter. Det gjelder i økende grad også risiko som skyldes digitale sårbarheter. Norske etterretningsmyndigheter har de senere årene advart om en økning i antall digitale trusler rettet mot norsk industri. Det er mange indikasjoner på at hele verdikjeden i petroleumssektoren nå er et mål for tilsiktede digitale angrep. Sektoren er svært viktig for norsk økonomisk bæreevne og for Norges internasjonale betydning og omdømme som olje- og gassleverandør. I ytterste konsekvens får alvorlig svikt i leveransene konsekvenser for land som importerer store deler av sin gass fra Norge.

Mens digitale sårbarheter har vært viet stor oppmerksomhet innen tradisjonell informasjons- og kommunikasjonsteknologi, har vektleggingen av slike sårbarheter innen prosess- og industrisektoren kommet det siste tiåret. I 2010 ble man oppmerksom på Stuxnet, som viste at målrettede digitale angrep kan utnytte digitale sårbarheter og påføre industrielt utstyr og infrastruktur signifikante skader. For olje- og gassektoren ble eksplosjonen i en oljerørledning i den tyrkiske byen Erzincan i 2008 en tankevekker. Flere år etter ulykken ble årsaken presentert, og det var tydelige indikasjoner på at dette var resultatet av et digitalt angrep. Hackere hadde slått av alarmer og kommunikasjonslinjer og økt trykket i rørledningen.

Deler av utvalgets omtale av olje og gass er basert på rapporten «Digitale Sårbarheter Olje & Gass (DNV GL)», se elektronisk vedlegg.

14.1 Olje- og gassinfrastruktur

Olje- og gassvirksomheten er basert på en omfattende infrastruktur som består av faste og flytende produksjonsinnretninger, flyttbare boreinnretninger, undervannsinstallasjoner, rørtransportsystemer, mottaks- og prosessanlegg, raffinerier, kontrollsentraler, forsyningsbaser, lagre, forsyningsfartøy, helikoptre og helikopterterminaler. Av infrastruktur er produksjonsplattformer, raffinerier, rørledninger og skipningsterminaler mest kritisk. Sanntidsoverføring av data fra brønn til land og sanntidsdeling av informasjon mellom personell offshore og personell på land gjør nye samarbeidsformer mellom ulike grupper og ulike ekspertgrupperinger – også omtalt som integrerte operasjoner – mulig. Mens man tidligere måtte få eksperter til å reise ut til en plattform for å løse et problem, kan problemet nå ofte løses fra land. Norsk olje og gass anslo i 2008 at integrerte operasjoner kan øke verdiskapingen med 300 milliarder kroner.

Det er omtrent 50 år siden man startet petroleumsvirksomhet på norsk sokkel, og flere av de første feltene er fortsatt i drift. Samtidig har aktiviteten bredt seg utover den norske sokkelen. I begynnelsen var det bare utenlandske selskaper på sokkelen, men etter hvert som kompetansen økte, kom norske selskaper med. I dag er det nær 40 selskaper på norsk sokkel. Statoil er det største selskapet, etterfulgt av internasjonale selskaper som ConocoPhillips, British Petroleum, Exxon, Shell, Total og ENI.

Petroleumsvirksomheten har hatt mye å si for den økonomiske veksten i Norge og for finansieringen av det norske velferdssamfunnet. I 2013 sto petroleumssektoren for 22 prosent av verdiskapingen i landet. Verdiskapingen i sektoren er mer enn dobbelt så stor som i landindustrien og rundt 15 ganger den samlede verdiskapingen i primærnæringene. Norge eksporterer 97 prosent av all gass, noe som gjør Norges til verdens nest største gasseksportør.

14.2 Roller og ansvar

Olje- og energidepartementet har det overordnede ansvaret for forvaltningen av petroleumsressursene på den norske kontinentalsokkelen. Departementet skal se til at petroleumsvirksomheten foregår etter de retningslinjene Stortinget og regjeringen gir, og har i tillegg et eieransvar for de statlige

selskapene Petoro AS og Gassco AS og for det delvis statlige oljeselskapet Statoil ASA.

Oljedirektoratet er administrativt underlagt Olje- og energidepartementet og er et statlig fagdirektorat og forvaltningsorgan for norsk petroleumsvirksomhet. Oljedirektoratet har et nasjonalt ansvar for at data og informasjon fra petroleumsvirksomheten er tilgjengelig og derved bidrar til verdiskaping. Oljedirektoratet har en sentral rolle innenfor petroleumsforvaltningen og er et viktig rådgivende organ for Olje- og energidepartementet. Direktoratet utøver forvaltningsmyndighet og skal bidra til å skape størst mulige verdier for samfunnet fra olje- og gassvirksomheten gjennom en forsvarlig ressursforvaltning med forankring i sikkerhet, beredskap og ytre miljø.

Arbeids- og sosialdepartementet har det overordnede ansvaret for forvaltning av arbeidsmiljøet og for sikkerhet og beredskap på norsk sokkel. Departementet gir føringer for Petroleumstilsynets prioriteringer gjennom årlige tildelingsbrev.

Petroleumstilsynet er et selvstendig, statlig tilsynsorgan med myndighetsansvar for sikkerhet, beredskap og arbeidsmiljø i norsk petroleumsvirksomhet. Petroleumstilsynet var tidligere en del av Oljedirektoratet. Regjeringen bestemte i 2002 at Oljedirektoratet skulle deles, slik at tilsynet med sikkerhet ble lagt til en egen etat (Petroleumstilsynet).[1] Petroleumstilsynet er nå underlagt Arbeids- og sosialdepartementet.

I tillegg har Petroleumstilsynet et spesielt samordningsansvar med andre etater som har ansvar på norsk sokkel. Ansvaret for deler av petroleumsvirksomheten er fordelt på andre departementer: Oljevernberedskap, helikoptertransport og radiokommunikasjon er underlagt Samferdselsdepartementet, petroleumsskattlegging er underlagt Finansdepartementet, helsemessige sider er underlagt Helse- og omsorgsdepartementet, og det ytre miljøet er underlagt Miljøverndepartementet. Flytende innretninger er underlagt Sjøfartsdirektoratet, som igjen er underlagt Nærings- og fiskeridepartementet.

Direktoratet for samfunnssikkerhet og beredskap (DSB) har et ansvar for oppfølging av prosesstyringsanlegg, på bakgrunn av brann- og eksplosjonsvernloven med forskrifter, samt storulykkeforskriften. Ved etablering av nye anlegg følger DSB opp saksbehandling, tilsyn og annet som blir gjort relatert til behandling av virksomhetens søknad om samtykke. I ordinært tilsyn er det vanlig at DSB følger opp hvordan virksomhetene sørger for at systemene deres virker etter intensjonene. Alle storulykkemyndighetene (DSB, Miljødirektoratet, Petroleumstilsynet, Næringslivets sikkerhetsorganisasjon (NSO) og Arbeidstilsynet) vil under tilsyn med storulykkevirksomheter følge opp denne typen systemer. Anlegg på land er underlagt storulykkeforskriften.

Norsk olje og gass (NOROG) er en interesse- og arbeidsgiverorganisasjon under Næringslivets Hovedorganisasjon for oljeselskaper og leverandørbedrifter knyttet til utforsking og produksjon av olje og gass på norsk kontinentalsokkel. Organisasjonen representerer 53 oljeselskaper og 54 leverandørbedrifter. Formålet med organisasjonens aktiviteter på IKT-sikkerhetsområdet er å forebygge gjennom erfaringsoverføring i NOROGs nettverk og prosjekter/arbeidsgrupper der interesserte medlemsbedrifter deltar. NOROG har et tett samarbeid med aktuelle myndigheter, i dette tilfellet NSM NorCERT og Petroleumstilsynet.

Ifølge Oljedirektoratets faktasider er 37 operatørselskaper registrert som operatører på norsk sokkel. Leverandørindustrien brukes som samlebegrep på aktørene som leverer produkter og tjenester til petroleumsvirksomheten.

Gassco AS er et statlig selskap som siden 2002 har hatt operatøransvaret for transport av gass fra den norske kontinentalsokkelen. Transportsystemet er omfattende og består av flere plattformer og tusenvis av kilometer med rørledninger. Gassco er operatør for Gassled, som er et interessentskap og den formelle eieren av infrastrukturen forbundet med gasstransporten fra norsk sokkel. Petoro AS og Solveig Gas Norway AS er de største eierne, med til sammen nær 70 prosent av eierandelene. Gassco har ikke eierandeler i Gassled, men har tilsyn med operatørselskapet.

Forskning og utvikling

Olje- og energidepartementet er et av de departementene som bevilger store summer til forskning og innovasjon hvert år. Det meste av overføringene til FoU skjer via programmer i Forskningsrådet. IKT inngår i flere store programmer. For eksempel forskes det mye på integrerte operasjoner i offshorevirksomheten, det er blant annet etablert et eget senter for dette temaet ved NTNU, og det pågår sikkerhetsrelevant forskning på IKT i større programmer som DEMO 2000 og PETROMAKS 2.

---

[1] Olje- og energidepartementet (2003): *Kronprinsregentens resolusjon om det nye Oljedirektoratets ansvar og oppgaver etter utskillelsen av Petroleumstilsynet.*

Internasjonalt samarbeid

Petroleumstilsynets DwH-rapport med vurderinger og anbefalinger for norsk olje- og gassektor inneholder en beskrivelse av internasjonale problemstillinger og pågående samarbeid på generelt nivå.[2] I dag reises det blant annet krav om internasjonal sikkerhetsregulering og -koordinering og om etablering av tverrnasjonale regelverkskrav. Fra flere hold er det tatt til orde for mer ensartede internasjonale sikkerhetsregimer i olje- og gassvirksomheten.

14.3 Hjemmelsgrunnlag og tilsynsvirksomhet

Petroleumsloven regulerer myndighetenes forvaltning av norske petroleumsressurser. Loven kommer til anvendelse på petroleumsvirksomhet knyttet til undersjøiske petroleumsforekomster som er underlagt norsk jurisdiksjon. Loven gjelder også petroleumsvirksomhet i og utenfor riket og norsk kontinentalsokkel når det følger av folkeretten eller av overenskomst med en fremmed stat. I 2013 ble ansvaret for å ivareta petroleumsloven § 9-3 Beredskap mot bevisste anslag delegert fra Olje- og energidepartementet til Arbeids- og sosialdepartementet (Petroleumstilsynet). Kapittel 9 i petroleumsloven stiller krav til sikkerhet og beredskap, også mot tilsiktede handlinger, men IKT er ikke nevnt spesielt i petroleumsloven.

Olje- og gassindustrien har et funksjonsbasert regelverk innenfor helse, miljø og sikkerhet (HMS). Regelverket har lagt til grunn at selskapene selv vurderer risiko, setter akseptkriterier og beslutter relevante tiltak. Dette gjøres gjennom risiko- og beredskapsanalyser i de enkelte selskapene. Bransjens egenutviklede standarder legges til grunn for arbeidet.

Næringens retningslinjer

Operatørselskapene har et selvstendig ansvar og en egeninteresse i å ivareta IKT-sikkerheten i egen virksomhet. Næringen har selv, gjennom Norsk olje og gass, utarbeidet spesifikke retningslinjer for informasjonssikkerhet i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer (sist revidert i 2009).[3] Bakgrunnen for etableringen av retningslinjene var en dramatisk økning i antall virusangrep, hendelser på norsk sokkel og ønsket om å etablere et reaksjonsmønster tilpasset prosesskontrollsystemer og ikke bare «normal IT-drift». Fra 2014 henvises det til retningslinjene i innretningsforskriften § 34 a.

Tilsyn

Siste års tilsynsrapporter på selskapsnivå er tilgjengelige på Petroleumstilsynets nettsider. Rapportene fokuserer på HMS og sikkerhet i jobbutøvelse for ansatte. På teknisk side har Petroleumstilsynet gjennomført tilsyn hos enkeltvirksomheter innenfor for eksempel prosessintegritet og barrierer. Tidligere tilsyn med IKT-sikkerhet fra 2007 har påvist mangler i barrierer mellom prosessnettverk og administrativt nett, mangler i IKT-sikkerhetskompetanse, mangelfull oppdatering av dokumentasjon og uklarheter rundt håndtering av feil i kommunikasjonssystemer. Disse forholdene er nå inkludert i retningslinjene til bransjen. Petroleumstilsynet gjennomfører systemtilsyn, og har ikke spesialistkompetanse på teknisk systemevaluering av IKT-sikkerhet.

14.4 Beredskap og hendelseshåndtering

Olje- og gassektoren er utpekt som fortsatt særlig utsatt for etterretningstrusler i Politiets sikkerhetstjenestes årlige trusselvurdering for 2015. Etterretningstjenestens rapport *FOKUS 2014* peker på cybertrusselen mot teknologi- og energivirksomheter. Også Olje- og energidepartementet vurderer industrispionasje som en risiko det aktivt må settes i verk forebyggende tiltak mot.

Det har vært en rekke hendelser mot olje- og gassektoren som har bidratt til å sette sikkerhet på dagsordenen. I 2012 ble oljeselskapet Saudi Aramco angrepet av et virus, og 30 000 datamaskiner ble ødelagt. I 2013 skapte Shamoon-viruset ny bekymring da det angrep prosesskontrollsystemer. I august 2014 gikk Nasjonal sikkerhetsmyndighet ut med et varsel til 300 virksomheter i olje- og energiselskaper. Det spesielle med denne situasjonen var ifølge Norsk olje og gass omfanget, antallet virksomheter som var angrepet, og at

[2] Petroleumstilsynet (2011): *Deepwater Horizon-ulykken – Vurderinger og anbefalinger for norsk petroleumsvirksomhet.*

[3] Retningslinje 104 *Anbefalte retningslinjer krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer, 110 Recommended guidelines for implementation of information security in Process Control, Safety and Support ICT systems during the engineering, procurement and commissioning phases, og retningslinje 123 Recommended guidelines for classification of process control, safety and support ICT systems based on criticality.*

det så ut til å være relativt avansert skadevare vedlagt e-postene.

Trusselen mot bransjen har dermed eksistert en tid, og også internasjonalt er bransjen blitt klar over trusselen. En frykter innbrudd og integritetsangrep mot prosesstyringssystemene, og med økende systemintegrasjon kan denne trusselen komme til å øke. En undersøkelse blant 46 selskaper som opererer på norsk sokkel,[4] viser at prosesstyringssystemene (SCADA-systemene) opererer i et miljø som er utsatt for høy grad av trussel for blant annet hacking. Sammenkobling mellom SCADA-systemer og andre IKT-systemer over Internett øker risikoen for bevisste angrep og tilfeldige feil i prosesstyringssystemene. Se også nærmere omtale av SCADA-problematikk i kapittel 13 «Energiforsyning» og kapittel 15 «Vannforsyning».

En uoffisiell, internasjonal undersøkelse blant amerikanske oljeselskaper konkluderer med at 60 prosent av selskapene ikke har en beredskapsplan mot digitale sårbarheter.[5] Det er en oppfatning om at dette også er representativt for selskapene på norsk sokkel. Mens selskapene legger stor vekt på beredskap for brann og eksplosjoner med mer, har mange av dem verken planer eller rutiner for å håndtere en hendelse basert på digitale sårbarheter. Det er få av selskapene som har etablerte rutiner for å koble seg fra Internett eller sperre forbindelsen mellom selskapets IKT-nettverk og selskapets produksjonsnettverk, og bare noen få aktører er tilknyttet VDI-systemet til Nasjonal sikkerhetsmyndighet.

Ved behov for melding om digitale trusler fra myndighetene til bedriftene i olje- og gassektoren har Petroleumstilsynet mulighet til å benytte næringens eget nettverk dersom de ordinære kommunikasjonsløsningene ikke er tjenlige. Ved en hendelse i 2014 sendte Nasjonal sikkerhetsmyndighet melding til Petroleumstilsynet, som brukte kontaktnettet sitt til å varsle bedriftene. Petroleumstilsynet er etterpå blitt kritisert for at meldingen ble gitt til feil personer, og at personer som burde blitt informert, ikke ble det. Det finnes ingen formell prosedyre for melding om digitale trusler fra sikkerhetsmyndighetene til selskapene. Noen selskaper har etablert en egen direkte dialog med sikkerhetsmyndighetene og blir fortløpende oppdatert om trusselbildet gjennom den. De store internasjonale selskapene blir oppdatert fra sine sentrale fagmiljøer. Det kan se ut som om mindre selskaper har en større utfordring når det gjelder å bli oppdatert om nye trusler.

Rapportering av hendelser

Hendelser og nesten-hendelser med alvorlig skadepotensial skal rapporteres til Petroleumstilsynet. Virksomhetene i olje- og gassvirksomheten opplever stadig angrep på IKT-systemene sine. Petroleumstilsynet har ikke avdekket IKT-sårbarheter som årsak til rapporterte hendelser. Varsel til bransjen har kommet fra NSM NorCERT og til det enkelte selskapet.

Petroleumstilsynets regelverk krever varsling av «alvorlig svekking eller bortfall av sikkerhetsrelaterte funksjoner eller barrierer, slik at innretningens eller landanleggets integritet er i fare».[6] Grensen for når digitale hendelser skal rapporteres, og for hva som skal rapporteres til Petroleumstilsynet, kan være noe uklar. Det samme gjelder koordinert innsamling av denne typen data. Uten en koordinert registrering har man begrenset mulighet til analyse av data og læring. Manglende rapportering kan skyldes at uønskede digitale hendelser ikke er tydelig omtalt i forskrift og lov og dermed heller ikke vektlagt i tilsyn. Det kan også skyldes at bedriftene er redde for omdømmet sitt, eller det kan være et uttrykk for at bedriftene ikke anser disse truslene som så alvorlige at de kan få alvorlige konsekvenser for produksjonen. Manglende åpenhet om og utveksling av erfarte digitale trusler gjør at samarbeidet i sektoren ikke er optimalt. Både Petroleumstilsynet og Norsk olje og gass har tatt initiativ til aktiviteter for å få satt arbeidet med digitale trusler på dagsordenen.

Kapasiteter for deteksjon og hendelseshåndtering

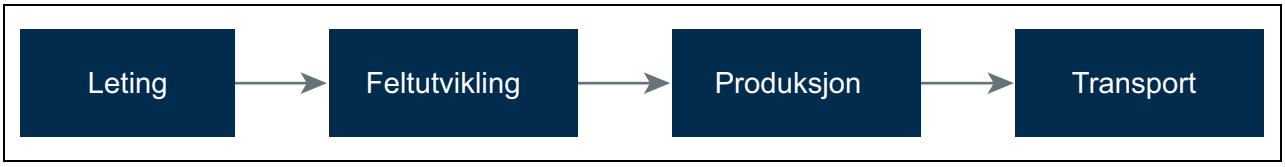
Operatørselskapene har et selvstendig ansvar for å ivareta IKT-sikkerheten hos seg selv og på sine felt. Oljedirektoratet har ingen operativ rolle i forbindelse med hendelser i næringen. Dersom en IKT-hendelse påvirker og fører til stopp i produksjonen og i leveranser fra norsk sokkel, vil Oljedirektoratets beredskapsvakt bli varslet. I gitte situasjoner vil Oljedirektoratet varsle videre til eget

---

4 Johnsen, Stig Ole (2012): *An Investigation of Resilience in Complex Socio-Technical Systems to Improve Safety and Continuity in Integrated Operations.* NTNU.

5 FOX IT (2015): *Cyber security: 60 percent of oil and gas companies do not have an Incident Response Plan in place.*

6 Helse- og omsorgsdepartementet, Klima- og miljødepartementet, Arbeids- og sosialdepartementet (2011): *Forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg (styringsforskriften)*, § 29.



Figur 14.1 Verdikjede olje og gass.

departement. Det er ikke etablert et felles responsmiljø for sektoren.

Det synes som om det er liten grad av myndighetsinitierte øvelser i håndtering av IKT-hendelser i sektoren eller sammen med andre sektorer. Oljedirektoratet har imidlertid deltatt i øvelser initiert av eget departement, men da med vekt på leveransesikkerhet fra norsk sokkel.

14.5 Digitale sårbarheter i olje- og gassektoren

Industrielle automatiserings-, kontroll- og sikkerhetssystemer som benyttes i olje- og gassektoren, er i stor grad digitalisert og avhengige av digital teknologi.

Det er gjennomført noen myndighetstilsyn hos enkeltvirksomheter innenfor olje- og gassektoren når det gjelder IKT-sikkerhet, og Petroleumstilsynet har bedt virksomhetene vurdere sin egen IKT-sikkerhet opp mot retningslinjene til Norsk olje og gass. De samlede resultatene viser at både landanleggene og produksjonsinnretningene har relativt gode systemer og rutiner for IKT-sikkerhet slik de vurderer situasjonen selv, mens riggnæringen kommer noe svakere ut. Dette gjelder spesielt på kriterier som at brukerne må ha tilstrekkelig forståelse for sikkerhetsrisiko og akseptabel bruk av systemene, og planer for gjenopprettelse etter at mulige hendelser har inntruffet.

Tidligere ble det benyttet isolerte og proprietære nett mellom prosessutstyr og kontrollsystemer. Behov for overføring av produksjonsdata til informasjonssystemer, samt fjernvedlikehold, gjør at fullstendig separasjon ikke lenger er praktisk mulig. Den økende bruken av fjernoperasjon fra naboplattformer eller land kan innebære bruk av felles kommunikasjonssystemer, og produksjonsutstyr kan dermed være eksponert for nettverksrelaterte sårbarheter.

14.5.1 Verdikjede

Den norske olje- og gassvirksomheten assosieres ofte med de store produksjonsinstallasjonene som henter hydrokarboner opp fra grunnen, de store landbaserte prosessanleggene som produserer olje- og gassprodukter, og de lange rørledningene på havbunnen som transporterer olje og gass til Europa. I olje- og gassvirksomhetens verdikjede inngår også sentrale ledd som salg, markedsføring, foredling, transport, forskning, myndighetsrapportering med mer. I virksomheten skiller en mellom oppstrømsaktiviteter som de aktiviteter som gjøres for å bringe borestrøm opp fra grunnen og prosessere denne, og nedstrømsaktiviteter som aktiviteter for å bringe olje- og gassprodukter ut til forbrukerne. I alle ledd i både opp- og nedstrømsaktiviteter er informasjonssystemer vitale for alle operasjoner som blir utført.

I de videre diskusjonene i dette kapittelet prioriteres den digitale sårbarheten i de fire leddene i verdikjeden der olje- og gassvirksomheten er spesiell i forhold til annen industri. Det er den digitale sårbarheten i letevirksomhet, under feltutvikling, i produksjonsfasen og i transport av olje og gass til Europa i de store rørledningssystemene. Anlegget på Mongstad er vesentlig i denne verdikjeden.

14.5.2 Letevirksomhet

Letefasen er en informasjonsintensiv fase. Formålet med leteaktivitetene er å finne nye forekomster av hydrokarboner som kan utvinnes. Enorme mengder data blir samlet inn. Disse representerer store verdier for olje- og gasselskapene blant annet for at de skal kunne vurdere verdi og lønnsomhet i mulige nye utbyggingsprosjekter. Kunnskap om verdien av nye felt kan påvirke børsverdien for selskapene. Viktige beslutninger om investeringer og samarbeidsforhold tas basert på informasjon om størrelser og hvilken type sammensetning (olje, gass, kondensat) man finner på feltet.

Den digitale sårbarheten til disse dataene blir primært relatert til beskyttelse mot tilgang til, sletting eller manipulasjon av dataene. Datastrukturene er sammensatte, og man trenger spesialistkompetanse for å kunne tolke og forstå dataene. Et strengt regime for informasjonsforvaltning er nødvendig for å beskytte disse dataene. Det er ikke kjent at det har vært noen hendelser relatert

til digital sårbarhet med denne typen data. Det virker som om bedriftene er bevisste på verdien av sin lete- og utvinningsrelaterte informasjon og beskytter denne godt.

Dokumenter med sammendrag og konklusjoner fra letevirksomhet vil være av meget stor interesse for utenforstående, og kan være et mål for digital spionasje. Digitale sårbarheter som kan føre til at slik informasjon kommer på avveie, består primært i manglende oppmerksomhet og opplæring hos de ansatte, i tillegg til manglende rutiner for klassifisering og behandling av sensitiv informasjon.

Databasen Diskos er sentral i norsk olje- og gassvirksomhet. Diskos er en nasjonal lagringsbase for lete- og utvinningsrelatert informasjon. Databasen er opprettet og utformet av Oljedirektoratet og oljeselskapene som er representert på norsk sokkel. Den inneholder til dels konfidensiell informasjon, og består hovedsakelig av brønn- og seismikkdata for norsk kontinentalsokkel. Mens oljeselskapene ikke har tilgang til hverandres data, har ansatte i offentlig virksomhet slik tilgang. Diskos styres av Oljedirektoratet og inneholder nesten alle kartdata som finnes for norsk sokkel. Riksrevisjonen påpeker at dataene kan ha stor betydning for konkurransen mellom oljeselskapene og være et mål for dataangrep fra andre stater.[7]

Sanntids IKT-systemer er vitale under borevirksomheten. Storulykken på Deepwater Horizon (DwH) skjedde under boring av en brønn på Macondo-feltet i Mexicogolfen. For å illustrere hvordan digitale sårbarheter på en boreplattform kan bidra til ulykker, og hva konsekvensene av en slik ulykke kan bli, er hendelsesforløpet som førte til ulykken gjengitt i boks 14.1.

14.5.3 Feltutvikling

Utvikling og utbygging av nye felt er en investeringsintensiv fase. Mange aktører er involvert, som produsenter av hele eller store deler av installasjonene, utstyrsleverandører og tjenesteleverandører. Konkurransen er hard, og et tilslag på et tilbud kan være avgjørende for et selskap. Olje- og gasselskapene har velfungerende, velprøvde og sikre anbuds- og evalueringsprosesser. Strenge

[7] Riksrevisjonen (2013): *Riksrevisjonens rapport om den årlige revisjon og kontroll for budsjettåret 2013*, Dokument 1 (2014-2015).

Boks 14.1 Deepwater Horizon-ulykken[1]

Den 20. april 2010 skjedde en utblåsing, eksplosjon og brann om bord på den flyttbare innretningen Deepwater Horizon (DwH). Elleve av de som var om bord da ulykken inntraff, omkom, og flere fikk alvorlige skader. Mer enn fire millioner fat olje strømmet ukontrollert ut av brønnen før lekkasjen ble stoppet.

Brønnen var designet slik at den senere skulle kunne brukes som produksjonsbrønn. Under boreprosessen traff man på høyere trykk enn man hadde forventet, noe som førte til endringer i det planlagte boreprogrammet. En måtte også gjøre endringer på grunn av operasjonelle problemer som oppsto underveis. DwH var utstyrt med moderne, databaserte sikkerhetssystemer relatert til overvåking av brønn, avstenging av brønn, frakobling av rigg, kraftforsyning, deteksjon og varsling av mannskap. Under ulykken sviktet alle disse informasjonssystemene helt eller delvis. Det ble i den påfølgende granskingen påvist at det var kjent at flere av informasjonssystemene hadde feil og mangler, og at dette var blitt ignorert og akseptert. Det var flere kjente programvarefeil på riggen. Et nytt system var bestilt, men feil i det nye operativsystemet gjorde at gammel programvare ikke lot seg kjøre på det nye operativsystemet. Noen av riggens alarmsystemer, inkludert riggens generelle alarmsystemer, var slått av. Dette medførte at selv om sensorer på riggen registrerte høye gassnivåer, giftig gass og brann, og overførte disse signalene til brann- og gassvarslingssystemet, ble ingen alarm aktivert. Blowout-preventeren (BOP) stengte ikke av brønnen, slik den skulle gjøre. Det er uklart om den ble skadet under ulykken, eller om den allerede var i ustand. Det var gjort observasjoner om lekkasjer fra BOP-ens hydrauliske kontrollsystem, uten at man hadde gjort noe med dette. Myndighetene hadde krevd en resertifisering av BOP-en, noe som ville gjøre det nødvendig med en nedstenging i 90 dager, men dette var ikke utført.

[1] Vinnem, J.E., Utne, I.B., Skogdalen, J.E. (2011): *Looking Back and Forward: Could Safety Indicators Have Given Early Warnings about the Deepwater Horizon Accident?* Deepwater Horizon Study Group. Working Paper – Jan-2011.

regler sørger for at informasjon om tilbud fra konkurrentene beskyttes, er tilgjengelig for kun et fåtall personer og bare blir benyttet til det som er formålet. Denne typen informasjon kan være et mål for digital spionasje.

Gjennom forskning, erfaring og samarbeid i bransjen har norsk industri bygd opp en bred ekspertise på feltutvikling av olje- og gassinstallasjoner til havs. Dette er kunnskap som gir bransjen konkurransefordeler ved både norske og internasjonale feltutbyggingsprosjekter. Slik kunnskap og dokumentasjon er ettertraktet og må beskyttes.

I byggefasen designes og dokumenteres installasjonene. Dokumentasjon om datanett, adresser med mer utveksles mellom leverandørene og oljeselskapet. Slik informasjon vil være av stor verdi for trusselaktører.

Digitale sårbarheter som kan føre til at slik informasjon kommer på avveie, består primært i manglende oppmerksomhet og opplæring hos de ansatte, manglende rutiner for klassifisering og behandling av sensitiv informasjon og manglende herding og oppdatering av programvare.

Utstyr for prosesskontroll tilpasses og utvikles i byggefasen. Det benyttes standardkomponenter som for eksempel PC-er med Microsoft Windows eller Linux. Det innebærer at kjente sårbarheter for disse kommersielle produktene også vil være til stede. Programvare som utvikles, er i begrenset grad designet, utviklet og testet med tanke på digitale sårbarheter.

Underleverandører spiller en viktig rolle i forbindelse med design og produksjon av nye installasjoner. Det er stor bekymring for at manglende sikkerhetskultur hos underleverandører fører til at digitale sårbarheter etableres i feltutviklingsfasen og blir med prosjektene over i produksjonsfasen.

Konsekvenser av uønskede hendelser grunnet digitale sårbarheter i feltutviklingsfasen er primært av økonomisk art for næringslivet.

14.5.4 Produksjon

Tidligere ble det benyttet proprietære nettverk mellom prosessutstyr og kontroll- og sikkerhetssystemer, mens det i dag ofte benyttes nettverk basert på Internett-teknologi (TCP/IP). Industrielle automatiserings- og kontrollsystemer var tidligere fysisk adskilt fra tradisjonelle informasjonssystemer og åpne nett. Overføring av produksjonsdata til informasjonssystemer og fjernvedlikehold gjør at en slik fullstendig separasjon i dag ikke er praktisk mulig. Dette betyr at produksjonsutstyr kan være mer eksponert for nettrelaterte sårbarheter. Dersom en angriper bryter gjennom forsvarsmekanismene til kontroll- eller sikkerhetssystemet, kan vedkommende blant annet forstyrre kontrollsystemets funksjonalitet ved å forsinke eller blokkere flyten av informasjon eller gjøre uautoriserte endringer i kontrollsystemet.

En amerikansk studie fra 2011 om prosesskontrollsystemer viser at det er flere digitale sårbarheter i slike systemer. Sårbarhetene er rapportert inn til Common Weakness Enumeration-registeret (CWE), der produsenter, forskere og leverandører kan se de siste oppdagede sårbarhetene og arbeide med å lukke dem.[8]

Personell som opererer installasjonene og bemanner kontrollrom, kan påføre installasjonene stor skade. Spredning av ondsinnet kode oppstår oftest på grunn av menneskelige feil. Det åpnes vedlegg i e-post, det settes inn minnepinner, det lades mobiltelefoner, bærbare datamaskiner kobles til kritiske nett, og så videre. Mobiltelefoner kan også lett etablere Internett-forbindelser. Brukere lures til å oppgi passord, med mer. Ved å legge operasjonsrom på land kan oppmerksomheten bli mindre og gi muligheter for flere slike sårbarheter. Mangelfull avlåsing og merking av rom, skap og kabling bidrar også til slike sårbarheter. Utro tjenere med omfattende rettigheter kan påføre virksomheten stor skade.

Fjernoperasjon fra naboplattformer eller fra land kan innebære bruk av felles kommunikasjonsløsninger. For å få redundante nettløsninger benyttes ofte felles, delte datanett. Slike nett kan være sårbare for avlytting, inntrenging og manglende tilgjengelighet, og kommunikasjonsenheter har operatørgrensesnitt som er sårbare. Et tjenestenektangrep på et lite beskyttet segment (for eksempel brukt til underholdningsformål) i et delt nettverk kan medføre at kritiske segmenter blir berørt. Ettersom datanettet går via en rekke plattformer, vil strømstans på én plattform kunne berøre nettforbindelsen fra andre plattformer.

Datanett i Nordsjøen er primært basert på fiberoptisk kabling på havbunnen. Det har vært få skader på denne infrastrukturen, men i områder med grunt vann (15–20 meter) og mye havstrøm har det oppstått 5–6 skader i løpet av de siste 15 årene.

Kontrollsystemene blir anskaffet og drevet i grenselandet mellom to kulturer – informasjons-

[8] Office of Electricity Delievery and Energy Reliability (2011): *Vulnerability analysis of energy delivery control systems.*

teknologi (IT) og operasjonsteknologi (OT). Manglende forståelse mellom disse miljøene kan medføre digitale sårbarheter. Eksempelvis prioriteres normalt konfidensialitet som den viktigste egenskapen i et IT-miljø, mens tilgjengelighet prioriteres høyest i et OT-miljø. Løpende oppdatering av programvare kan aksepteres i et IT-miljø, men kreve mer omfattende testing i et OT-miljø.

Integrerte operasjoner bidrar til integrasjon av organisasjonene som jobber på feltene og på land, ved at personer og team knyttes sammen i avanserte (virtuelle) kommunikasjonsrom. Samtidig kan nye samarbeidsrelasjoner internt i oljeselskapene og mellom leverandørene og oljeselskapene bli skapt. *Integrerte operasjoner* er et bredt begrep, og selskapene legger gjerne noe ulikt innhold i begrepet.

Lavere oljepris og reduksjon i produksjonen vil kunne øke incentivet for å effektivisere driften og ta i bruk integrerte operasjoner. Integrerte operasjoner kan gi konsekvenser for kommunikasjon og samhandling, innføring av ny teknologi og endret beslutningstaking og HMS-ledelse.[9] Når oppgaver flyttes til land og man blir avhengig av at kommunikasjonsnettene er oppe, kan dette endre risikobildet.

Eldre anlegg representerer en større digital sårbarhet enn nye. Kontrollsystemene var isolert og ikke tenkt oppkoblet i nettverk og integrert med andre IKT-systemer. Disse kontrollsystemene inneholder ikke det samme nivået av innebygd sikkerhet som nyere systemer.

Olje- og gassinstallasjoner benytter i stor utstrekning underleverandører med eget utstyr og systemer i komplette pakker i form av moduler/«containere». Dette er ikke minst vanlig i tilknytning til boreoperasjoner. Slike moduler skal knyttes til strøm og nett. Manglende dokumentasjon gjør det vanskelig å kontrollere hvilke digitale sårbarheter hver enkelt av disse modulene medfører.

Konsekvensene av uønskede hendelser basert på digitale sårbarheter i produksjonsfasen vil i første rekke være av økonomisk art. Når produksjonen må stenges, innebærer det tapte inntekter for næringslivet, og samfunnet får reduserte skatter og avgifter. Uønskede hendelser vil få betydning for selskapenes omdømme, noe som igjen kan påvirke Norges omdømme som en stabil produsent og leverandør av energi. Dersom sabotasje- og terrororganisasjoner lykkes i å kontrollere vitalt produksjonsutstyr, kan konsekvensen bli miljøødeleggelse og tap av menneskeliv. Olje- og gassektoren er spesielt utsatt fordi det behandles store mengder brann- og eksplosjonsfarlig materiale, og fordi ansatte bor på installasjonene.

14.5.5 Transport

Norge er en viktig leverandør av olje og gass til Europa. Olje og gass blir i hovedsak levert gjennom rørledninger, men også med skip. Rapporten *The partnership between the Norwegian Oil & Gas Industry and the EU countries,*[10] viser hvor viktige norske gassleveranser til Europa er, og også hvor viktige petroleumsaktivitetene på norsk sokkel er for næringslivet i Europa.

Rørledninger er eksponert for sabotasje og ulykker, siden de i store områder ligger ubeskyttet. I tillegg påvirker automatiserings-, kontroll- og sikkerhetssystemer selve flyten av hydrokarboner i rørene. Disse systemene kan også være sårbare. Rørledningssystemene inkluderer stigerør, prosessanlegg og mottaksterminaler.

Ifølge kravene til beredskap i petroleumsloven skal Gassco til enhver tid opprettholde en effektiv beredskap med sikte på å møte farer og ulykkessituasjoner. Gasscos beredskapsorganisasjon bygger på et nært samarbeid med Statoil og andre tjenesteleverandører, myndigheter og nødetater.

14.5.6 Avhengigheter av andre samfunnsfunksjoner

For å redusere utslipp av CO_2 fra kraftproduksjon på oljeinstallasjonene baserer nye feltutbygginger seg ofte på kraftforsyning fra land (elektrifisering). De fleste av disse installasjonene må stenge produksjonen i tilfelle brudd på kraftforsyningen fra land. Det har over lengre tid vært en økende oppmerksomhet rettet mot digitale sårbarheter i distribusjonssystemer for elektrisk kraft. Slike distribusjonssystemer er komplekse nettstrukturer med stor avhengighet av styring- og kontrollsystemer.

Store avstander og store havdyp gjør at det er kostbart å etablere datanett til oljeinstallasjoner på norsk sokkel. Fiberoptiske kabler på havbunnen kan være utsatt for skade fra byggevirksomhet, fiskeriaktivitet og erosjon. Det kan være utfordrende å etablere redundante og helt uavhengige nettverksløsninger. Manglende kommunikasjon kan bety umiddelbar nedstenging av produksjon på plattformer som opereres fra land eller fra

[9] Oljeindustriens landsforening (nå Norsk olje og gass) (2007): *HMS- og Integrerte operasjoner: Forbedringsmuligheter og nødvendige tiltak.*

[10] ECON (2014): *The partnership between the Norwegian Oil & Gas Industry and the EU countries.*

Boks 14.2 Digital sabotasje på rørledning i Tyrkia

Rørledningen fra Baku i Aserbaidsjan går via Tbilisi i Georgia til Ceyhan i Tyrkia. Statoil er, sammen med ti andre foretak, deleier i rørledningen. Rørledningen er utstyrt med sensorer for hver mil. Trykk, oljeflyt og andre kritiske indikatorer blir sendt til et sentralt kontrollrom gjennom et trådløst overvåkingssystem. Kameraer overvåker hele den 1 099 mil lange rørledningen. Eksplosjonen den 7. august 2008 aktiverte ikke et eneste feilsignal. Tyrkiske myndigheter hevder at en feilfunksjon forårsaket eksplosjonen, kurdiske separatister (PKK) hevder at de står bak. Hovedeieren, British Petroleum, hadde rørledningen operativ igjen etter tre uker.

Det har senere vist seg at 60 timer med overvåkingsvideoer var slettet av hackere. Et infrarødt overvåkingskamera som ikke var koblet til det samme nettverket, viser to menn med bærbare datamaskiner som oppholdt seg i nærheten av rørledningen noen dager før eksplosjonen. Senere undersøkelser har avslørt at hackerne utnyttet et svakt punkt i systemet, selve overvåkingskameraene. Kameraenes kommunikasjonsprogramvare hadde sårbarheter som hackerne brukte til å få tilgang til og komme seg inn i det interne datanettverket. Inne i nettverket fant hackerne en maskin som benyttet et Windows operativsystem, og som var ansvarlig for alarmstyringsnettverket. De kunne plassere egen kode her som gjorde det mulig å snike seg tilbake når de måtte ønske. Det sentrale elementet i angrepet var å få kontroll over styringssystemet, slik at de kunne øke trykket i rørledningen uten at alarmer ble utløst. Angriperne kunne infiltrere programvaren på flere ventilstasjoner uten å trenge inn i hovedkontrollsentralen. De kunne øke trykket slik at det forårsaket en eksplosjon, og de kunne manipulere overvåkingssystemene slik at det ikke ble sendt meldinger om feilfunksjonering og lekkasjer til kontrollrommet.

naboplattformer. Dette er også kritisk for rørledninger, der blant annet trykk og mengde må kunne reguleres og overvåkes i hele systemet.

Avhengighet av kraftforsyning

Kraftproduksjon på land som alternativ til kraftproduksjon på olje- og gassinstallasjonene er et miljøtiltak som nå innføres på en rekke installasjoner. I henhold til Innstilling nr. 114 (1995–1996) fra Stortingets energi- og miljøkomite besluttet Stortinget (St.prp. nr. 65 (1996–97)) at «ved alle nye feltutbygginger skal det legges fram en oversikt over energimengden og kostnadene ved å elektrifisere installasjonen framfor å bruke gassturbiner».

Martin Linge blir det sjuende feltet på norsk sokkel som får strømtilførsel fra land. Til nå er tilsvarende løsning etablert for feltene Gjøa, Valhall, Ormen Lange, Troll A, Snøhvit og Goliat. Stortinget har besluttet at Johan Sverdrup-feltet skal få dekket kraftbehovet sitt fra land, og at feltene Gina Krog, Ivar Aasen og Edvard Grieg senest innen 2022 skal forsynes med kraft fra land.[11]

Det store energibehovet til en olje- og gassinstallasjon stiller krav til elektrisitetsproduksjon og infrastruktur på land og vil ha betydning for den innenlandske kraftbalansen. Utfall i leveranse av elektrisk kraft vil føre til at produksjonen på installasjonen stopper.

Sikring av systemene som styrer norsk kraftforsyning, er regulert i forskrift om beredskap i kraftforsyningen. De elektriske anleggene som forsyner landanlegg og petroleumsinstallasjonene, er ikke omfattet av disse bestemmelsene, men er regulert av Petroleumstilsynets forskrifter.

Avhengighet av elektronisk kommunikasjon

Datakommunikasjon til oljeinstallasjoner på kontinentalsokkelen er primært basert på fiberoptisk kabel, men i noen grad også radiolinje eller satellittkommunikasjon. Firmaet Tampnet opererer det største offshore kommunikasjonsnettverket i Nordsjøen og betjener de fleste olje- og gassinstallasjoner i Nordsjøen ved fiberkabler og punkt-til-punkt radiolinjeforbindelser. Tampnet har dermed en unik rolle som leverandør av infrastruktur til norsk olje- og gassvirksomhet. De kan tilby redundans ved å kombinere linjeforbindelsene, og reduserer dermed sårbarheten for utfall. Tampnets hovedprodukt er stabil og pålitelig fysisk kommunikasjon mellom to punkter. Sikring av trafikken på nettverket og bruk av nettverket er brukeren selv ansvarlig for.

[11] Norges vassdrags- og energidirektorat (2015): *Kraft fra land til Johan Sverdrup-feltet.*

En av de viktigste endringene som nå pågår i petroleumsvirksomheten, er relatert til bruk av IKT. IKT-baserte løsninger og samhandlingsmønstre innen leting, reservoarstyring, boring, drift, vedlikehold og logistikk er i fokus. Nye driftsformer skaper nye risikomomenter. Personell på land overvåker prosesser på plattformer og rigger, og de mottar mye informasjon. Økt utnytting av IKT kan lede til økt avhengighet og økt sårbarhet. Den digitale sårbarheten vil øke ved økt automatisering og fjerndrift. Med fjerndrift gjør man seg helt avhengig av en elektronisk kommunikasjonsinfrastruktur og pålitelige prosesstyrings- og IKT-systemer. Her er det mange utfordringer, ikke minst når det gjelder informasjonssikkerhet, og da spesielt tilgjengelighet og integritet. Digitaliseringen innebærer bruk av videokonferanser og video-overvåking (CCTV), blant annet i forbindelse med drillingoperasjoner og i forbindelse med overvåking av helse, miljø og sikkerhet. Trenden er at gamle analoge systemer blir integrert med digitale systemer, og at kommunikasjon går over IP.

Den teknologiske utviklingen har også ført med seg økt bruk av fjernstyrte undervannsbåter. Mer enn halvparten av norsk olje- og gassproduksjon skjer ved hjelp av undervannsbrønner, og denne andelen blir stadig større. Disse blir ofte operert fra såkalte flerbruksfartøyer, som vanligvis er skip, lekter eller halvt nedsenkbare innretninger. Fartøyene kan være utstyrt for konstruksjon og vedlikehold av faste installasjoner, ha boligkapasitet, tilby tjenester som lagerplass, vann-, trykkluft- og elektrisitetsforsyning, kontorplass, kommunikasjonssentral og landingsplass for helikoptre. Personellet på flerbruksfartøy kan bestå av mange faggrupper. På skipene etterspør de datanettverk og større båndbredde. Det er flere utganger til mobilnettet. Hvis ikke det er til stede, går kommunikasjonen via satellitt. Mannskapet kan bruke ulike simkort, ett til sjøs og ett i land. MCP, som leverer mobiltjenester offshore, ser på kompresjon av mobiltrafikk for å kunne dekke viktig datatrafikk.

Avhengighet av satellittbaserte tjenester

Det er stor skipsaktivitet i tilknytning til olje- og gassvirksomheten. Maritim navigasjon er i dag basert på en rekke typer utstyr som kan brukes uavhengig av hverandre. Mye navigasjonsrelatert utstyr ombord på et fartøy er tilkoblet GPS og bruker posisjonsinformasjon fra GPS for utstyrets sekundære funksjoner. Det gjelder blant annet radar og gyrokompass. Integrasjon av systemer om bord og hvordan disse er avhengige av hverandre, kan variere fra skip til skip. Ved plutselig tap av GPS-signaler vil denne integrasjonen av systemer i mange tilfeller skape et komplekst alarmbilde og et behov hos navigatøren for å skaffe seg oversikt over hvordan ulike typer navigasjonsutstyr er påvirket, og hvordan ulike navigasjonshjelpemidler kan benyttes under den videre navigasjonen.[12]

En rekke fartøy holder seg tett inntil oljeinstallasjonene ved hjelp av dynamiske posisjoneringssystemer (DP) som er avhengige av posisjonssignaler fra satellitt. Et DP-system er et styringssystem som automatisk holder skipet i en posisjon eller på en programmert rute, samt holder skipets retning konstant. Dette skjer ved hjelp av aktiv styring av propeller, thrustere og ror. Et fellestrekk ved DP-systemer er at de anvender satellittnavigasjon (GPS og GLONASS) som posisjonsreferansesystem for nøyaktig posisjonering. Gyrokompass, vind-, strøm- og bølgesensorer, akustiske systemer, treghetsnavigasjon, mikrobølgesystemer og laser inngår som støtte- og reservesystemer. Data fra sensorsystemene overføres kontinuerlig til datamaskiner som beregner nødvendig pådrag for å posisjonere fartøyet med tilstrekkelig nøyaktighet i forhold til kravene for spesifikke operasjoner.[13]

En kollisjon mellom en plattform og for eksempel et forsyningsfartøy eller en flytende boligplattform kan få alvorlige konsekvenser. På samme måte kan feil i posisjoneringssystemer føre til alvorlige hendelser i forbindelse med dykkeaktivitet. Antall fartøyer på kollisjonskurs er blitt sterkt redusert de siste årene, blant annet på grunn av utvidet radarovervåking av installasjonene.

14.5.7 Kompetanse og sikkerhetskultur

Forståelsen for den digitale sårbarheten i virksomheten og evnen til å innføre tilstrekkelige tiltak for å beskytte seg mot digitale trusler er relatert til kulturen i virksomheten. En god kultur for å ta de digitale truslene på alvor er avhengig av den generelle sikkerhetskulturen i sektoren og vilje til å bruke ressurser på adekvate og tilstrekkelige tiltak. Petroleumstilsynet sier i sin

---

[12] Norsk romsenter (2013): *Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur.*

[13] Ibid.

hovedrapport[14] etter gjennomgangen av DwH-ulykken blant annet:

> «Sikkerhetskulturen i Olje- og Gassnæringen har en sammenheng med kostnadskutt, utsatt vedlikehold og manglende investeringer i sikkerhetssystemer. Dette er et ledelsesansvar. I stedet for å ta inn over seg usikkerheten aktørene står overfor i forkant av en uventet hendelse, klandrer vi dem for at de ikke på forhånd skjønte det vi ser så tydelig i ettertid. I stedet for å lære noe om hvor stor usikkerhet vi står ovenfor i beslutningene vi fatter, blir vi etterpåkloke. Igjen blir konsekvensen at vi undervurderer behovet for robuste beslutninger fordi vi lærer oss å undervurdere usikkerhet om fremtiden.»

Granskningsrapporten etter terrorangrepet mot Statoils gassanlegg i In Amenas i 2013 viste blant annet til at arbeid med sikkerhet ikke hadde fått like stor oppmerksomhet som det tradisjonelle HMS-arbeidet. Rapporten inneholdt flere anbefalinger og pekte blant annet på viktigheten av å definere en ambisjon for selskapets sikkerhetsarbeid, og at sikkerhet måtte være en integrert del av virksomheten gjennom en helhetlig sikkerhetstilnærming.[15]

Fagmiljøene innen IKT-sikkerhet og prosess er adskilte, noe som er en utfordring for samhandlingen og helheten i sikkerhetsarbeidet. Dersom en stopper en prosess i automasjonsverdenen, vil det kunne gi større skade enn selve hendelsen. Tradisjonelt har IKT-sikkerhet vært konsentrert om kontorstøttesystemer, mens prosessikkerhet omhandler hydrokarboner, høyt trykk og fysiske og mekaniske prosesser. I en doktorgradsavhandling fra 2012 pekes det på forutsetninger for trygg og sikker fjerndrift og fjernstøtte. Blant disse fremheves god design av arbeidsprosesser og systemer, samspill i distribuerte team, stabilitet og kvalitet i kommunikasjon og systemer, sikker-tilstands-prosedyre og en proaktiv ledelse.[16]

14.6 Fremtidige problemstillinger og trender

Investeringsviljen til tiltak for å forebygge digitale trusler i olje- og gassvirksomheten på norsk sokkel vil bli utfordret i nedgangstider. Viljen til å investere i sikringstiltak i et område der man så langt ikke har hatt alvorlige konsekvenser av hendelser, vil bli satt på prøve.

Forskning og utvikling pågår for å bringe frem løsninger for å navigere, analysere og kombinere store datamengder. Dette skaper ikke bare muligheter for olje- og gassvirksomheten, men også nye trusler. Intelligente enheter som kan motta kontrollsignaler utenfra, kan manipuleres hvis ikke tilgangen beskyttes godt nok. Ved å analysere store datamengder kan man avdekke mønstre som avslører rutiner i anvendelse, bruksmønster, svakheter og mangler i teknologi, tilstand på utstyr, og så videre.

Stadig smartere og flere sensorer overvåker og kontrollerer de fysiske prosessene. Nye forretningsmodeller der leverandørene selv får ansvar for å samle inn, overvåke og forbedre eget utstyr, diskuteres i sektoren. Dette vil gjøre det nødvendig at leverandørene får bedre tilgang til sensordata og innsamlet historikk, samt mulighet til å oppdatere programvaren sin. Flere aktører med tilgang til kritiske produksjonssystemer vil øke eksponeringen for inntrenging av skadelig programvare.

Mange av innretningene på norsk kontinentalsokkel er designet for en levetid på mellom 15 og 25 år, og en rekke av disse har fått samtykke til forlenget levetid. Det betyr at mye av utstyret og programvaren er utdatert. Se ytterligere omtale i punkt 5.6 «Teknologiarven».

Digitaliseringen av sektoren pågår kontinuerlig. Tingenes Internett vil føre med seg flere enheter med digitale sårbarheter. Mengden av data som skal transporteres, øker, og standard IKT-utstyr vil i større grad være integrert med de spesialiserte styresystemene.

14.7 Vurderinger og tiltak

Det er utvalgets oppfatning at dagens sikkerhets- og tilsynsregime gitt med hjemmel i petroleumsloven er for svakt med tanke på den viktigheten anlegg på norsk sokkel har for norsk økonomisk bæreevne og for Norges internasjonale betydning og omdømme som olje og gass-leverandør. IKT-sikkerhetsnivået er i dag bestemt av bransjen selv gjennom egenutviklede standarder

---

[14] Petroleumstilsynet (2011): *Deepwater Horizon-ulykken – Vurderinger og anbefalinger for norsk petroleumsvirksomhet.*

[15] Granskningsgruppe (2013): *Angrepet mot In Amenas – Rapport fra granskningen av terrorangrepet mot In Amenas.* Utarbeidet for styret i Statoil ASA.

[16] Johnsen, Stig Ole (2012): *An Investigation of Resilience in Complex Socio-Technical Systems to Improve Safety and Continuity in Integrated Operations.* NTNU.

basert på ISO-standardene for sikkerhetsledelse. I sektoren ser man et behov for å oppdatere disse retningslinjene. I revisjonsarbeidet som pågår, er Petroleumstilsynet ikke invitert med. Utvalget ser at denne modellen gir et sterkt eierskap for bransjen. Den frakoblede myndighetsrollen er uheldig med tanke på de samfunnshensynene som rent bedriftsøkonomisk styring ikke ivaretar. Uønskede hendelser i digitale systemer på norsk sokkel, som i neste omgang kan gi utslag i fysisk skade på anlegg, jf. Tyrkia-hendelsen og Stuxnet, kan få store konsekvenser, ikke bare for Norge, men også for Norges viktige kunder i utlandet. I ytterste konsekvens får alvorlig svikt i leveransene konsekvenser for land som importerer store deler av sin gass og olje fra Norge. Utvalget mener at anlegg på norsk sokkel har betydning for vitale samfunnsinteresser og rikets sikkerhet, og at det ikke kan utelukkes at alvorlige hendelser kan inntreffe i fremtiden. Dette taler for en revisjon av sikkerhets- og tilsynsregimet sektoren har i dag. Utvalget anbefaler følgende:

14.7.1 Overføre sikkerhetstradisjonen innen HMS til det digitale området

Olje- og gassektoren har en lang sikkerhetstradisjon, en sterk sikkerhetskultur og høy kompetanse når det gjelder HMS. Selskapene har selv bygd ut infrastrukturen som er på norsk sokkel, inklusiv kommunikasjonsinfrastruktur. Arbeidet med IKT-sikkerhet er også så langt drevet av bransjen selv og Norsk olje og gass, samt gjennom initiativer til samarbeid som den enkelte virksomhet tar overfor Nasjonal sikkerhetsmyndighet og andre sikkerhetsvirksomheter. Bransjen selv har tatt initiativ for bedre IKT-sikkerhet og utviklet en felles standard for sikkerhetsstyring, samt etablert samarbeid innen forebyggende sikkerhet.

Det funksjonelle regelverket plasserer et stort ansvar på virksomhetene, som daglig opplever digitale trusler. For å redusere risiko implementerer selskapene barrierer, dels for å hindre at en uønsket hendelse skjer, dels for å redusere konsekvensene av en uønsket hendelse som har inntruffet. Det har vært økende oppmerksomhet rundt barrierer som hindrer en uønsket hendelse, men kvaliteten på disse barrierene er i liten grad testet og verifisert. *Utvalget mener at bransjen bør videreutvikle den gode sikkerhetstradisjonen innen HMS, og overføre denne tradisjonen til det digitale området. Utvalget vil her henvise til arbeidet som gjøres i EU med hensyn til personvern og IKT-sikkerhet.*

14.7.2 Verdivurdere sektorens anlegg og IKT-systemer, og etablere regelverk for digitale sårbarheter

Sikkerhetsloven og dens virkeområde er under revisjon. I påvente av ny sikkerhetslovgivning og en eventuell implementering av NIS-direktivet fra EU bør krav til IKT-sikkerhet gjøres tydelig i forskrifter. Kapittel 9 i petroleumsloven stiller krav til sikkerhet. I 2013 fikk Petroleumstilsynet også ansvar for sikring og beredskap mot bevisste anslag, slik det fremgår av petroleumsloven § 9-3. Den omtalte lovparagrafen har ingen forskrifter eller juridiske forarbeider knyttet til seg. De sentrale forskriftene for den digitale sårbarheten i sektoren finnes i HMS-forskriftene for petroleumsaktiviteten og i arbeidsmiljøforskriftene. Forskriftene er ikke konkrete når det gjelder digitale trusler, men omfatter implisitt også digital sikkerhet. *Utvalget mener at det bør foreligge krav fra tilsynsmyndigheten (Petroleumstilsynet) om at barrierer mot digitale sårbarheter skal være etablert.*

Ingen av olje- og gassinstallasjonene er per i dag definert som skjermingsverdige objekter i henhold til sikkerhetsloven. Behovet for beskyttelse bør uansett vurderes i lys av virksomhetens betydning for statens inntekter, og – som utvalget har påpekt ovenfor – den internasjonale betydningen olje- og gasseksporten har for våre viktige samarbeidspartnere. *I påvente av ny sikkerhetslov, samt eventuelle pålegg og direktiver fra EU, anbefaler utvalget at det settes i gang et arbeid med verdivurdering og klassifisering av anlegg og IKT-systemer.*

14.7.3 Tydeliggjøre rolle og kapasitet hos Petroleumstilsynet

Det norske tilsynsregimet i olje- og gassektoren er basert på prinsippet om internkontroll, trepartssamarbeidet og risikobasert tilnærming innen HMS. Det norske regimet kan derfor virke overordnet og ikke detaljstyrende på forhold som blant annet har med den digitale sikkerheten å gjøre. Det norske regelverket inneholder en rekke krav som regulerer myndighetenes kontroll av selskapene, i tillegg til å regulere søknader, rapporter, varslinger med mer fra selskapene til myndighetene. Selskapene har kunnskap om verdikjeden. Petroleumstilsynet har faglig myndighetsansvar for sikkerhet, beredskap og arbeidsmiljø i petroleumsvirksomheten på norsk kontinentalsokkel, samt på enkelte anlegg på land.

Utvalget observerer at Petroleumstilsynet har verdikjedekompetanse og kompetanse på teknisk

sikkerhet i sektoren, men begrenset kapasitet når det gjelder tilsyn med sektorens IKT-sikkerhet og sårbarhet. *Utvalget foreslår derfor at Petroleumstilsynet styrkes betraktelig på dette området.*

14.7.4 Vurdere tilknytning til responsmiljø for IKT-hendelser

Sektoren mangler et felles responsmiljø. Bransjen er internasjonal og består av utenlandske og norske selskaper. De utenlandske selskapene kan være del av større internasjonale konsern og ha sikkerhetssamarbeid via sitt moderselskap eller eget responsmiljø innad i virksomheten. Bare noen få aktører i bransjen er tilknyttet NSM NorCERT. De små selskapene, som ikke er en del av et CSIRT-samarbeid, faller utenfor. Det er ikke etablert noe felles kontaktpunkt for sektoren som myndighetene eksempelvis kan benytte til varsling om nettbaserte angrep. Det er også få formelle fora der sektoren kan utveksle erfaringer. *Utvalget anbefaler at virksomhetene i sektoren enten inngår et samarbeid med KraftCERT eller finner andre løsninger for operativt samarbeid.* Ved valg av KraftCERT kan sektoren oppnå synergier som følge av likhet i teknologi, slik som styringssystemer. Dette er i tråd med løsninger som er valgt internasjonalt, slik som blant annet ICS-CERT i USA. Dette vil eventuelt aktualisere en debatt om alternativ tilknytning for KraftCERT.

Barrierer som reduserer konsekvensene av en uønsket hendelse, er mer mangelfulle i bransjen enn forebyggende barrierer. Det har vært økende oppmerksomhet rundt barrierer som hindrer en uønsket hendelse, men kvaliteten på disse barrierene er i liten grad testet og verifisert. Bransjen har en egen beredskapsorganisasjon som skal tre i kraft ved større hendelser, jf. sivilt beredskapssystem. Utvalget er ikke kjent med at denne har øvd på å håndtere store IKT-hendelser. *Utvalget anbefaler derfor at sektoren gjennomfører øvelser i håndtering av uønskede IKT-hendelser.*

Kapittel 15
Vannforsyning

Samfunnet forventer at vannforsyningen er så robust at vannverket kan levere nok og godt vann selv om vannforsyningssystemet utsettes for ulike typer trusler og påkjenninger. Dette gjelder også ved utfordringer som oppstår som følge av digitale sårbarheter.

I dette kapittelet har vi konsentrert oss om vannforsyning. Mange av de problemstillingene vi beskriver, har imidlertid direkte overføringsverdi til avløpshåndtering. Svikt i vannforsyningen vil også medføre svikt i avløpshåndteringen. Uten vann til å transportere avløpet i ledningsnettet vil avløpsnettet bli tilstoppet. Konsekvensene av dette ville svært fort blitt uakseptable og uhygienisk.

I en undersøkelse utført av Myndigheten för samhäldsskydd och beredskap (MSB), som kartla SCADA-sikkerhet i svensk vannforsyning, heter det i konklusjonen:

> «Resultaten från enkäten indikerar att kunskaperna om informationssäkerhetsfrågor hos personal inom svensk dricksvattenförsörjning är relativt låg (…) Dessutom är kunskapen om befintliga riktlinjer och föreskrifter ofta bristfällig.»[1]

I en fersk undersøkelse utført av Mattilsynet i 2015[2] ble det sendt ut et spørreskjema til om lag 500 vannverk.[3] Undersøkelsen viser de samme tendensene som den svenske.

Utvalgets omtale av vannforsyning er basert på innspill fra SINTEF.

15.1 Vann- og avløpsinfrastruktur

Sikker vannforsyning er i stadig større grad avhengig av robuste digitale systemer. Vannforsyningen styres og forvaltes i dag via SCADA, ledningsdatabaser, adgangskontroll og en rekke andre IKT-baserte systemer. Økende bruk av driftskontrollsystemer (DKS)[4] innen drift av vann- og avløpssystemer (VA-systemer) gir bedre overvåking og styring og dermed økt effektivisering, pålitelighet og produktivitet. Samtidig gjør denne digitaliseringen VA-sektoren sårbar for nye typer farer og trusler.

Figur 15.1 viser bruken av DKS innen vannbransjen – fra nedbørfelt via vannbehandling og distribusjonsnett til avløpsnett og videre til avløpsrenseanlegg.[5] Driftskontrollsystemet brukes til å styre og overvåke vann- og avløpssystemene og til å overvåke ulike målepunkter både i nedbørfelt, i nettet og i prosessanlegg. Ulike utestasjoner er også koblet til driftskontrollsystemet, som for eksempel vannpumpestasjoner, høydebasseng, reduksjonskummer, målekummer, avløpspumpestasjoner, påslippspunkter, avløp, overløp, nedbørstasjoner, vassdragsmålestasjoner og bekkerister. Prosessanlegg (vannbehandlingsanlegg og avløpsrenseanlegg) har ofte egne driftskontrollsystemer som samler inn tilsvarende informasjon fra ulike målere/sensorer i disse anleggene.

For en del vannverk har det historisk sett vært vanlig med ulike DKS-er for henholdsvis ledningsnett og prosessanlegg, gjerne med en eller annen form for overføring av måleverdier og alarmer mellom systemene. DKS-ene består av ulike elektroniske komponenter som er plassert i et stort geografisk område. Systemene varierer i oppbygging fra vannverk til vannverk.

---

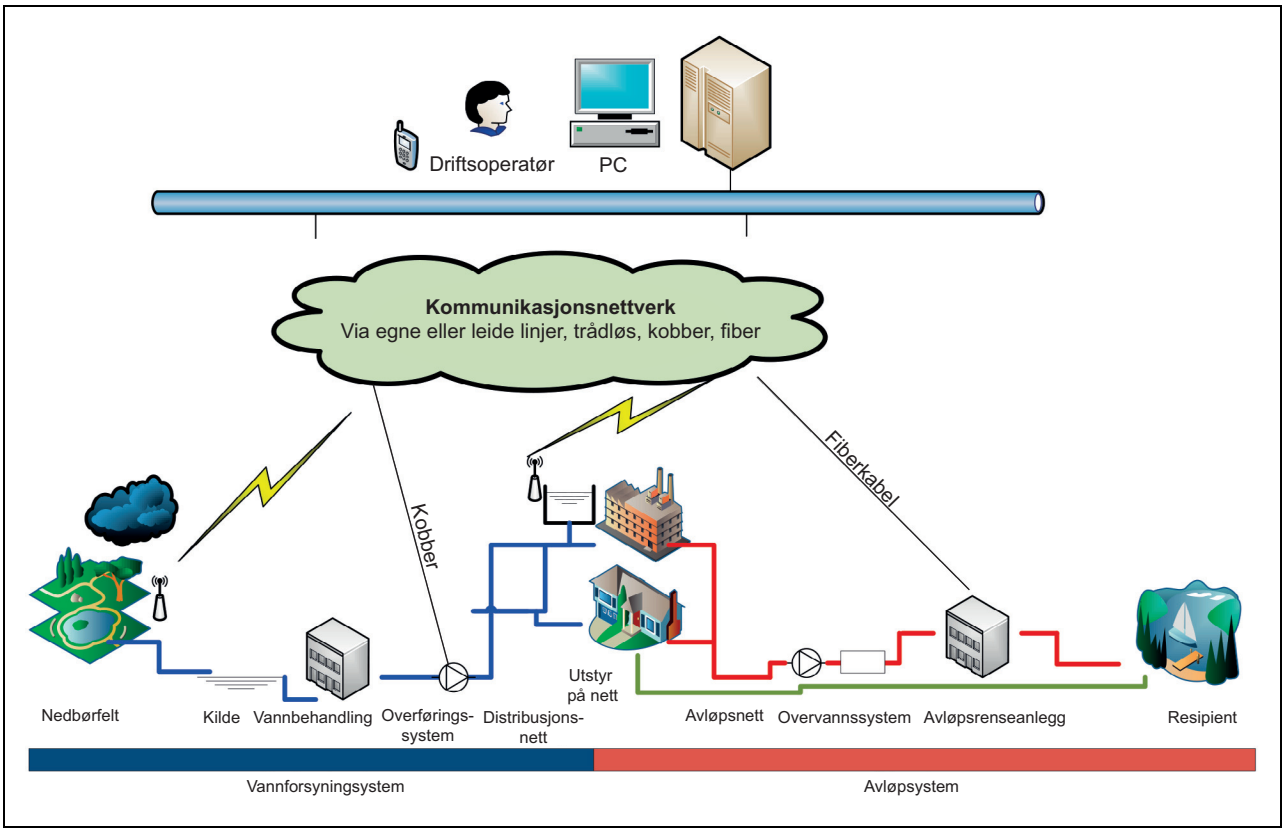
1 MSB (2010): *Kartläggning av SCADA-säkerhet inom svensk dricksvattenförsörjning.*

2 Undersøkelsen er ikke publisert.

3 Norsk Vann. Rapport 195/2013: *Sikkerhet og sårbarhet i driftskontrollsystemer for VA-anlegg.* 11.03.2013. Undersøkelsen var basert på sjekklisten utarbeidet i Norsk Vann. Rapport 195/2013.

4 *Driftskontrollsystem* brukes synonymt med SCADA-system, se for øvrig kapittel 13 «Energiforsyning».

5 Som beskrevet i Norsk Vann (2013): Jaatun M.G., Røstum J. og Petersen S. (2013): *Veiledning for sikkerhet av driftskontrollsystemer for VA-systemer.*



Figur 15.1 Vann og avløp fra nedbørfelt til resipient med angitte eksempler på hvordan driftskontrollsystemer styrer og overvåker (figur hentet fra Norsk Vann. Rapport 195/2013).[1]

[1] Jaatun M.G., Røstum J. og Petersen S. (2013): *Veiledning for sikkerhet av driftskontrollsystemer for VA-systemer.* Norsk Vann. Rapport 195/2013.

15.2 Roller og ansvar

I Norge er totalt cirka 1 800 vannverk registrert i Vannverksregisteret, hvorav cirka 1 100 kommunale eller interkommunale.

Vannforvaltningen i Norge er sektorisert med en forvaltning og et lovgrunnlag som er delt på flere departementer. Det innebærer at det relevante lovgrunnlaget for vannverk fremstår som noe uoversiktlig. Dette forholdet har vært påpekt ved flere anledninger, og Helse- og omsorgsdepartementet har derfor fått rollen som overordnet «vannmyndighet». Ansvaret er likevel fordelt på mange aktører. Hovedaktøren er kommunene som eier og drifter over 90 prosent av alle norske vannverk.

Helse- og omsorgsdepartementet (HOD) har det overordnede ansvaret for norsk vannforsyning og avløpshåndtering og fastsetter forskrifter.

Klima og miljødepartementet har ansvar for rammebetingelsene for kommunenes vann- og avløpsgebyr.

Mattilsynet har ansvar for blant annet matloven og for godkjenning og tilsyn etter drikkevannsforskriften.

Nasjonalt folkehelseinstitutt er faglig rådgiver for HOD, Helsedirektoratet (Hdir), Helsetilsynet (Htil), Mattilsynet og andre når det gjelder helsefaglige spørsmål om blant annet vannforsyning/drikkevann. Miljødirektoratet er ansvarlig for vannforskriften og forurensningsforskriften.

Miljødirektoratet er ansvarlig for vannforskriften og forurensningsforskriften.

Norges vassdrags- og energidirektorat (NVE) behandler konsesjonssøknader og meldinger etter § 8 i vannressursloven.

Direktoratet for samfunnssikkerhet og beredskap (DSB) er nasjonal brannmyndighet og gir føringer for brannvern overfor befolkningen, virksomheter og kommunene. DSB forvalter lov om kommunal beredskap.

Nasjonal sikkerhetsmyndighet (NSM) fører tilsyn etter sikkerhetsloven med objektsikkerhetsforskriften. Noen av vannverkene i Norge er definert som skjermingsverdige objekter.

Fylkesmannen er forurensningsmyndighet for en rekke virksomheter. Fylkesmannen gir utslippstillatelser og fører tilsyn og kontroll etter forurensningsloven, forskrifter og tillatelser og etter lov om kommunal beredskapsplikt.

Vannverkseieren bygger og driver vannverk i tråd med gjeldende regelverk.

Utvalgte *fylkeskommuner* har rollen som vannregionmyndighet, med et særlig ansvar for å koordinere prosessen med å gjennomføre planarbeidet i tråd med vannforskriften.

Kommunene er i hovedsak eierne av vann- og avløpsanlegg og har ansvar for overordnet areal og teknisk planlegging. Kommunene skal påse at alle bygninger har vann og avløp før det blir gitt byggetillatelse. De er også forurensningsmyndighet for avløpsanlegg i mindre tettbebyggelser.

15.3 Hjemmelsgrunnlag og tilsynsvirksomhet

Drikkevannsforskriften[6] med tilhørende veileder er grunnleggende i norsk drikkevannsarbeid. Drikkevannsforskriften er fastsatt med hjemmel i lov om matproduksjon og mattrygghet mv. (matloven), lov om helsemessig og sosial beredskap og lov om folkehelsearbeid (folkehelseloven). Det er vannverkseieren som er ansvarlig for at forsyningen av drikkevann oppfyller kravene til tilfredsstillende mengde og tilfredsstillende kvalitet.

Dagens drikkevannsforskrift med tilhørende veileder fokuserer i liten grad på IKT-sikkerhet. Det samme gjelder sikkerhets- og beredskapsveiledningen fra Mattilsynet fra 2006.[7] Norsk Vanns nye lærebok[8] innen vann- og avløpsteknikk fra 2014 omhandler ikke IKT-sikkerhet og bruk av IKT innen vannbransjen.

Mattilsynet er godkjennings- og tilsynsmyndighet for vannverk. Andre viktige lover som påvirker sikkerheten i vannforsyningen, er sikkerhetsloven og sivilbeskyttelsesloven.

15.4 Beredskap og krisehåndtering

Som det går frem av lov om kommunal beredskapsplikt, har hver enkelt vannverkseier, altså i hovedsak hver enkelt kommune, et selvstendig ansvar både for å iverksette forebyggende tiltak for å hindre uønskede hendelser og kriser og for å håndtere situasjonen om en hendelse skulle oppstå. Planer for å håndtere uønskede hendelser skal gå frem av kommunens kriseplanverk. Dette gjelder både for tilsiktede og utilsiktede hendelser.

Det er per i dag ikke etablert en felles funksjon eller et responsmiljø som kan oppdage og bidra til å håndtere eventuelle digitale angrep, slik vi finner i andre sektorer. Kommunal- og moderniseringsdepartementet har imidlertid tatt initiativ til å bygge opp en CERT-ordning.

15.5 Digitale sårbarheter i vannforsyningen

15.5.1 Bruk av driftskontrollsystemer innen vannforsyning

Digitale avhengigheter fører med seg økt kompleksitet og nye sårbarheter. Vannforsyningen benytter i dag i økende grad IKT-systemer og fjernstyring i alle deler av driften. IKT er blitt en integrert del av vannforsyningssystemet og fremstår som en egen infrastruktur i vanninfrastrukturen.

Driftskontrollsystemer (DKS) for styring og overvåking av anleggene er i seg selv et av de mest sårbare punktene i et vannforsyningssystem.

Økt bruk av DKS innen vannbransjen har gjort det mulig å effektivisere driften. Det reduserer kostnadene, og færre ansatte trengs for å drifte anleggene. Videre kan man nå innføre bedre tjenester, som tilbyr raskere responstid ved hendelser og bedre overvåking av anleggene. Systemene

Boks 15.1 Svikt i DKS

En av de mest klassiske hendelsene knyttet til svikt i DKS innen vannsektoren er Maroochy Shire-hendelsen i Australia i år 2000, der en tidligere innleid IT-konsulent hadde installert DKS som styrte 300 pumpestasjoner for avløp via radiokommunikasjon. Konsulenten fikk ikke jobb i vannverket og hevnet seg ved å manipulere pumpestasjoner, ventiler og luker slik at en million liter ubehandlet avløpsvann rant ut i nærliggende vassdrag.[1]

[1] J. Slay and M. Miller: *«Lessons Learned from the Maroochy Water Breach» in Critical Infrastructure Protection*, vol. 253, E. Goetz and S. Shenoi, Eds., ed: Springer Boston, 2007, pp. 73–82.

[6] Helse- og omsorgsdepartementet (2002): *Forskrift om vannforsyning og drikkevann (Drikkevannsforskriften)*.

[7] Mattilsynet 2006: *Økt sikkerhet og beredskap i vannforsyningen. Veiledning.*

[8] Norsk vann (2014): *Vann- og avløpsteknikk.*

har samtidig gjort sektoren mer sårbar for nye typer trusler. DKS har gått fra å være lukkede systemer som bare virket på egne maskiner, til å bli integrerte systemer som også er tilknyttet kontorstøttesystemer og Internett. Det er kjent at IKT-baserte styringssystemer kan manipuleres på ulike måter, noe som gjør at systemene i seg selv kan utgjøre en sikkerhetsrisiko.

Vann- og avløpssektoren kjennetegnes av geografisk spredt infrastruktur. Særlig gjelder dette vann- og avløpsnettet, som har anlegg og utestasjoner lokalisert der behovet for anlegg finnes (kummer, pumpestasjoner og så videre). Tilhørende IKT-infrastruktur må følgelig være tilsvarende geografisk plassert. For prosessanleggene, som for vannbehandling og avløpsrensing, er alt utstyr samlet i én eller flere bygninger, og den geografiske utfordringen er mindre. Dette gjør fysisk sikring enklere.

I dag kan pumper og ventiler fjernstyres og overvåkes mye enklere enn tidligere. Større anlegg, som vannbehandlingsanlegg og avløpsrenseanlegg, er også blitt mer kompliserte og krever avansert styring av de ulike integrerte prosessene. Nye vannbehandlingsanlegg er kompliserte prosessanlegg med mange komponenter, signaler i styringssystemet og prosess- og analyseinstrumenter. Manuell drift av de mest komplekse vannbehandlingsanleggene er ikke mulig, spesielt ikke over lengre perioder. Ved hurtige endringer i inngangsdataene, slik som ved endringer i råvannskvalitet under flomperioder, er det behov for raske endringer i driftsbetingelsene. Dette forutsetter styring av anleggene via driftskontrollsystemer.

Vannbransjens ønske om reduserte lekkasjer og effektivisering medfører økt bruk at IKT. Smarte vannmålere tilsvarende AMS, som innføres i strømsektoren, prøves nå ut i en del norske vannverk. I Oslo skal det for eksempel installeres om lag 2 500 smarte vannmålere i løpet av 2015 som et prøveprosjekt for at man skal skaffe seg erfaring med bruken. Innføring av smarte vannmålere og mer aktiv styring av driftsforholdene på ledningsnettet vil kreve økt oppmerksomhet rundt IKT-sikkerhet.

IKT-sikkerhet knyttet til ledningsdata

Når det gjelder sikring av IKT-systemer og den informasjonen som ligger i disse systemene, snakker man gjerne om sikring av konfidensialitet, integritet og tilgjengelighet (se forøvrig punkt 5.1 «Hva er IKT-sikkerhet?»):

- *Konfidensialitet* innebærer å sikre at informasjonen er tilgjengelig bare for dem som har autorisert tilgang. Eksempler på tap av konfidensialitet er at hackere får tilgang til hemmelig informasjon som ligger lagret i driftskontrollsystemet (DKS), eller at ledningsdata (GIS) kommer på avveier.
- *Integritet* innebærer å sikre at informasjonen og metodene/beregningene er nøyaktige og fullstendige. Uvedkommende kan da ikke endre informasjonen eller systemet som behandler informasjonen.
- *Tilgjengelighet* innebærer å sikre autoriserte brukeres tilgang til informasjon og tilhørende ressurser ved behov. Eksempel på tap av tilgjengelighet er at driftsoperatørene ikke klarer å logge seg på systemet og endre verdier ved behov. Tilgjengelighet kan også henspille på evnen et vannbehandlingsanlegg har til å levere rent vann.

Når det gjelder drifts- og styringssystemer, vil integritet og tilgjengelighet ofte være vel så viktig som konfidensialitet. Man er avhengig av at systemet er tilgjengelig og gjør de oppgavene det er satt til. Dette forutsetter også at systemet har tilgang til riktig informasjon til enhver tid. Samtidig vil tap av konfidensialitet gjøre det lettere å tappe integriteten og tilgjengeligheten ved en senere anledning.

Ledningskartverk tilgjengelig på Internett

Det har de senere årene pågått en diskusjon i vannbransjen om ledningsdata skal ligge offentlig på Internett. Ut fra praktiske hensyn bør ledningskartverk være åpent tilgjengelige for alle, men mye tyder på at det ut fra sikkerhetshensyn bør være restriksjoner med hensyn til hvem som får tilgang. I mangel av myndighetssignaler om informasjonssikkerhet har vannbransjen selv anbefalt at ledningskartverk ikke bør gjøres fritt tilgjengelige på Internett.[9] En må videre være klar over at mange vannverk har lagt mye informasjon om sine DKS-er ut på Doffin i forbindelse med anbud. Innsynssystemene for kart legges stadig oftere over på ulike portalløsninger der data ligger lagret i skybaserte tjenester.

I en krisesituasjon uten strøm og ekom vil det fortsatt være viktig å lokalisere ledninger, kummer og så videre. Her pågår det et tverrsektorielt arbeid i regi av Kommunal- og moderniseringsdepartementet som blant annet skal se på regel-

[9] http://norskvann.no/images/pdf/ledningskartverk.pdf.

verksløsninger knyttet til ledninger i grunnen og informasjonssikkerhet.[10]

Driftskontrollsystemer og risiko

Det er en tendens til at driftskontrollsystemer i økende grad blir integrert med tradisjonelle kontorstøttesystemer og tilkoblet Internett. Driftskontrollsystemene er dermed ikke lenger selvstendige systemer, men integrerte løsninger, noe som gjør at driftskontrollsystemene er utsatt for de samme sårbarhetene som vanlige IKT-systemer, blant annet med hensyn til virus og hacking. Den økende bruken av IKT, sammen med økt bruk av hyllevare og sammenkobling mot andre nett i større grad, gjør at sårbarheten for IKT-trusler er større enn før.

SINTEF har i flere publikasjoner belyst sikkerheten i norske vannverk. I arbeidet sitt har de fått tilbakemeldinger fra en del vannverk om at ulike nasjonale sikkerhetsaktører og -rådgivere – som NSM og Forsvarets forskningsinstitutt – tilsynelatende vurderer det samme trusselbildet forskjellig. Dette kom godt frem på TEKNAs konferanse om samfunnssikkerhet i vannbransjen i april 2015, der begge aktørene holdt innlegg. Der NSM basert på sine data peker på viktigheten av å fokusere mer på IKT-sikkerhet, har FFI i sine analyser for utvalgte vannverk nedtonet den digitale sårbarheten. For vannbransjen fremstår en slik dobbeltkommunikasjon som forvirrende, og det kan for mange være uklart om den digitale sårbarheten utgjør en stor trussel eller om den er økende.

NSM skriver i årets statusrapport, *Risiko 2015*,[11] at de har avdekket alvorlige sårbarheter innen norsk vannforsyning i løpet av 2014. Sårbarhetene kunne i verste fall gitt uvedkommende mulighet til å lamme vannforsyningen. NSMs vurdering er at risikoen ved bruk av DKS ikke er blitt mindre i 2015. De peker i sin trusselvurdering for 2015 på sårbarheten i norske vannverk, men det er usikkert hvor bredt datagrunnlag denne vurderingen bygger på.

Tradisjonelt har ikke IKT-sikkerhet i driftskontrollsystemer vært viet stor oppmerksomhet, verken i vannbransjen eller i industrien for øvrig. Det er imidlertid eksempler på hacking av vannverk i USA via driftskontrollsystemet (DKS), og automatiserte verktøy gjør det nå enkelt for hackere å lete opp kontrollenheter som er koblet til Internett. Det er også enkelt for uvedkommende å skaffe seg informasjon om kritiske deler av et DKS via Internett. Standard passord for enkelte systemer kan finnes via Internett, og manualer og videoer for hvordan de ulike DKS-ene virker, kan også lastes ned. Dette gjør det mulig for ikke-eksperter å tilegne seg kunnskap om eventuelle sårbarheter ved de enkelte DKS-ene.

Innføring av systemer som gjør fjernaksess innen drift av vannforsyningen mulig, har gjort det enkelt og effektivt å få tilgang til status for vannforsyningssystemene utenom kontortid. Med en hjemmevaktordning kan en operatør logge seg på systemene og se på status på driften av anleggene og også endre driftsbetingelse (slå av og på, lukke/åpne ventiler). Dette er en fordel med tanke på tilgjengelighet og effektivitet for brukerne, men på den andre siden innebærer muligheten for en slik ekstern pålogging til systemene en fare for at uvedkommende får tilgang til VA-systemene dersom sikkerhetsmekanismene ikke er gode nok. Dette kan dermed påvirke integriteten og til og med konfidensialiteten til systemet.

Tradisjonelle risiko- og sårbarhetsanalyser i vannbransjen fokuserer oftest på prosesstekniske problemstillinger, siden kunnskap om IKT-systemer som regel representerer et ukjent fagområde for vanningeniører. Mattilsynet har tradisjonelt også hatt lite oppmerksomhet rettet mot sårbarheten knyttet til IKT og driftskontrollsystemer, og synes å ha liten faglig kompetanse når det gjelder IKT-sikkerhet. Dette gjenspeiles også i de veiledningene og forskriftene som er tilgjengelige.

I en undersøkelse utført av Mattilsynet i 2015[12] ble det sendt ut et spørreskjema til om lag 500 vannverk.[13] Figur 15.2 viser to resultater fra undersøkelsen. På spørsmålet «Er det tilstrekkelig bevissthet rundt IKT-sikkerhet i hele organisasjonen?» svarer 67 prosent «Ja» og 30 prosent «I noen grad». Vannbransjen i Norge ser altså ut til å være rimelig fornøyd med eget ambisjonsnivå og egen bevissthet vedrørende IKT-sikkerhet. Når det derimot kommer til mer konkrete spørsmål som: «Er det krav til regelmessig bytte av alle passord?» svarer 61 prosent «Nei». Dette viser at det er lite sammenfall mellom svarene på de ulike spørsmålene, og det er grunn til å tro at mange vannverk ikke har full forståelse av de spørsmålene som stilles.

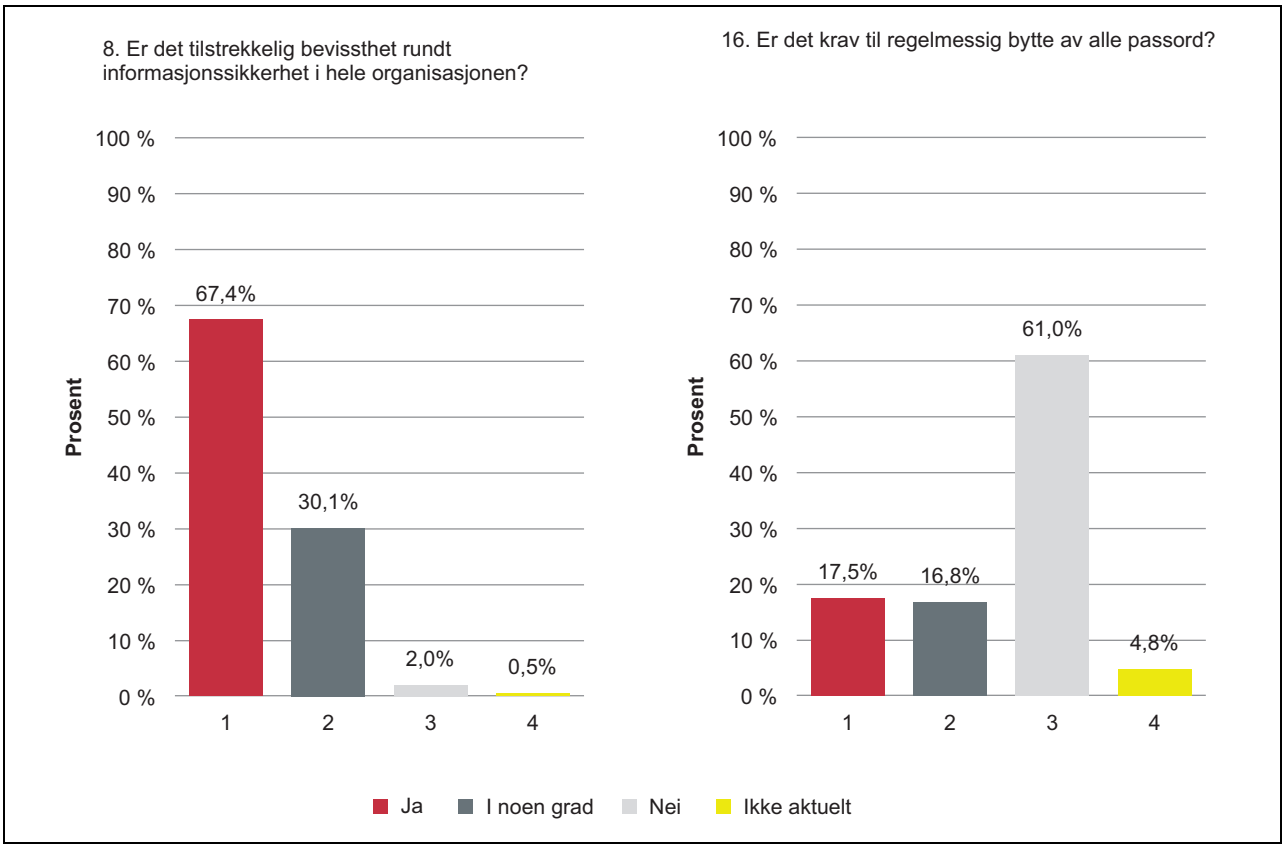
---

[10] Samarbeidsforum for ledninger i grunnen, Kommunal- og moderniseringsdepartementet.

[11] Nasjonal sikkerhetsmyndighet (2015): *Risiko 2015*.

[12] Presentasjon av Mattilsynet på TEKNAs konferanse «Samfunnssikkerhet og vannbransjen», 21.–22. april 2015.

[13] Basert på sjekklisten utarbeidet i Norsk Vann. Rapport 195/2013.



Figur 15.2 Eksempler på svar fra Mattilsynets spørreundersøkelse i 2015 til norske vannverk knyttet til informasjonssikkerhet.

Kilde: Mattilsynet.

SINTEF er i samtaler med leverandører av driftskontrollsystemer blitt kjent med at flere av vannverkene fikk sine leverandører av DKS til å fylle ut spørreundersøkelsen på vegne av vannverket. Dette illustrerer at IKT-sikkerhet ikke er grundig forankret hos ledelsen i alle vannverk. Resultatene viser at det er stort behov for kompetanseheving og økt oppmerksomhet rundt IKT-sikkerhet hos vannverkene.

15.5.2 Vannforsyningens avhengighet av kraft og ekom

Vannforsyningen er sårbar overfor svikt i de kritiske infrastrukturene kraft og ekom. En del elementer i vannforsyningssystemet vil ha en viktigere funksjon enn andre, og dette må gjenspeiles i innebygd sikkerhet ved hvert enkelt anlegg. Viktige utestasjoner kan for eksempel være vannbehandlingsanlegg, enkelte vannpumpestasjoner og høydebasseng. Dersom vannverket for eksempel er avhengig av kommunikasjon via en mobiltelefonsentral (basestasjon), er det viktig å være klar over at basestasjonene normalt bare har begrenset nødstrømskapasitet. Hvert enkelt vannverk må foreta en gjennomgang av hvilke komponenter og stasjoner som er mest kritiske med tanke på kraftforsyning og kommunikasjon, og sørge for at systemene knyttet opp mot disse er sikret i henhold til ønsket akseptnivå.

15.5.3 Organisatoriske forhold og kompetanse

Det er behov for økt IKT-sikkerhetskompetanse innen vann og avløp i kommunal teknisk sektor.[14] Dette er knyttet til blant annet teknisk kompetanse, bestillerkompetanse og gjennomføringskapasitet. Dersom en ser mangelen på kompetanse i lys av de andre utfordringene bransjen står overfor, som klimaendringer, forfall av infrastruktur, økte krav til sikkerhet, med mer, kan konsekvensen være at mange vannverk ikke har kapasitet til å prioritere de digitale sårbarhetene.

Mattilsynets gjennomgang av IKT-sikkerhet knyttet til driftskontrollsystemer i vannbransjen[15] viser at det er behov for ytterligere økt oppmerk-

[14] Rambøll (2013): *Utfordringer og muligheter i kommunalteknisk sektor.* FOU-prosjekt nr. 134038.

somhet og kunnskapsheving knyttet til IKT-sikkerhet. Dette gjelder både ledelsen i vannverkene og resten av de ansatte. Et godt sikkerhetsarbeid er i utgangspunktet et ledelsesansvar, men ledelsen må ha faglig støtte når det gjelder IKT-sikkerhet, og hver enkelt ansatt må få økt bevissthet rundt IKT-sikkerhet. For å øke bevisstheten om IKT-sikkerhet har Norsk Vann blant annet gitt ut en veiledning om sikkerhet i driftskontrollsystemer for vann- og avløpssystemer. Denne veiledningen gir en god innføring i sikring av DKS.

Bruk av midlertidig innleide konsulenter, bruk av leverandørens personell og drift utsatt til tredjepart medfører at det enkelte vannverk ytterligere tømmes for kompetanse. I tillegg blir kompetanseheving vanskelig, da fagmiljøene normalt er små, jf. det store antallet vannverk som finnes i Norge.

Organisasjonen må ha evne til læring. Det vil si at den må være i stand til å registrere og analysere ulykker og hendelser og bruke dette som grunnlag for både formell og uformell erfaringsoverføring og læring. Det er også viktig å trekke lærdom ut av det som fungerer, og å lære fra egne og andres erfaringer knyttet til svikt i IKT-systemer via egne systemer for hendelseshåndtering.

Organisasjonen må også ha reaktiv handlingsdyktighet og beredskapsevne. Det vil si at den må være i stand til å håndtere de uønskede hendelsene og ulykkene som måtte inntreffe, som tekniske sammenbrudd, brann eller terrorhandlinger. Dette inkluderer også evne til å gjenopprette funksjoner, slik at DKS raskt kommer opp å gå igjen etter en hendelse. For å få god beredskapsevne mot IKT-sikkerhetshendelser må det trenes. I forhold til vanlige øvelser i vannverkene kjennetegnes IKT-sikkerhetsøvelser av at en må knytte hendelser som inntreffer med lengre tids mellomrom til hverandre. For eksempel kan en forstyrrelse som oppstår én dag, ha sammenheng med tapet av en bærbar PC som inneholdt ledningskartverket, tre måneder tidligere.

Potensielle årsakskjeder går på tvers av organisasjoner, institusjoner og teknologiske systemer, og kartlegging av risiko og sårbarhet og ikke minst beredskap krever samhandling og koordinering. Ofte kan koordineringsutfordringer se enkle ut på papiret, der aktører kan gis ansvar for å tenke helhetlig. Mange kommuner opplever det imidlertid som utfordrende for eksempel å inkludere ulike ekomleverandører i sitt ansvar for helhetlige risiko- og sårbarhetsanalyser (ROS-analyser) og beredskap.

En utfordring for mange vannverk er også forholdet til kommunens egen IKT-avdeling. I mange kommuner er det en egen IKT-avdeling eller et eget interkommunalt IKT-selskap som beslutter hvilke systemer som skal anskaffes, vedtar sikkerhetsnivåer og til dels har ansvar for drift av systemene. IKT-avdelingen i en kommune betjener mange ulike kommunale etater og har ikke nødvendigvis god vannfaglig forståelse.

Tilsvarende har gjerne vannverkets ansatte god vannfaglig kompetanse, men mindre kompetanse knyttet til IKT og IKT-sikkerhet. Vannverksorganisasjonen vil uansett ha et overordnet sikkerhets- og beredskapsansvar i henhold til drikkevannsforskriften, og det må avklares hvordan grensesnittet bør være opp mot IKT-avdelingen og IKT-leverandørene, både for anskaffelser og for drift.

Et felles responsmiljø for vannbransjen ville kunne bidra til bedre planlegging av hendelseshåndtering og sørge for informasjonsdeling av hendelser knyttet til svikt i IKT i norske vannverk. Imidlertid synes en egen CERT-funksjon for alle landets vannverk som en krevende modell.

Større avhengigheter mellom kritiske infrastrukturer endrer også tilsynsrollen og krever økt tverrfaglig kompetanse i de ulike tilsynene. Hvis Mattilsynet skal kunne vurdere robustheten til vannverkene, må de også se etter svakheter i sektorer som leverer tjenester til vannsektoren (strøm, ekom). Sikkerhet innen vannforsyning er i utgangspunktet vannverkseierens ansvar, men er også noe man oppnår på tvers av andre involverte organisasjoner. Dette innebærer store koordineringsutfordringer på tvers av sektorer/infrastrukturer.

Mattilsynet som tilsynsmyndighet har ansvar for å ivareta funksjoner med betydning for vannsikkerheten. For tilsynet medfører dette nye utfordringer og spørsmål om hvor langt inn i leverandørkjedene de skal føre tilsyn. Skal de nøye seg med å inspisere kontraktene vannverkene har med sine leverandører, eller skal de også gå i detalj hos leverandørene?[16] Et viktig spørsmål er om Mattilsynet i tilstrekkelig grad er i stand til å gjennomføre tilsyn av vannverkene, tatt i betraktning den nye utviklingen.

---

[15] Presentasjon av Mattilsynet på TEKNAs konferanse «Samfunnssikkerhet og vannbransjen», 21.–22. april 2015.

[16] Almklov (2011): *Offentlige etaters rolle i å sikre robusthet i komplekst organiserte og tett koblede infrastruktursektorer.*

15.6 Vurderinger og tiltak

15.6.1 Øke IKT-sikkerhetskompetansen i norske vannverk

Som nevnt over er det i dag svært mange små vannverk i Norge, og modenheten når det gjelder IKT-sikkerhetsarbeid, synes å være på et tidlig stadium. Det store antallet vannverk gjør en god fremdrift på dette området vanskelig, siden det kreves spisskompetanse for å kunne ivareta IKT-sikkerhetsansvaret på en god måte. Se punkt 19.3 «Kompetansesituasjonen i samfunnet».

Vannverkenes ROS-analyser må inkludere sikkerhetsvurderinger knyttet til IKT og IKT-sikkerhet. IKT-sikkerhet må inkluderes i det generelle beredskapsarbeidet, og det må gjennomføres øvelser som inkluderer IKT-hendelser. Vannverkenes avhengighet av kraft og ekom må inngå i ROS-analysene, og tiltak for å håndtere bortfall må inngå i beredskapsplanene. Vannverkene må ha oversikt over hvilke elementer av vannforsyningssystemet som er mest kritiske ved utfall, og sette i verk nødvendige tiltak for å hindre dette.

Kommunerevisjonen i de enkelte kommunene må vurdere om de skal foreta revisjon av IKT-sikkerheten til det kommunale vannverket. Kommunerevisjonen har i enkelte vannverk prioritert IKT-sikkerhet. Selv om en revisjon medfører mye arbeid for de ansatte i vannverket, er erfaringene at revisjonene gir IKT-sikkerheten et løft. I tillegg vil en kommunerevisjon føre til at den politiske ledelsen blir bevisst på problemstillingen.

Siden bare et fåtall av norske kommuner og vannverk har anledning til å delta på nasjonale konferanser, er regionalt samarbeid svært relevant. Regionalt samarbeid kan også utvides til å utgjøre et praksisfellesskap, der ansatte med ansvar for problemstillinger relatert til IKT-sikkerhet både kan få faglig påfyll, utveksle erfaringer og få praktisk støtte i enkeltsaker.

Med så mange små enheter er det en kompetanseutfordring å etablere og opprettholde nødvendige fagmiljøer innen IKT-sikkerhet. *Utvalget mener at Mattilsynet i samarbeid med Norsk Vann bør stimulere til større og mer ressurssterke fagmiljøer i kommunene. Dette kan gjøres på flere måter, eksempelvis ved økt interkommunalt samarbeid eller ved strukturendring.*

Utvalget foreslår videre at det tas initiativ til å dekke de nye utfordringene vi står overfor innenfor IKT-sikkerhet. Både myndighetssiden og Norsk Vann bør kunne bidra med å organisere kurs, gjerne i samarbeid med andre organisasjoner, som for eksempel NSM eller undervisningsinstitusjoner, der det er hensiktsmessig. *Det bør også utvikles kurs og studieretninger innenfor prosesstyring, systemintegrasjon og IKT, noe som kan bidra til at bransjen får den kompetansen som trengs for å drifte systemene i fremtiden.*

Bedre organisering av driftsassistanser vil også være et mulig tiltak. Det vises i den sammenheng til Norsk Vanns rapport *Fra driftsassistanser til regionale vannassistanser*[17] med anbefalinger om hvordan dagens fylkesvise driftsassistanser på vannområdet kan videreutvikles til mer helhetlige vannassistanser som gir et styrket og effektiviserende tilbud til deltagerkommuner og vannverk, blant annet på sikkerhets- og beredskapsområdet.

15.6.2 Styrke tilsyn og veiledning i IKT-sikkerhet

Det er behov for økt oppmerksomhet hos Mattilsynet når det gjelder IKT-sikkerhet. Dette inkluderer utarbeidelse av forskrifter som definerer krav til IKT-sikkerhet, og tilhørende veiledningsmateriell for vannverk. Vannverkene synes å ha behov for utfyllende informasjon utover de generelle kravene som er tillagt vannverkseieren i drikkevannsforskriften[18]. *Det bør vurderes et tettere samarbeid mellom de ulike tilsynsmyndighetene for at hvert enkelt tilsyn skal bli bedre i stand til å føre tilsyn med sin sektor knyttet til hendelser som går på tvers av sektorene (vann, strøm, ekom).* Mattilsynet har i etterkant av den tidligere omtalte spørreundersøkelsen om IKT-sikkerhet inngått avtale med NSM om kursing av egne ansatte i IKT-sikkerhet. Mattilsynet har i dag ikke kapasitet eller mandat til å drive kursing av hvert enkelt vannverk. En veiledningsrolle på området må også ses i forhold til tilsynsrollen deres.

Relevante myndigheter bør avklare og vedta et nødvendig ambisjonsnivå for IKT-sikkerhet for vannverkene. Dette har lenge vært etterlyst av vannverkene og av Norsk Vann. Utarbeidelse av et kompetansehevende kurs for vannverkene som kan bidra til å styrke sikkerhetsarbeidet, vil være avhengig av det vedtatte ambisjonsnivået.

Helse- og omsorgsdepartementet har startet et arbeid med å revidere drikkevannsforskriften med tilhørende veileder. *Revisjonen må også inkludere IKT-sikkerhet og IKT utover det generelle kravet om at vannverkseieren er ansvarlig for å levere sikkert drikkevann.*

---

[17] Norsk Vann (2014): *Fra driftsassistanser til regionale vannassistanser.* Rapport 203/2014.

[18] Helse- og omsorgsdepartementet (2002): *Forskrift om vannforsyning og drikkevann (Drikkevannsforskriften).*

15.6.3 Bedre systemer for hendelseshåndtering

Den enkelte virksomhet er ansvarlig for IKT-sikkerheten. Det synes imidlertid å være et behov for å etablere et felles responsmiljø for hendelseshåndtering. Et eget responsmiljø for vann er kanskje ikke realistisk, tatt i betraktning det store antallet små enheter i vannsektoren. Tre alternativer kan være:

Alternativ 1: Kommunene oppretter en egen kommune-CERT, som ikke bare omfatter vannforsyning, men også andre deler av kommunenes ansvar for kritiske samfunnsfunksjoner, som primærhelsetjeneste, kriseledelse og brann og redning. Utvalget er kjent med at det er tatt et initiativ til å etablere en kommune-CERT.

Alternativ 2: Fylkesmannen tar initiativ til en regional plan for hendelseshåndtering for kommunale vannverk. Et slikt initiativ bør inneholde et forpliktende samarbeid på tvers av vannbransjen, også for å støtte opp under et praksisfellesskap på regionalt og nasjonalt plan. Dette bør også ses i sammenheng med diskusjonen om å etablere en fremtidig krisestøtteenhet for vannverkene i Norge, tilsvarende det Sverige har. En norsk krisestøtteenhet bør ha kunnskap også om IKT-sikkerhet.

Alternativ 3: At vannverkene knytter seg opp mot allerede eksisterende hendelseshåndteringsmiljø.[19]

Utvalget anbefaler at Helse- og omsorgsdepartementet, i samråd med Justis- og beredskapsdepartementet og Kommunal- og moderniseringsdepartementet, utreder muligheten for et responsmiljø for hendelseshåndtering som ivaretar vann og avløp.

15.6.4 Gjennomføre risiko- og sårbarhetsanalyser før en eventuell innføring av smarte vannmålere

Ved en eventuell større innføring av smarte vannmålere, tilsvarende AMS som innføres i strømsektoren, bør det foretas en omfattende risiko- og sårbarhetsanalyse. Ukritisk implementering av funksjonalitet som knytter smarte vannmålere tettere sammen med driftskontrollsystemer, vil føre med seg en oppbygging av sårbarhet med betydelig skadepotensial. Innføring av smarte vannmålere og mer aktiv styring av driftsforholdene på ledningsnettet vil kreve økt oppmerksomhet rundt IKT-sikkerhet. Utvalget mener det er viktig med en god og bredt dekkende risiko- og sårbarhetsanalyse i forkant av teknologiskifter, ved bruksendringer og ved system- og organisasjonsendringer. *Utvalget anbefaler derfor at det gjennomføres nødvendige risiko- og sårbarhetsanalyser før innføring av smarte vannmålere inn mot driftskontrollsystemene.*

---

[19] Se kapittel 14 «Olje og gass» hvor det vurderes tilknytning til responsmiljø for IKT-hendelser.

Kapittel 16
Finansielle tjenester

Finansnæringen er en IKT-intensiv næring og leverer i stor grad sine tjenester på digitale plattformer. Norsk finansnæring var tidlig ute med å ta i bruk IKT i sine produksjonsprosesser. Særlig samarbeidet grupper av banker om standardisering og felles IKT-løsninger – i første omgang om IKT-systemer for kontoføring, deretter om IKT-systemer for registrering av transaksjoner mellom konti. Finansforetakene har benyttet IKT til å effektivisere interne prosesser, og ligger i forkant i bruk av IKT for håndtering av kundedimensjonen. Dette har medført en kompleksitet i IKT-systemer og verdikjeder som gjør næringen sårbar for både tilsiktede og utilsiktede hendelser. Den internasjonale, organiserte kriminaliteten øker. Kriminaliteten har så langt vært rettet mot distribusjonskanalene som benytter Internett. Den rammer også mobile løsninger og løsninger knyttet til brukersteder.

Finansiell stabilitet innebærer at det finansielle systemet er solid nok til å formidle finansiering, utføre betalinger og fordele risiko på en tilfredsstillende måte. De basiskapasitetene og basisleveransene som er nødvendige for å opprettholde finansiell stabilitet, kan ikke leveres uten velfungerende IKT-systemer. Det norske systemet er i likhet med systemene i de andre nordiske landene kjennetegnet av at forbindelsene mellom bankene er samordnet og elektronisk basert i større grad enn i mange andre land. Dette gjør det norske banksystemet utsatt dersom noen skulle lykkes i å ta kontroll over eller ødelegge sentrale felles funksjoner. I tillegg til finansielle og materielle tap kan de samfunnsmessige konsekvensene bli store, og befolkningen vil kunne oppleve betydelige belastninger i dagliglivet.

Finansnæringen må ta høyde for at det kan komme omfattende, organiserte angrep som vil kunne føre til store økonomiske tap. Dette skyldes at flere pengetransaksjoner fra næringslivet digitaliseres, samtidig som kriminelle, med metoder som blir stadig mer avanserte, følger pengestrømmen på nettet.[1]

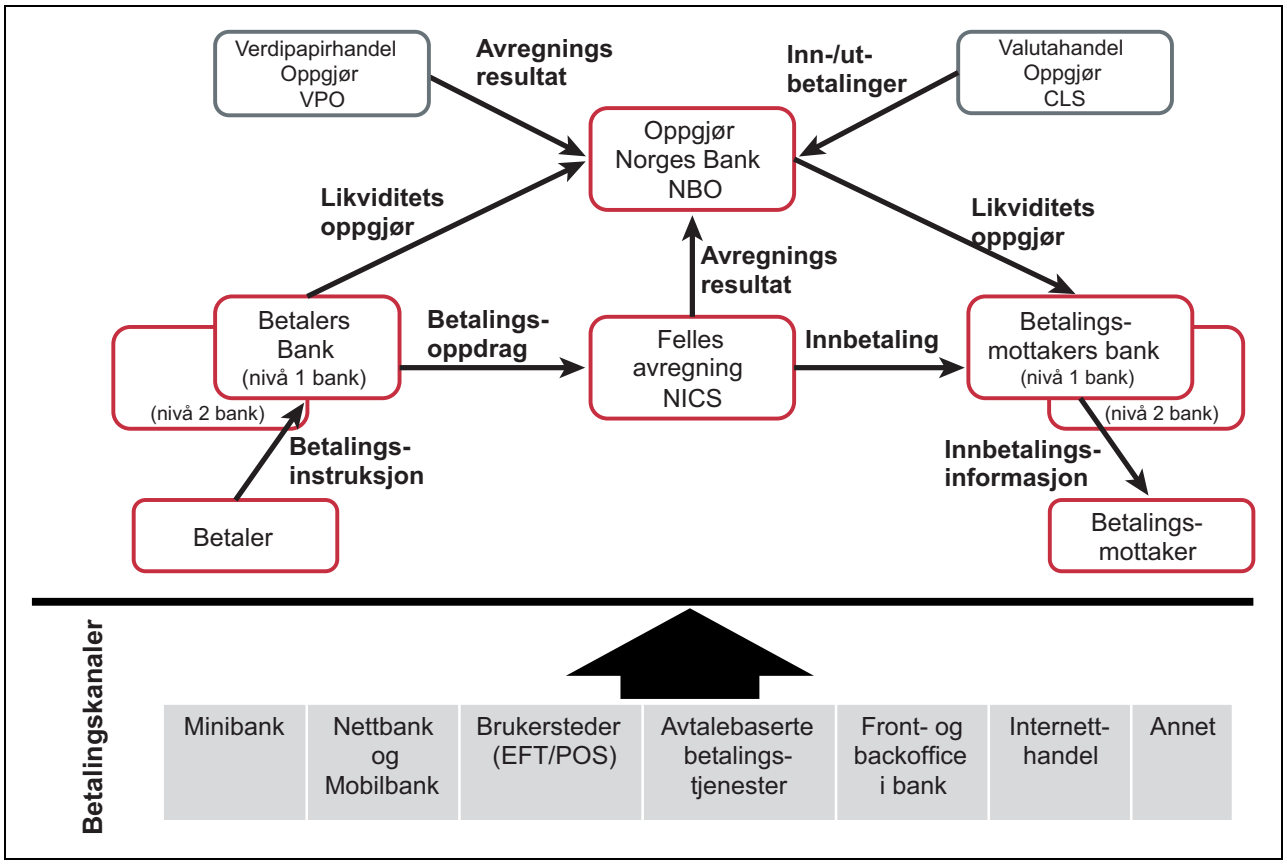
For enkeltpersoner er en av de største endringene nye former for elektroniske betalingstjenester, samt overgangen til et stadig mer kontantløst samfunn. I 2012 ble det gjennomført 1,63 milliarder korttransaksjoner her i landet. Her ligger Norge høyt sammenlignet med andre land. Samtidig går bruken av kontanter som betalingsmiddel ned, og her ligger Norge svært lavt sammenlignet med andre land.

16.1 Finansiell infrastruktur

Betalingssystemet består av interbanksystemer og systemer for betalingstjenester. *Interbanksystemer* er systemer for overføring av penger mellom banker, med felles regler for avregning og oppgjør. *Systemer for betalingstjenester* er systemer som er basert på standardvilkår for overføring av penger fra eller mellom kundekonti i banker eller andre som kan yte betalingstjenester.

Betalingssystemene er en helt sentral forutsetning for at kapital skal kunne formidles på en sikker måte mellom aktører nasjonalt og internasjonalt, for eksport og import av varer og tjenester, i grossistleddet, i varehandelen (detaljistleddet), for verdipapirhandel og for handel med finansielle tjenester. Betalingssystemene kan deles inn i ulike lag – fra der transaksjoner oppstår, til transaksjonene er avsluttet. En nærmere beskrivelse av betalingssystemene er gitt i punkt 16.5.1, der også sårbarhetene er beskrevet. En forenklet fremstilling av transaksjonsflyten fra der betalingen oppstår, samt innsamling, avregning og oppgjør, er gitt i figuren under.

[1] Næringslivets sikkerhetsråd (2014): *Mørketallsundersøkelsen 2014 – Informasjonssikkerhet, personvern og datakriminalitet.*



Figur 16.1 Transaksjonsflyten i det norske betalingssystemet.

Kilde: Finanstilsynet.

16.2 Roller og ansvar

Finansdepartementet har ansvar for en rekke underliggende etater og statlige foretak, blant annet Finanstilsynet og Norges Bank. Finansdepartementets rolle overfor de tilknyttede virksomhetene varierer, men felles for alle er at Finansdepartementet gir retningslinjer for virksomhetene basert på det lovverket Stortinget har vedtatt. Finansdepartementet har på lik linje med de andre fagdepartementene et overordnet ansvar for å ivareta sikkerheten i sektorens IKT-infrastruktur og for at det forebyggende informasjonssikkerhetsarbeidet i sektoren er tilfredsstillende.

Finanstilsynet er det sentrale offentlige organet som kontrollerer og vurderer om banker, forsikringsselskaper, finansieringsforetak, verdipapirforetak, børs og autoriserte markedsplasser, verdipapirregistre, eiendomsmeglere, e-pengeforetak, revisorer og autoriserte regnskapsførere følger de lover og regler som er vedtatt for finansmarkedet, og driver virksomheten med akseptabel risiko. Tilsynet skal også se til at institusjonene tar hånd om forbrukernes interesser og rettigheter. Finanstilsynets hovedmål er finansiell stabilitet, velfungerende markeder og forbrukervern. Finanstilsynet leder og er sekretariat for Beredskapsutvalget for finansiell infrastruktur (BFI). Se punkt 16.4 for en nærmere beskrivelse av BFI.

Norges Bank er sentralbanken i Norge, og har som mål å fremme den økonomiske stabiliteten i landet. Banken har utøvende og rådgivende oppgaver i pengepolitikken og skal medvirke til robuste og effektive betalingssystemer og finansmarkeder. Norges Bank forvalter valutareservene i landet. Statens pensjonsfond utland skal støtte statlig sparing for finansiering av fremtidige utgifter og underbygge langsiktige hensyn ved bruk av Norges petroleumsinntekter. Norges Bank forvalter Statens pensjonsfond utland, og har delegert gjennomføringen av forvaltningsoppdraget til Norges Bank Investment Management (NBIM).

Finans Norge er hovedorganisasjon for finansnæringen i Norge, og representerer mer enn 200 medlemsbedrifter fra bank og forsikring, med rundt 50 000 ansatte. Finans Norge har ulike oppgaver på IKT-sikkerhetsområdet, både som premisslegger for et omforent sikkerhetsnivå på betalingsområdet og som representant for medlemmene i ulike fora der IKT-sikkerhet diskuteres, herunder Næringslivets Sikkerhetsråd. Som

næringsorganisasjon arbeider Finans Norge med selvregulering og standardisering innen IKT-sikkerhet nasjonalt og i EU, og fungerer som høringsinstans på vegne av norsk finansnæring i forbindelse med lov- og forskriftsendringer.

Norwegian Interbank Clearing System (NICS) er sentralt for gjennomføring av betalinger i Norge. Finans Norge forvalter, på vegne av finansforetakene, flere felles operasjonelle infrastrukturer (FOI) innen betalingsinfrastrukturen – både direkte og gjennom *NICS Operatørkontor*, som driftes av Finans Norge. NICS Operatørkontor er konsesjonshaver for banknæringens hovedavregning.

BankID ble initiert av Finans Norge i 2000, og eies av bankene. Over tre millioner nordmenn har nå BankID, som er den mest utbredte og brukte elektroniske ID-en i Norge. Ingen andre europeiske land er på et tilsvarende nivå. BankID-sertifikatene utstedes av bankene. Bakgrunnen for etableringen av BankID var at banknæringen skulle kunne spille samme rolle i kundebetjening og tjenestetilbud over åpne nett som i den fysiske verden. Dette krevde en samordnet struktur for sikker autentisering og signering i åpne nett. Videre mente man at utbredelsen av sikker digital kommunikasjon i befolkningen krevde at brukerne kunne benytte samme sikkerhetsordning ofte og i flere sammenhenger.

BankAxept ble tidligere administrert av Finans Norge, men er nå etablert som et eget AS, eid direkte av bankene. BankAxept er det dominerende kortsystemet i Norge. Ni av ti kortbetalinger med norske kort skjer via BankAxept.

FinansCERT ble etablert av finansnæringen i 2013, og er et heleid datterselskap av Finans Norge. Målsettingen til FinansCERT er at finansnæringen skal være godt rustet til å møte trusler utenfra rettet mot finansinstitusjonenes IKT-virksomhet og mot digitale tjenestekanaler til kundene. FinansCERTs formål er å koordinere og støtte finansnæringen i håndteringen av IKT-sikkerhetshendelser, samt forebyggende arbeid.[2] En nærmere beskrivelse av FinansCERT følger i punkt 16.4 «Beredskap og hendelseshåndtering».

Sentrale leverandører innenfor sektoren er Nets, Evry og SDC. Nets tilbyr betalings-, kort- og identitetsløsninger i de nordiske landene og leverer de tekniske betalingsløsningene mellom norske banker og for dagsoppgjøret i Norges Bank. Evry er en stor tjenesteleverandør i det norske finansmarkedet, og håndterer i løpet av et år i overkant av 300 millioner betalingstransaksjoner. SDC er en annen IKT-leverandør i det nordiske finansmarkedet, og hadde i 2014 82 norske banker på kundelisten.

Forskning og utvikling

Nasjonalt har Finanstilsynet tidligere hatt bistand fra Selmersenteret i Bergen og Norsk Regnesentral til analyser av henholdsvis sikkerhet i nettbank og sikkerhet i betalingskort. I tillegg har de vært involvert i prosjekter om operasjonell risiko ved Universitetet i Stavanger. Internasjonalt har Finanstilsynet deltatt i EUs forskningsprosjekt rettet mot tiltak for å gjøre finanssektorens bruk av Internett sikrere,[3] samt arbeid med forslag til aktuelle områder det bør forskes mer på når det gjelder sikkerhet. Samtidig jobber næringen tett sammen om å se på fremtidige behov. Eksempelvis har Bankenes Standardiseringskontor tatt et initiativ overfor Standard Norge for at det skal iverksettes tiltak for å øke satsingen på internasjonal standardisering på sikkerhetsområdet.

Internasjonalt samarbeid

Norge har tett kontakt med internasjonale organisasjoner, som ISACA og FI-ISAC. *ISACA* er en internasjonal forening som fokuserer på styring av og kontroll med IKT og tilbyr globalt anerkjente sertifiseringer. *Financial Institutes – Information Sharing and Analysis Center (FI-ISAC)* er et europeisk tiltak primært med deltakere fra CERT-er, bankorganisasjoner og politimyndighet. Det er et uformelt samarbeid mellom enkeltland og definerte myndigheter, blant annet støttet av ENISA. FI-ISAC utveksler til dels konfidensiell informasjon om sårbarheter, angrep og tiltak knyttet til bruk av de elektroniske betalingsløsningene.

ITSG (International IT Supervisors Group) er en uavhengig internasjonal arbeidsgruppe som har IT-tilsyn som arbeidsområde. Formålet med samarbeidet er å utnytte kunnskap og erfaringer på tvers av landegrensene. Det gjelder for både stedlige og dokumentbaserte tilsynsmetoder. Utveksling av kunnskap når det gjelder bruk av rammeverk, standarder og beste praksis ved gjennomføring av tilsynsaktiviteter innenfor IT-områ-

[2] FinansCERT Norge opererer i dag for medlemmer i Finans Norge. Det er åpent for at også andre aktører i finansnæringen kan slutte seg til FinansCERT.

[3] Henholdsvis CoMiFin: Communication Middleware for a secure and dependable Financial Infrastructure (under EUs 7. rammeprogram) og European Security Research and Innovation Forum (ESRIF), som ett av flere underlag for EUs 8. rammeprogram.

det, er et viktig tema i de årlige møtene deres. Forumet består av cirka 20 deltagerland, og det ble startet i 2002 som en forlengelse av samarbeidet tilsynsmyndighetene hadde for overgangen til år 2000. Områder som blant annet IT-sikkerhet, cybersikkerhet, utkontraktering, skytjenester og beredskap, er områder som har fått bred dekning på de årlige møtene. I tillegg blir større hendelser gjennomgått. Gjennom kontaktlister er det stor grad av informasjonsutveksling. Dette gjelder både for hendelser og for risikoøkninger som de enkelte medlemslandenes institusjoner opplever.

European Banking Authority (EBA) satte i 2014 ned en arbeidsgruppe som skulle gjennomgå medlemslandenes tilnærming til IT-tilsyn og informasjonssikkerhet med tilhørende lovverk. Resultatet ble at det i regi av EBA ble etablert en gruppe som skal legge til rette for økt samarbeid og erfaringsutveksling på områdene som er nevnt ovenfor. Arbeidet vil pågå fra 2015 og vil bli en viktig arena for å bidra til å øke kvaliteten og kunnskapen på IT-tilsynsområdet. *De nordiske tilsynene* har løpende samarbeid og et årlig samarbeidsmøte der IT- og informasjonssikkerhet er tema. I tillegg blir det gjennomført felles tilsyn i banker med grenseoverskridende virksomhet. Dette medfører en stor grad av kunnskaps- og erfaringsutveksling.

Finanstilsynet mener selv at metodeverktøyet som benyttes i Norge, er godt og på høyde med tilsvarende i sammenlignbare land. Utvikling og tilpasning i tråd med teknisk utvikling, trusselbildet og regelverksendringer i EU er likevel nødvendig. Dette krever et tett samarbeid med aktørene som er nevnt ovenfor. DNB trekker frem finanstilsynene i USA og Singapore som særlig kompetente innenfor informasjonssikkerhet. Viktigheten av medlemskap og dialog med private/frivillige organisasjoner som bidrar med tidlig varsling og teknisk kompetanse, blir også påpekt.

16.3 Hjemmelsgrunnlag og tilsynsvirksomhet

Finanstilsynet har som en av sine oppgaver å føre tilsyn med sektorens bruk av IKT og betalingssystemer. Hjemmelsgrunnlaget for arbeidet er blant annet finanstilsynsloven og lov om betalingssystemer med tilhørende forskrifter. Også hvitvas-

Boks 16.1 Finanstilsynets verktøykasse

Finanstilsynet utarbeider hvert år en risiko- og sårbarhetsanalyse av finansforetakenes bruk av IKT. ROS-analysen er basert på funn fra tilsyn gjennom året, innrapporterte hendelser fra foretakene, meldinger i henhold til meldeplikten, spørreundersøkelser og intervjuer med foretakene og IKT-bransjen, regelverksendringer nasjonalt og fra EU, samarbeid og kontakter med andre lands tilsynsmyndigheter og annen relevant informasjon om hendelser og utviklingstrekk i bransjen.

Seksjon for tilsyn med IT- og betalingstjenester i Finanstilsynet har tilsynsansvar når det gjelder finansforetakenes bruk av IKT og finanstilsynslovens bestemmelser. Bestemmelsene er konkretisert i forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT-forskriften). For å vurdere om finansforetakene etterlever kravene i IKT-forskriften, benytter IT-tilsynet såkalt egenevaluering, med spørsmål basert på Cobit, ITIL, ISO og andre kilder, tilpasset av Finanstilsynet for det norske finansmarkedet. Rapportering av alvorlige og kritiske IKT-hendelser er fra 1. desember 2009 forskriftsregulert gjennom IKT-forskriften. Basert på rapporterte hendelser lager IT-tilsynet statistikker og analyserer årsaksforhold. I tillegg er meldeplikten for systemer for betalingstjenester et viktig virkemiddel for oppfølging av betalingssystemene. Meldeplikten er utformet som en egenevalueringsmelding med 19 kontrollspørsmål. I tillegg til disse verktøyene (som er beskrevet på Finanstilsynets nettside) har Finanstilsynet utviklet en del egne verktøy til eget, internt bruk.

Finanstilsynet samarbeider tett med Norges Bank. Finanstilsynet samhandler også regelmessig med andre tilsynsmyndigheter. I tillegg har de regelmessige møter med BankID og FinansCERT, samt møter med Finans Norge og BSK. Utover det samarbeider Finanstilsynet med IT-tilsyn i andre land, både i Norden, i EU/EØS og globalt, om utvikling av verktøykassen. En nyopprettet gruppe under EBA forventes på sikt å bli en sterk bidragsyter, og Finanstilsynet deltar direkte. I EBA pekes det på både Finanstilsynets IKT-forskrift og ROS-analyse som gode eksempler til etterfølgelse og mal for felles europeiske tiltak.

kingsloven kommer til anvendelse. For oppfølging av sektorens operasjonelle risiko, inkludert bruk av IKT, benyttes kapitalkravforskriften, IKT-forskriften og forskrift om risikostyring og internkontroll som hjemmelsgrunnlag i det praktiske tilsynsarbeidet. Nåværende IKT-forskrift er fra 2003, og tilsynsmetodene har siden blitt utviklet med beste praksis og anerkjente internasjonale rammeverk.

Virksomheten til *Norges Bank* er regulert gjennom sentralbankloven og betalingssystemloven. Her kommer det blant annet frem et ansvar for å vurdere effektiviteten til systemer for betalingstjenester og hva disse systemene betyr for effektiviteten til det norske betalingssystemet, inkludert samspillet med andre lands betalingstjenester.

Finanstilsynet samarbeider med Norges Bank der omfanget av tilsynet ligger innenfor det felles ansvarsområdet. Det gjelder spesielt betalingstjenester og avregning/oppgjør innen betalingsformidlingen, der det tidvis er gjennomført enkelte felles tilsyn. Samarbeidet er regulert gjennom betalingssystemloven.

Gjennom mandat gitt av Finans Norge fastsetter *Bankenes Standardiseringskontor (BSK)* standarder og sikkerhetskrav for transaksjons- og meldingsutvekslingen mellom bankene. BSK fastsetter også sikkerhetskrav til minibanker og kortterminaler, samt til kortutstedelse. BSK-krav omfatter også BankID, inkludert FOI (felles operativ infrastruktur). Bankene er gjennom dette forpliktet til et felles avtalt nivå for sikkerhet og risiko som er nødvendig for å kunne ha gjensidig tillit i en informasjonsutvekslingskjede.

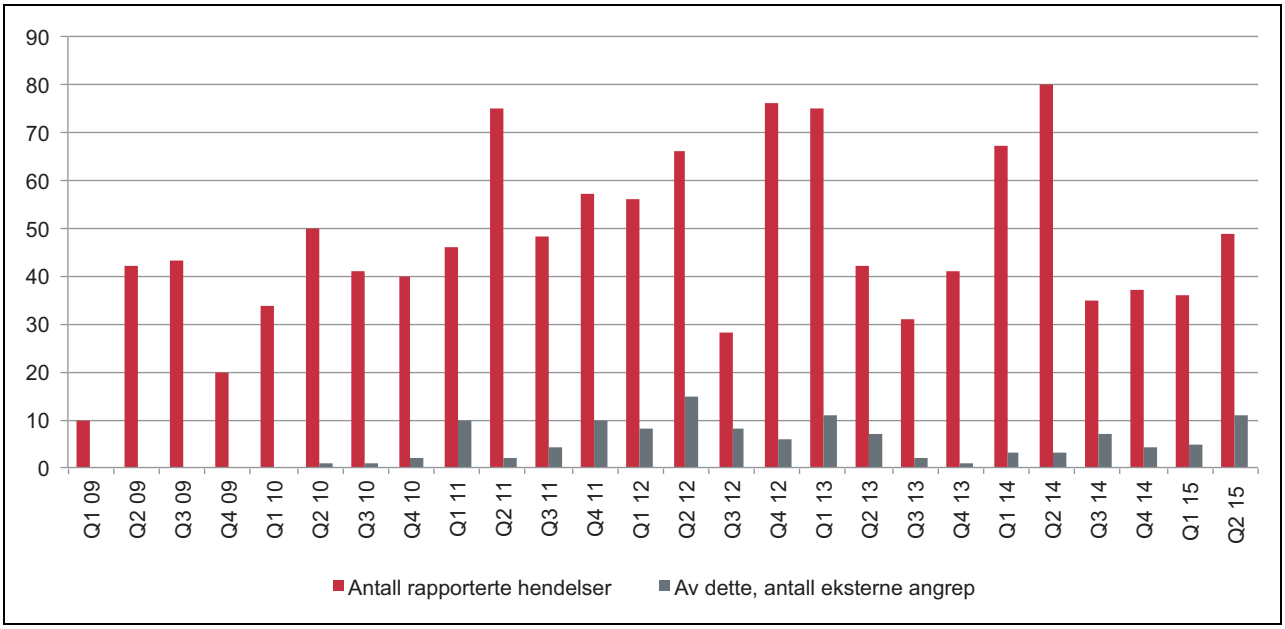
16.4 Beredskap og hendelseshåndtering

Ansvaret for håndtering av hendelser går frem av IKT-forskriften og er tillagt finansinstitusjonene og deres leverandører. Dette inkluderer krav til hendelseshåndtering for gjenoppretting, eskalering og rapportering til ledelse, samt krav om å iverksette korrektive tiltak for å unngå at samme problem oppstår på nytt. I tillegg er det krav om at alvorlige og kritiske hendelser skal rapporteres til Finanstilsynet uten unødig opphold. På denne måten får myndighetene en oversikt over hendelsesbildet, samtidig som de er sikret rask informasjon om alvorlige hendelser.

Figur 16.2 viser antall rapporterte eksterne angrep i forhold til det totale antallet rapporterte hendelser for perioden 2009 til 2015, aggregert per kvartal.

Finanstilsynet anslår at i kjernevirksomheten til tilsynsobjektene deres finner cirka 70 prosent av de alvorlige hendelsene sted på områder der institusjonene bruker underleverandører.

Finanstilsynet har etablert en rutine for å motta og behandle hendelsesrapporter og har en beredskapsplan for situasjoner der en virksomhet under tilsyn utsettes for en alvorlig IKT-krise. Beredskapsplanen viser til hendelsesrapporteringen som en aktuell kilde for å identifisere en



Figur 16.2 Antall rapporterte eksterne angrep i forhold til totalt antall rapporterte hendelser.

Kilde: Finanstilsynet.

beredskapssituasjon. Finanstilsynsdirektøren skal sammen med lederen for tilsynsansvarlig avdeling beslutte om det skal varsles til instanser utenfor Finanstilsynet, eksempelvis styret, departementer, bransjeorganisasjoner, media og så videre. Beredskapsplanen viser også til Beredskapsutvalget for finansiell infrastruktur (BFI).

Beredskapsutvalget for finansiell infrastruktur (BFI) har ansvaret for å komme frem til og koordinere tiltak for å forebygge og løse krisesituasjoner og andre situasjoner som kan resultere i store forstyrrelser i den finansielle infrastrukturen. Ifølge sitt mandat skal BFI i en krisesituasjon varsle og informere berørte aktører og myndigheter om hvilke problemer som har oppstått, hvilke konsekvenser problemene kan medføre, og hvilke tiltak som settes i verk for å løse problemene. BFI har etablert en rutine for varsling, problemhåndtering og informasjonsformidling som skal gjelde i en beredskapssituasjon. Finanstilsynet leder og er sekretariat for BFI, og vurderer når det skal kalles inn til møter. BFI representerer en viktig møteplass for sentrale finansaktører i Norge. Finanstilsynet er omfattet av myndighetenes sivile beredskapssystem (SBS), og BFI tar hånd om den nødvendige koordineringen innenfor finansiell sektor.

FinansCERT er en egen sektor-CERT (responsmiljø) for finansnæringen, og har et utstrakt samarbeid med aktører i næringen, samt et eksternt nettverk med både myndighetene/politiet og internasjonale nettverk innen IKT-sikkerhet. FinansCERT mottar informasjon fra mange kilder og videresender relevant informasjon til finansbedriftene og sentrale aktører i infrastrukturen.

FinansCERT Norge deltar aktivt i hendelseshåndtering og har en døgnkontinuerlig beredskap. Videre opererer FinansCERT et system for rask og sikker informasjonsdeling til relevante personer i aktuelle miljøer i næringen. Eksempelvis produseres det kvartalsvise rapporter om trusselbildet, der alvorlige trusler presenteres med en vurdering av trusselnivået, en vurdering av om trenden er økende eller synkende, og en aktørprofil for hver trussel. Et annet eksempel er deling av indikatorer i forbindelse med nettbanksvindel i nær sanntid.

Videre gjennomfører FinansCERT aktiviteter som forum og «community» for responsmiljøene i norske banker og forsikringsselskaper. FinansCERT har ikke en myndighetsrolle i sektoren, og omfatter per dags dato ikke alle virksomhetene i sektoren. FinansCERT har imidlertid et uttalt mål om å omfatte alle virksomheter i sektoren, men er fortsatt i en etableringsfase. FinansCERT tar sikte på å være ferdig etablert som planlagt med fem ansatte i løpet av 2015.

Boks 16.2 Fisking av nettbankpåloggingsinformasjon

I 2015 har mange nettbanker opplevd gjentatte forsøk på å fiske (lure) påloggingsinformasjon fra bankenes kunder. Med denne informasjonen vil de kunne logge seg inn i kundenes nettbank og stjele pengene på konto. For en bedrift eller offentlig virksomhet kan dette være store summer. Angrepene skjer ved at det sendes epost-spam eller SMS-spam som utgir seg for å være fra banken, der kunden bes om å klikke på en link for å låse opp en sperring eller lese en melding. Dersom kunden trykker på linken, kommer hun til en falsk nettbank. Bankene, sammen med FinansCERT og andre leverandører og samarbeidspartnere, jobber hardt for å motvirke og håndtere disse angrepene. Det har vært gjort forsøk på å stjele mange titalls millioner kroner, men disse har i stor grad blitt avverget – ofte fordi bankene har delt informasjon som gjør at de er bedre forberedt. Hendelsene viser viktigheten av god sikkerhetsbevissthet hos kundene, samt nytten av rask informasjonsdeling og aktiv hendelseshåndtering/skadebegrensning når angrep skjer.

Bankenes Standardiseringskontor (BSK) følger internasjonale trender og bevegelser for kriminelle angrep mot minibanker og terminaler, og anbefaler mottiltak til banker i Norge. BSK har også en egen nettbanksikkerhetsgruppe (med representanter fra bankene) som går igjennom hendelser og aktuelle mottiltak. NICS Operatørkontor har et eget opplegg for selvsertifisering og egenmelding for banker som deltar i NICS (i praksis alle banker). Der legges det vekt på varsling av egne hendelser til andre deltagere og rutiner for håndtering av de skjevhetene som oppstår i fordeling av likviditet når driftsavbrudd oppstår i en bank. Operatørkontoret involveres direkte i hendelser ved driftsstans hos deltagere, og det er gitt utsettelser som innebærer senere innleveringsfrister til siste daglige avregning.

I forbindelse med etableringen av objektsikkerhetsforskriften gjorde finanssektoren en vurdering av om det var objekter som skulle foreslås underlagt sikkerhetsloven. Det er kun pekt ut et mindre antall skjermingsverdige objekter i sektoren. Finanstilsynet har imidlertid i samarbeid med

BFI pekt ut objekter som skal gis prioritet fra myndighetenes side ved en alvorlig situasjon for leveranser av elektronisk kommunikasjon og kraft.

16.5 Digitale sårbarheter i finanssektoren

I Finanstilsynets ROS-analyse for 2014 vurderes det at betalingstjenestene generelt er stabile og har tilfredsstillende kvalitet. Til tross for at det i 2014 ble registrert en økning i antall alvorlige hendelser, truet ikke disse den finansielle stabiliteten. Finanstilsynet understreker imidlertid at noen av disse, dersom de hadde fått utviklet seg, kunne skapt uro for den finansielle stabiliteten.[4] Norges Bank uttrykker gjennom rapporten *Finansiell infrastruktur 2015* at det har vært få avvik i interbanksystemene og verdipapiroppgjørssystemet det siste året.

Figur 16.3 viser utviklingen av hendelser siden 2010, der disse er veiet med hvilken konsekvens de har fått for ulike typer tjenester.

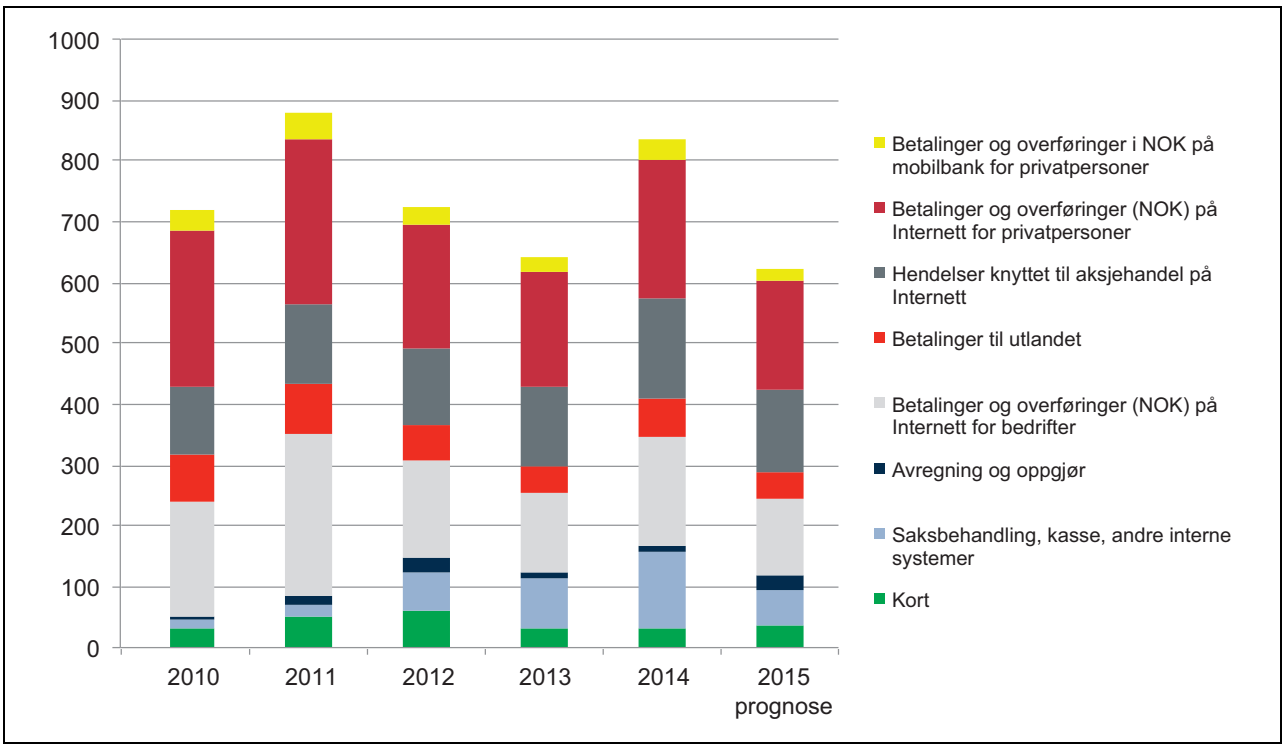
Sårbarhetene beskrives i det følgende ut fra fem områder. Det handler om å

1. formidle kapital på en sikker måte mellom aktører nasjonalt og internasjonalt
2. sikre befolkningen tilgang til betalingsløsninger for å kunne opprettholde nødvendig handel
3. sikre at betalinger og andre finansielle transaksjoner gjennomføres på en sikker og korrekt måte
4. sørge for sikker og stabil drift av finansielle registre
5. kommunisere med befolkningen om kritiske hendelser i bank- og finanssektoren.

16.5.1 Formidle kapital nasjonalt og internasjonalt

Betalingssystemene er en helt sentral forutsetning for formidling av kapital på en sikker måte mellom aktører nasjonalt og internasjonalt, for eksport og import av varer og tjenester, i grossistleddet, i varehandelen (detaljistleddet), for verdipapirhandel og handel med finansielle tjenester. Betalingssystemene kan deles inn i ulike lag, fra der transaksjonene oppstår, til transaksjonene er avsluttet, slik som vist i tabell 16.1. I prinsippet må alle ledd og lag fungere for at transaksjonen skal kunne gjennomføres. Sårbarheten vurderes å være størst der transaksjonene oppstår, mens konsekvensene øker oppover i verdikjeden. Konsekvensene for finansiell stabilitet er størst ved man-

[4] Finanstilsynet (2015): *Risiko- og sårbarhetsanalyse (ROS) 2014*. Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT).



Figur 16.3 Hendelser veiet mot konsekvens.

Kilde: Finanstilsynet.

Tabell 16.1 Hovedinndeling av betalingssystemer

Hovedinndeling av betalingssystemer	Funksjon	Overordnet om sårbarheter
Internasjonalt oppgjørssystem CLS (Continuous Linked Settlement)[1]	Sentralt system for sikkert oppgjør med akseptabel risiko av internasjonale betalinger (valuta).	Få hendelser, liten grad av endring, ingen direkte kundeinvolvering (PC-er kommer lenger ned i verdikjeden).
Norges Banks oppgjørssystem (NBO)[1]	Sentralt for oppgjør av betalinger i Norge.	Alvorlige feil vil kunne stoppe betalingssystemene.
Bankenes felles avregnings- og oppgjørssystem NICS (Norwegian Interbank Clearing System)[1]	Sentralt for gjennomføring av betalinger i Norge. Dette laget inkluderer banker, som har konsesjon for å drive avregnings- og oppgjørssystemer (avleverer i praksis transaksjonene til NICS).[2]	Alvorlige feil over lengre tid vil få alvorlige konsekvenser for finansiell stabilitet.
Verdipapiroppgjøret (VPO) forvaltet av Verdipapirsentralen	Leverer pengeoppgjøret direkte til Norges Banks oppgjørssystem. System for overføring av finansielle instrumenter, med fellesregler for avregning og oppgjør.	Alvorlige feil vil kunne stoppe verdipapirhandelen.
Bankenes *egne* betalingssystemer, inkludert transaksjonsinnsamlingssystemer	Deler av infrastrukturen er felles, eksempelvis for pengeautomater. Leverandøren Evry er sentral.	Feil som oppstår, kan avgrenses, men for de største bankene vil konsekvensene være store. Feil får også konsekvenser for kundene.
Bankenes *felles* betalingssystemer, inkludert transaksjonsinnsamlings-systemer	Felles infrastruktur, der BankAxept er den sentrale løsningen. Mange mindre løsninger inngår i felles infrastruktur. Ivaretas i dag i stor grad av leverandøren Nets.	Kan medføre store konsekvenser for kundene, særlig om bortfallet varer i lang tid.
Bankenes felles autentiseringssystem	Felles autentiseringssystem (inkludert digital signatur) ivaretas av BankID Norge AS. Drift av systemer er utkontraktert til Nets.	Representerer et ledd som kan medføre store konsekvenser ved bortfall.

[1] Disse benytter det internasjonale meldingssystemet SWIFT, som er et sentralt meldesystem for gjennomføring av internasjonale betalinger mellom kunder (i ulike land) via banker (korrespondentbanker).
[2] For store transaksjoner benyttes SWIFT-format også videre til NBO.

glende muligheter for oppgjør. Ettersom aktørene i finanssektoren i stor utstrekning benytter den samme nettverksinfrastrukturen, vil dette medføre en konsensentrasjonsrisiko der konsekvensen ved en feilsituasjon er stor. For kundene kan bortfall av felles betalingstjenester representere store konsekvenser, særlig om bortfallet varer over lang tid.

16.5.2 Sikre befolkningen tilgang til betalingsløsninger

BankAxept-løsningen er fortsatt dominerende som betalingsmiddel i varehandelen, ettersom alle aksepterer BankAxept. De internasjonale kredittkortene har gradvis økt sin andel, men det vil likevel være slik at bortfall av BankAxept-løsningen får størst konsekvenser for befolkningen ved bortfall over lang tid. Dette vil også ha innvirkning på finansiell stabilitet.

Det vurderes likevel å være store fordeler med et felles system der store investeringer i effektivitet og sikkerhet kan resultere i robuste løsninger og felles grensesnitt som er til fordel for forbrukerne. Dette er situasjonen i Norge, samtidig som konsekvensene ved bortfall også dermed kan bli størst.

Det introduseres stadig nye tekniske tjenesteelementer, eksempelvis med bruk av smarttelefon og trådløs kommunikasjon for både chip og smarttelefon. Selv om dette representerer fleksibilitet for den enkelte brukeren, kan det samlet medføre økt sårbarhet.

Handel på Internett er i sterk økning. En virtuell valuta er en type uregulerte digitale penger som ikke er utstedt eller garantert av en nasjonal sentralbank, og kan fungere som betalingsmiddel ved kjøp og handel.

De ulike løsningene for betalingsformidling er mange og med ulikt sikkerhetsnivå. Det er forskjell på grensekryssende betalingstjenester innenfor og utenfor EU/EØS. Dette er omhandlet i nasjonale retningslinjer for sikkerhet ved Internett-betalinger og i forslag til forskrift til betalingssystemloven.[5] Se også nærmere omtale av PSD2 i punkt 16.6.

Slike løsninger i stort omfang kan representere en økt samfunnsmessig risiko. Denne utviklingen kan være krevende å forholde seg til for både forbrukerne, næringen og myndighetene. Det er større sannsynlighet for kriminelle angrep på tjenestene i et åpent nett.

Boks 16.3 Mobil «lommebok»

Smarttelefoner brukes i økende grad til betalingstjenester. I tillegg til nettbank og ulike former for SMS-betalinger er kontaktløse betalinger (NFC – Near field communication) en av de nye betalingstjenestene som er kommet. NFC innebærer at man betaler med både betalingskort og mobilen bare ved å holde enheten inntil betalingsterminalen. Mobiltelefonen eller betalingskortet er knyttet opp til en bankkonto eller en kredittkortkonto. ApplePay er eksempel på en slik tjeneste. Den norske tjenesten mCash er en annen form for mobil lommebok, som benytter seg av en annen type teknologi, der mobilkameraet benyttes i kombinasjon med en QR-kode i butikken.

[5] Finanstilsynet (2015): *Endelige retningslinjer for sikkerhet i internettbetalinger.* Med virkning fra 15.08.2015.

Dynamikken i EØS-samarbeidet og euro-området vil kunne gi store endringer på bank- (særlig for betalingssystemer) og verdipapirområdet. Endringene kan samlet bidra til å øke operasjonell risiko i en overgangsperiode. Det er en risiko for at felles EØS-regler kan resultere i at kravene til IKT-sikkerhet blir lavere enn de kravene vi allerede har i Norge.

16.5.3 Sikre betalinger og andre finansielle transaksjoner

Det omfattende samarbeidet i finansnæringen i Norge har bidratt til at betalingssystemene har vært effektive (frigjort store ressurser), stabile (basert på tilgjengelig statistikk) og sikre (basert på statistikk over tapsutviklingen). Sett opp mot andre, sammenlignbare, land ligger Norge lavt når det gjelder tap. Tiltak som har bidratt til denne utviklingen, har blant annet vært finansforetakenes vektlegging av konfidensialitet, integritet og tilgjengelighet, finanssektorens samarbeid i regi av felles organer og bransjeorganisasjoner, og myndighetskrav til sektoren.

Det betyr likevel ikke at man unngår en potensiell alvorlig hendelse i fremtiden. Dette gjelder både potensielle tilsiktede og utilsiktede hendelser. For tilsiktede hendelser har trusselaktørene vist at de har både vilje, kreativitet og ressurser til å angripe banker. I tillegg kan hvitvasking representere en økt risiko med misbruk av betalingssystemer og inngår som et element i økt internasjonal organisert kriminalitet.

Lange og uoversiktlige leverandørkjeder er en utfordring. Hvem som er involvert i finansnæringens «økosystem» vil kunne utfordre og øke risikoen fremover. I tillegg kan større omfang av kjøp av ressurser og kompetanse utenfor Norge, og nedbygging av ressurser i Norge, på sikt medføre utfordringer med å opprettholde tilstrekkelig styring og kontroll med betalingsløsningene. Driveren for bankenes utkontraktering er primært kostnadskutt, men også det å sikre nøkkelkompetanse og global videreutvikling av teknologi.[6] Endringstakten, både hos finansforetakene og på leverandørsiden, den teknologiske utviklingen og nye aktører både nasjonalt og internasjonalt vil stille store krav til aktørene for å opprettholde den stabiliteten Norge har hatt på betalingssystemområdet de seneste årene.

[6] Gottschalk, Petter (2013): *Flytting av arbeidsoppgaver til utlandet. En oversikt over forskning om mål og resultat når virksomheter setter ut til andre å utføre tjenester. BI. Til Finansforbundet.*

Boks 16.4 Svindel og bedragerier mot nettbankene

Fra cirka 2007 har hacking, angrep og ransforsøk mot nettbankene vært en reell trussel. Julen 2007 ble to norske banker utsatt for et nettbanktrojanerangrep samtidig, der angriperne forsøkte seg på automatisert pengeoverføring etter at kunden hadde logget på nettbanken. Bankene oppdaget det, og samarbeidet tett om å håndtere og motarbeide angrepene. Bankene tok følgende lærdom av dette:

- Det er viktig at kundene forstår truslene tilstrekkelig, og gjør sin del av jobben med å motvirke dem. For bankene innebærer dette å være åpen om trusselbildet og informere om sikkerhetshendelser, slik at kundene får en god forståelse av trusselbildet.
- De digitale truslene rammer ofte bredt, og går gjerne mot flere banker samtidig. Samarbeid og informasjonsdeling mellom bankene er en effektiv og kosteffektiv måte å motvirke angrep på.
- En tilstrekkelig god forståelse av de digitale tjenestenes oppbygging og virkemåte for å oppdage og forstå angrep er viktig. En slik forståelse kommer ikke av seg selv, men vil være et resultat av bevisste valg, prioriteringer og investeringer.
- Samarbeid og gode nettverk er viktig. Blant annet skjer angrepene ofte i flere land samtidig, og det kan være mye å lære ved å samarbeide over landegrensene. Videre har samarbeidet mellom bankene og politiet/Kripos resultert i flere arrestasjoner og dommer for nettbankbedragerier i Norge de siste årene.

I årene etter 2007 ble det gradvis hyppigere angrep mot nettbankene, dette var et viktig moment i etableringen av FinansCERT i 2013.

Boks 16.5 Hacking mot banker har gitt store økonomiske tap internasjonalt

I 2014 ble opp mot hundre banker og finansielle institusjoner i 30 land rammet av angrepene fra en gruppe hackere kalt Carbanak. Ifølge en rapport fra Kaspersky Lab medførte hendelsene store økonomiske tap, der eksempelvis en enkelt bank ble tappet for over 10 millioner dollar. Hendelsen viste at hackerne fikk de største utbyttene via elektroniske transaksjoner. Ingen norske banker ble rammet av angrepet.

Enkelte problemstillinger må vies særskilt oppmerksomhet ved utkontraktering ut av Norge. Noen av disse er knyttet til:

- Annen jurisdiksjon som ofte er vanskelig å overskue konsekvensene av for eksempel norske myndigheters behov for rask tilgang til data i en gitt situasjon.
- Korrupsjonsgrad og den «iboende» kriminaliteten som følger av dette.
- Beskyttelse av personopplysninger.
- Bruk av skytjenester kan representere gode løsninger for mindre virksomheter som hver for seg har liten samfunnsmessig betydning. Det er noe helt annet når det gjelder samfunnsmessig virksomhet eller for eksempel bankenes IKT-løsninger på sentrale områder som kundereskontro. Slik de fleste leverandørene av skytjenester i dag opererer, kan en kunde kanskje sikre at dataene lagres i en region, for eksempel Europa. For virksomheter som banker, der hele bankens virksomhet i praksis er IKT-basert, vil det å ha hele bankens kundeportefølje i en slik løsning kunne være problematisk. Foreløpig er det bankenes egne vurderinger av risiko og kvalitative regelverk som styrer dette.

16.5.4 Sikker og stabil drift av finansielle registre

Med finansielle registre menes i denne sammenheng registre som gir oversikt over fordringer, innskudd, lån, pant, heftelser, eierskap og forsikringer.

Mange av betalingstjenestene må av naturlige grunner distribueres helt ut til sluttbrukerne, og kanalene som benyttes kan være sårbare. Det som ofte betegnes som kjernesystemer, innlån,

utlån, depotsystemer (omfatter også pant), panteregistre, forsikringssystemer og eiendomsregistre (offentlige), inngår i finansforetakenes sentrale løsninger.

Særlig når det gjelder banker og forsikring, behandles denne typen løsninger i stor grad fortsatt på sentrale stormaskiner og har flere lag med beskyttelse. Bruk av nye distribuerte plattformer kan ha samme strenge driftsopplegg. Det gjør at aktører via offentlige nett ikke uten videre får tilgang, og terskelen for å hacke seg inn er større enn for løsninger som er knyttet direkte opp i Internett. Dette har resultert i at det er rapportert få slike hendelser i Norge. På den annen side er det en vurdering at ressurssterke kriminelle grupper og stater som er engasjert i denne typen virksomhet, har kapasitet til å utøve skadeverk.

En annen potensiell sårbarhet er at mange av denne typen systemer er gamle, med til dels komplekse løsninger som er utviklet gradvis over mange år. Deler av teknologien er under utfasing, og kompetansen er heller ikke så lett tilgjengelig lenger. Konsekvensene av en alvorlig og langvarig hendelse på denne typen systemer vil kunne bli katastrofal, både for samfunnet, for næringslivet og for den enkelte innbygger.

16.5.5 Kommunisere med befolkningen om kritiske hendelser

En rekke sårbarheter kan utfordre kommunikasjonen med befolkningen om kritiske hendelser i bank- og finanssektoren og om hvordan den enkelte bør forholde seg for å opprettholde normalitet i dagliglivet. Sårbarheten vurderes å kunne være stor på dette området.

Finansforetakene har et klart ansvar for å informere kundene sine om alvorlige hendelser som får konsekvenser for dem. Finanstilsynet har eksempler på at enkeltforetak ikke tar dette ansvaret ved en alvorlig hendelse, men i praksis peker på leverandøren. Bransjeorganisasjoner tar ofte et sektoransvar for informasjon om alvorlige situasjoner som ikke bare berører den enkelte bank. Det er et samarbeid på dette området gjennom Beredskapsutvalget for finansiell infrastruktur (BFI), med deltagelse fra myndigheter, bransjeorganisasjoner, viktige enkeltforetak (representativ deltagelse) og andre med viktige oppgaver for beredskapen. Hensikten er å sikre en formell møteplass om forebyggende arbeid og ved alvorlige beredskapssituasjoner der BFI blant annet skal gi råd til de utøvende myndighetene.

Finansmyndighetene har et ansvar for å informere om alvorlige hendelser som får konsekvenser for finansiell stabilitet, finansforetak og kunder. Dette må skje ut fra det mandatet myndighetsorganet har, eksempelvis Norges Bank ut fra sentralbankloven, Finanstilsynet ut fra finanstilsynsloven og Finansdepartementet som overordnet myndighetsorgan for hele finanssektoren. Andre myndighetsorganer som har et horisontalt ansvar, kan også være aktuelle, men bør samordne dette med sektormyndigheten. Som et eksempel har tjenestene til Nav og Skatteetaten vært gjenstand for samordning mellom sektormyndighetene. Finanstilsynet har redegjort for rutiner for varsling og beredskap overfor andre etater ved alvorlig svikt i betalingsformidlingen. Fra motsatt perspektiv har Nav og Skatteetaten redegjort for de mest kritiske ut- og innbetalingene. Varslingsveien vil være fra Finanstilsynet til

Boks 16.6 Virksomhetenes avhengighet av betalingssystemer

Nav er helt avhengig av tilgjengelige betalingssystemer for å løse sitt samfunnsoppdrag. Hver måned er 1,4 millioner brukere avhengig av utbetalinger fra Nav. Nav har lagt inn beredskap ved å være tilknyttet to banker. En fjerdedel av betalingsoverføringene gjennomføres fast gjennom den andre bankforbindelsen. Med dette får begge bankene utbetalinger regelmessig, og det er mulig å bytte bankforbindelse dersom den ene forbindelsen skulle være nede, selv om dette vil ta noen dager. For de mest kritiske utbetalingene er Nav ferdig med transaksjonene til bankene fem–ti dager før de skal inn på konto. Dette er en sikkerhetsmargin dersom systemene er utilgjengelige eller det oppstår feil i transaksjonene. Utenfor Navs virkemiddelapparat kan det også oppstå svikt som hindrer at brukerne får utbetalingene til rett tid – enten ved at Navs bankforbindelser blir forhindret fra å gjennomføre transaksjoner videre til brukernes banker, eller at brukerne i ytterste ledd ikke får brukt kort til betalinger i butikk eller uttak i minibanker. Nav har liten innflytelse på disse to scenarioene, men ønsker å vite hva slags beredskap bankene har for dette, ettersom Nav fort vil ende opp med å være kontaktpunktet for alle brukerne dersom de blir rammet. Nav har derfor tatt et initiativ overfor Finanstilsynet for å skaffe seg innsikt i de beredskapstiltakene finansnæringen har etablert.

Finansdepartementet, som så vil varsle videre til det aktuelle departementet, som igjen vil varsle den aktuelle underliggende etaten.

På tross av øvelser på dette temaet og andre forberedelser vil det alltid være utfordrende å håndtere alvorlige hendelser som får store samfunnsmessige konsekvenser, på en optimal måte. I tillegg er det utfordrende å få delt kunnskapen om kontinuitet og beredskap på nasjonalt nivå i tilstrekkelig grad.

16.5.6 Særskilte personvernutfordringer

Finansinstitusjoner i Norge utveksler i stor grad personopplysninger med enheter i andre stater. I transaksjonsdata inngår personopplysninger eller opplysninger som kan knyttes til en person. Dette er nødvendige opplysninger for å kunne vite «hvem som har betalt hva», eller «hvem som har kjøpt hvilke verdipapirer». Krav til personopplysningsinnhold i transaksjoner er regulert blant annet gjennom EU-lovgivning. Gjennom en felles operasjonell infrastruktur (FOI) behandles store mengder persondata. I felles registre på forsikringssiden oppbevares også store mengder personopplysninger, noen av dem sensitive.

Boks 16.7 Angrep mot storbanken JPMorgan Chase

Høsten 2014 ble den amerikanske storbanken JPMorgan Chase utsatt for et stort cyberangrep da en gruppe hackere brøt seg inn i datasystemene deres. Ifølge The New York Times ble rundt ni andre banker og meglerhus rammet av innbruddet, som beskrives som et av de mest omfattende noensinne. En av konsekvensene av angrepet var at personopplysninger til 83 millioner personer og virksomheter kom på avveie.

Hendelsen ble etterforsket av amerikanske myndigheter og skapte frykt for at den stjålne informasjonen kunne bli brukt i svindelforsøk. I tillegg var det en reell mulighet for at kunder ville tape tillit til banken, som i etterkant gikk bredt ut til sine interessenter og redegjorde for hvilke sikkerhetstiltak de hadde etablert for å unngå lignende hendelser. Ifølge redegjørelsen hadde JPMorgan Chase investert mer enn 250 millioner dollar og gitt mer enn 1 000 ansatte i oppdrag å satse på cybersikkerhet innen utgangen av 2014.

Utlevering av personopplysninger til andre lands stater er hjemlet i lover innrettet på å bekjempe terrorfinansiering, hvitvasking, skatteunndragelser og annen kriminalitet. Utenom slike offentligrettslige bestemmelser er utleveringsadgang regulert gjennom avtaler (konsernavtaler, herunder «Binding Corporate Rules», utkontrakteringsavtaler og så videre). Finansinstitusjonene har konsesjoner gitt fra både Finanstilsynet og Datatilsynet som regulerer virksomheten og behandlingen av personopplysninger.

Med bakgrunn i den amerikanske loven FATCA (Foreign Account Tax Compliance Act), har Norge og USA inngått en avtale om informasjonsdeling som innebærer at alle norske banker og finansinstitusjoner skal identifisere hvilke kunder som er skattepliktige til USA. Det blir oversendt informasjon om privatpersoner og eiere av selskaper som har konto i norske banker, og som er bosatt i USA, født i USA eller er amerikanske borgere. Personvernhensyn ble diskutert da reglene ble innført.

Finansinstitusjoner i Norge har også ulike hjemler til å utveksle informasjon med andre finansinstitusjoner som ledd i for eksempel gjennomføring av kontraktsforpliktelser med kunder (oppgjør/betalingsforpliktelser/tvisteløsning) og kriminalitetsbekjempelse (hvitvaskingsloven). Ved utkontraktering av virksomhet vil finansinstitusjoner inngå direkte avtaler med den som får oppdraget. Dette vil kunne være foretak i Norge og i utlandet.

Finansinstitusjoner prioriterer personvern når de utvikler nye tjenester og systemer. Dette er ifølge krav etter gjeldende regelverk, herunder personopplysningsloven, IKT-forskriften og hvitvaskingsloven. Finansinstitusjoner er også underlagt streng taushetsplikt, noe som begrenser utlevering av personopplysninger og utvikling av nye tjenester og systemer.

I 2007 gjennomførte Nordea en gransking etter at det ble hevdet at bankansatte i Nordea hadde lekket informasjon om kongehuset og andre kjendiser til Se og Hør. Granskingen var avhengig av at det fantes logger med oversikt over hvilke ansatte som hadde gjort oppslag på ulike konti. Datatilsynet hadde ingen innvendinger mot granskingen og er et eksempel på at kundenes personvern kan veie tyngre enn de ansattes personvern.

Finans Norge ser både store utfordringer og muligheter knyttet til innsamling av store data i forbindelse med utvikling av nye tjenester og systemer. I vurderingen av ulike muligheter må næringen veie flere hensyn opp mot hverandre,

for eksempel forretningsdrift/inntjening, taushetsplikt, sikkerhet, kundevennlighet og hensynet til den enkeltes personvern. Det totale regelverksbildet næringen er underlagt, setter begrensninger og rammer for hvilke systemer og tjenester som kan utvikles og markedsføres, og hvilken informasjon som kan behandles av finansinstitusjoner.

I en rapport fra Forbrukerrådet i 2014 påpekes det blant annet at det eksisterer en rekke uklare betingelser om bruk av personopplysninger. Det blir også påpekt problemstillinger knyttet til eventuell misbruk av digitale spor. Forbrukerrådet mener at bankene bør prioritere produktinnovasjon på betalingstjenesteområdet, og kommer til å følge utviklingen for å sikre at forbrukernes interesser blir ivaretatt i denne prosessen.[7]

Boks 16.8 Konsekvenser for finanssektoren ved bortfall av ekom

I DSBs nasjonale risikobilde for 2014 synliggjøres store konsekvenser for finansiell stabilitet som følge av bortfall av ekomtjenester i fem døgn:

- Det antas at pengetransaksjoner stopper opp og terminaler fungerer i begrenset grad.
- Uten tilgang til kunde-, konto-, og saldoinformasjon vil korttransaksjoner og utlevering av kontanter stoppe etter et par dager.
- «Masseutbetalinger» (for eksempel trygd fra Nav), nett- og mobilbank, utenlandshandel og oppgjørssystemer faller bort.
- Forbindelsen mellom bankene faller ut.

Finanssektorens nødløsninger kan minske skadene hvis nettet innimellom fungerer, men hvis kommunikasjonen faller helt bort, vil alle finansielle transaksjoner stoppe opp. Stans i pengesirkulasjonen får virkninger for finanssektoren, næringslivet, publikum og offentlig virksomhet. Det at finansielle registre og nasjonale felleskomponenter som Enhetsregisteret, matrikkelen og Altinn ikke fungerer, antas å føre til forsinkelseskostnader.

[7] Forbrukerrådet (2014): *Du selger deg billig – En rapport om betalingsløsninger og personvern.*

16.5.7 Avhengighet av kraft og elektronisk kommunikasjon

Avhengigheten av elektronisk kommunikasjon (ekom) er stor. Sentrale finansaktører bruker i stor grad samme kraft- og ekomleverandører. Finansbedrifter og IKT-leverandører kan ikke selv sikre reservekommunikasjon dersom teleoperatørenes leveranser faller ut. Bankenes Standardiseringskontor stiller krav til felles infrastruktur, men det stilles i bransjen spørsmål om hvem som sitter på den helhetlige oversikten. Dette er avgjørende for å sikre reell redundans.

Finanstilsynet har vært pådriver i arbeidet med å forankre finanssektorens prioritering av tilgang til kraft og ekom i en beredskapssituasjon. Det er gjennomført møter mellom aktørene og etablert rutiner for at kraft- og ekomleverandører skal kunne prioritere kritiske finanstjenester i en krisesituasjon. Dette er gjort i samråd med BFI.

16.6 Fremtidige problemstillinger og trender

Det antas at utviklingen av betalingstjenester fremover i større grad vil foregå utenfor den tradisjonelle banksektoren. Ny teknologi, nye aktører og forretningsmodeller gjør dette mulig, noe som skaper økt konkurranse i markedet for betalingstjenester – særlig for småbetalinger. Internasjonale aktører som PayPal og Google har betalingsløsninger som ikke er utviklet i bank. Et annet eksempel er Starbucks, som på kort tid har vokst seg til å bli en stor bank i USA. Utviklingen av nye betalingstjenester vil gi forbrukerne flere instrumenter å velge mellom, slik at de kan velge det som passer dem best. I en rapport fra Norges Bank fremgår det at dersom nye betalingsmåter skal få gjennomslag, må brukerne oppleve at tjenestene er raskere eller har funksjoner som eksisterende betalingstjenester ikke har. Samtidig må sikkerheten være god og prisen akseptabel.[8]

I EU foregår det store diskusjoner på regelverkssiden, blant annet om det nye betalingstjenestedirektivet PSD2 (Payment Services Directive 2), som trer i kraft tidlig i 2016. DG FISMA oppgir at årsaken til at behandlingen av direktivet har vært så tidkrevende, er at rådet har vært opptatt av gode tiltak på informasjonssikkerhet. Finanstilsynet har påpekt to vesentlige områder i det nye direktivet:

[8] Langbråten, Nina (2012): *Nye betalingsmåter.* Norges Bank.

- Tilbydere av betalingsinitiering og kontoinformasjon og deres rett på vegne av den som betaler, å initiere betalinger og innhente kontoinformasjon.
- Krav til styring av operasjonell- og sikkerhetsrisiko knyttet til betalingsløsninger og krav til autentisering, der tidligere henvisninger til NIS-direktivet nå er erstattet med lovtekst i direktivet.

Internasjonalt fremheves finansmarkedsinfrastrukturer som avgjørende for å opprettholde finansiell stabilitet, og Norge fremheves som et land med en moderne og stabil finansmarkedsinfrastruktur.[9] I en rapport fra The Bank for International Settlements (BIS)[10] fremheves det at IKT-angrep på finansielle systemer øker i frekvens og omfang og stadig blir mer sofistikerte. Til tross for at dette området er høyt prioritert av ledelsen i selskaper, fremheves det at tiltakene må intensiveres, gitt den hurtige utviklingen i truslene mot finansiell infrastruktur. Det nevnes blant annet utfordringer med deling av gradert informasjon i multinasjonale selskaper, og myndighetene oppfordres til å bistå virksomhetene med å løse disse utfordringene gjennom koordinerte tiltak mellom offentlig og privat sektor.

I Finanstilsynets ROS-analyse for 2014 går det frem at det i 2014 var over 550 typer ulike virtuelle valutaer på verdensbasis. Virtuelle valutaer deles inn i to kategorier – sentrale og desentrale. De desentrale virtuelle valuatene som bitcoin, som ikke har noen aktør bak seg, representerer en økt risiko for brukerne, ettersom brukerne ikke har rettsbeskyttelse utover allmenn lovgivning. Finanstilsynet deltok i 2014 i et arbeid i regi av EBA (European Banking Authority), der man så på om virtuelle valutaer kan og bør reguleres. Rapporten konkluderte blant annet med at «risikoen man ser, overstiger langt de fordelene man kan se, særlig i europeisk sammenheng». Som en konsekvens av konklusjonene i rapporten har flere lands myndigheter gått ut med varsler og fra-

[9] International Monetary Fund (IMF) (2015): *Financial System Stability Assessment for Norway.*

[10] The Bank for International Settlements (BIS) (2014): *Cyber resilience in financial market institutions.*

Boks 16.9 Endringer i føringer

Verdiøkende tjenester knyttet til betaling og kontoinformasjon kommer på markedet, der nye grupper av tjenesteleverandører blir regulert i det nye betalingsdirektivet. ECB (European Central Bank)/ EBA (European Banking Authority) har tatt initiativ for å definere sikkerhetskrav. Kravene vil gjelde for foretak under regulering.

Et overordnet premiss er at kravene ikke fører til uønskede innlåsingseffekter. Sikkerhetskravene for tilgang til konto må ikke være slik at de låser kunden inne i det eksisterende tjenestetilbudet, og reglene må ikke være slik at de låser tilbyderne ute når det gjelder å tilby alternative eller verdiøkende løsninger.

Det er ønskelig at kravene kan bidra til at tjenestene kan virke på tvers av landene i Europa.

Finanstilsynet ser nå konturene av prinsipper som anses hensiktsmessige for å oppnå dette.

- Det skal defineres standardiserte grensesnitt som tilbydere kan benytte for å få tilgang til konto.
- Der det eksisterer en standard når det gjelder krav til sikkerhet for et gitt sikkerhetsnivå, skal denne standarden kunne benyttes/ tilbys. Dette kan tenkes å gjelde innenfor områder som PKI, kryptering og autentisering.
- Proprietære løsninger som låser kunden inne og tjenestetilbyderen ute, er ikke ønskelige.
- Effektivitet i oppgjør og levering av varer og tjenester, samt ønsket om utvikling av nye tjenester, tilsier at tilgangen til konto bør være direkte og ikke indirekte.
- En tilbyder av tjenester som bygger på kontoinformasjon, skal autentisere seg overfor kunden og banken.
- Tilbyderen skal kunne bygge på bankens autentiseringsløsning.
- Tilbyderen skal kommunisere med bruker og bank på en sikker måte i henhold til tekniske standarder utviklet av EBA i nært samarbeid med ECB.

EBA har tidligere utgitt ECBs anbefalinger til sikkerhet når det gjelder Internett-betalinger. Grunnsikringen har ikke vært ansett som tilstrekkelig på dette området. Anbefalingene innebærer en innskjerping av sikkerheten når det gjelder betalinger med blant annet kort utstedt av norske banker og kredittkortselskaper. Anbefalingene gjelder fra 15. august 2015.

rådet finansnæringen å kjøpe eller eie slik virksomhet. Det advares mot at virtuelle valutaer kan innebære stor risiko for brukerne, ettersom de ikke er regulert eller garantert av en sentralbank. Hittil er ingen forpliktet til å motta virtuelle valutaer som betaling, og Skattedirektorat har vurdert omsetning av bitcoin til å være en elektronisk tjeneste og ikke en valuta.[11]

Valutaer som bitcoin og litecoin kan være med på å tilrettelegge for kriminalitet, ettersom valutaene tillater anonymt eierskap og anonyme overføringer av verdier. Samfunnets kontrollinstanser og politiet vil da ikke lenger kunne følge pengestrømmer ved mistanke om ulovlige transaksjoner. Det er eksempler på at bitcoin er blitt brukt av kriminelle til å presse individer og bedrifter for penger, for eksempel ved løsepengeviruset CryptoLocker.

16.7 Vurderinger og tiltak

Utvalget mener at finansnæringen representerer en sektor med høy bevissthet rundt de truslene og sårbarhetene økt digitalisering medfører, sammenlignet med andre sektorer. Sikkerhet har hittil ikke vært en konkurransefaktor, men noe finansnæringen har samarbeidet om for å kunne ta i bruk ny teknologi. Dette er begrunnet i blant annet økonomi, slik at bankene kan komme frem til gode fellesløsninger på et tidlig tidspunkt. Utvalget mener det er viktig at finansnæringen fortsetter å styrke og effektivisere den samhandlingen som allerede eksisterer. Dette vil også være avgjørende på grunn av den sterke avhengigheten mellom bankene, for eksempel at det for kundene vil være et problem når andre banker er utilgjengelige.

God operasjonell risikostyring er sentralt for å forstå nivået på risiko i en virksomhet, og er særlig viktig for virksomheter i finansnæringen, der IKT er et helt sentralt virkemiddel. Finanstilsynets krav bidrar til at det gjennomføres regelmessige risikoanalyser, men det sikrer ikke nødvendigvis nivået på kvaliteten. Det er viktig at sektoren – både virksomhetene og tilsynsmyndighetene – gjennomfører kvalitativt gode risikoanalyser, gitt kompleksiteten i arkitektur og verdikjeder.

Utvalget foreslår følgende tiltak:

16.7.1 Styrke innsatsen på vurdering av fremtidige betalingstjenester

Utviklingen av nye betalingstjenester foregår raskt og utfordrer de tradisjonelle samarbeidsmønstrene mellom bankene. Ut fra et næringsperspektiv og av effektivitetshensyn er dette en utvikling som gir både enkeltpersoner og næringslivet mange fordeler. Dette utfordrer imidlertid finansnæringen med hensyn til håndtering av risiko. Det er lagt stor vekt på raskt å omsette ny teknologi til nye tjenester. Brukervennlighet og «time to market» vil ofte prioriteres, noe som kan gå på bekostning av sikkerhet og operasjonell stabilitet. Dette er eksempler på at de nye betalingstjenestene kan medføre nye digitale sårbarheter, der utfordringene ligger utenfor nasjonal kontroll og Norge ikke i like stor grad har mulighet til å påvirke.

Finansforetak vil kunne bli involvert i å tilrettelegge løsninger som ikke er tilstrekkelig sikre. Selv om dette foreløpig er svært begrenset, vil det kunne øke i omfang og bli en utfordring, blant annet ved at det blir flere ledd i verdikjeden som bankene ikke har kontroll over.

Utvalget mener finansnæringen bør rette mer oppmerksomhet mot disse problemstillingene, blant annet for å sikre at regelverket også fremover er relevant og tilpasset. Finansdepartementet bør innta en tydeligere rolle for å følge med på nye aktører som tilbyr bank- og betalingstjenester.

16.7.2 Videreføre tverrfaglig samarbeid for god beredskapsevne og håndtering av alvorlige tilsiktede IKT-hendelser

Utvalget mener det er viktig å videreføre det gode arbeidet som gjøres i dag med hensyn til rapportering og håndtering av tilsiktede IKT-hendelser. En systematisk tilnærming til hendelseshåndtering bidrar til effektiv gjenoppretting, statistisk oversikt over utviklingen og ikke minst evne til å lære av feilene for å iverksette nye og/eller justerte tiltak. Utvalget oppfatter Finanstilsynets initiativ for 2015 om identifisering av rotårsaker til alvorlige hendelser som viktig i denne sammenheng. Utvalget mener det er positivt at bransjen selv har tatt initiativ til FinansCERT. Det synes å være et stort eierskap til FinansCERT i sektoren. Utvalget poengterer at det må tilrettelegges for bredere samarbeid og informasjonsdeling nasjonalt. Det er avgjørende med et godt organisert samarbeid på tvers av CERT-ene for å få best mulig nytte ut av ressursene.

I tillegg mener utvalget at FinansCERT, i samarbeid med foretakene, må ta høyde for å etablere

[11] Norges Bank (2014): *Finansiell infrastruktur 2014.*

risikoindikatorer som kan fange opp hendelser som ikke følger hittil kjente angrepsmønstre («black swan»[12]), og i større grad være forberedt på sjeldne, men store hendelser.

Utvalget er kjent med arbeidet i Beredskapsutvalget for finansiell infrastruktur (BFI) og de fellesøvelsene som BFI iverksetter årlig. Det er viktig å tørre å planlegge for de sjeldne krisescenarioene, som at den elektroniske infrastrukturen blir utilgjengelig over lengre tid, og at man må gå over til alternative løsninger. *Utvalget stiller spørsmål ved hvor godt forberedt sektoren vil kunne være til å håndtere de store krisene, og mener BFI, i samarbeid med FinansCERT, må ta initiativ til mer samordnede og komplekse øvelser, med tilstrekkelig tyngde og realisme.* Dette blir desto viktigere, gitt utviklingen av lange og komplekse leverandørkjeder. Videre bør krisekommunikasjon til kundene øves.

16.7.3 Analysere sårbarhetskonsekvensene som følge av utkontraktering ut av landet

Utvalget mener det er en svakhet at det er få økonomiske incentiver til å tenke langsiktig med hensyn til kompetansebehov ved utkontraktering. Det må stilles krav til hva slags kompetanse og kapasitet organisasjonen som utkontrakterer, må ha for faktisk å ivareta ansvaret rundt leverandøroppfølging. Utvalget opplever en usikkerhet rundt hvorvidt for mange utkontrakterer for mange av oppgavene eller har for lite ressurser til at de reelt kan kontrollere og følge opp avtalen og leveransene. Utvalget er samtidig kjent med at det er vanskelig å finne tilstrekkelig kompetanse i Norge.

Utvalget mener noe av kompetansen må være virksomhetsnær, spesielt med hensyn til beredskap. Det er viktig at virksomhetene har et bevisst forhold til hvilken kompetanse som ikke bør utkontrakteres. Selv om utkontraktering av virksomhet kan være innenfor akseptabel risiko for det enkelte foretaket, kan det medføre samfunnsmessige konsekvenser som ikke kan aksepteres dersom et stort antall foretak i en sektor flytter sin IKT-virksomhet ut av landet.

Etter utvalgets vurdering må Finansdepartementet gi Finanstilsynet i oppdrag å vurdere hva de langsiktige konsekvensene av offensiv bruk av utkontraktering kan bli. Det bør vurderes om utkontraktering av virksomhet som kan være viktig for samfunnet, bør ha krav om at det til enhver tid skal være en virksom «cold backup» lokalt i Norge. I finanssektoren i Norge er det regler for utkontraktering både i IKT-forskriften og i forskrift om risikostyring og internkontroll, men det bør vurderes om disse bør videreutvikles og detaljeres basert på den foreslåtte kompetansevurderingen. *Utvalget mener det er viktig å modnes når det gjelder denne problemstillingen, ettersom utstrakt bruk av utkontraktering på sikt kan bidra til å svekke den nasjonale evnen til utvikling og oppfølging på sentrale kompetanseområder.*

16.7.4 Videreføre og styrke engasjementet for å påvirke internasjonal regulering av IKT-sikkerhetsmekanismer

Utvalget observerer at det er en økende trend at man har felles regelverk med EU og andre internasjonale aktører. Utvalget anerkjenner Finans Norges frykt for å få lavere sikkerhetskrav i Norge som følge av felles regelverk i EU. Internasjonal konkurranse vil kunne bidra til å drive kravene ned mot en nedre grense, selv om Norge i utgangspunktet kan definere strengere minimumskrav. Det er viktig at Finansdepartementet tar en gjennomgang av hvilke arenaer Norge har tilgang til, samt benytter de mulighetene som finnes for å påvirke utviklingen tidligst mulig. *Utvalget er enig med Finanstilsynet i at tilsynsaktivitetene må være à jour med beste praksis, og oppfordrer Finanstilsynet til å videreføre det omfattende samarbeidet som allerede pågår internasjonalt, med andre lands og EUs tilsynsorganer.*

16.7.5 Styrke beredskapstiltak for utviklingen mot det kontantløse samfunnet

Norge er ett av få land der kontantandelen av det samlede pengevolumet er på under 5 prosent. Økt innføring av mer brukervennlige og kosteffektive betalingsløsninger vil sannsynligvis føre til at kontantandelen fortsatt vil synke. Imidlertid spiller fortsatt kontanter en viktig rolle i samfunnet. Det å benytte kontanter som en del av beredskapsløsningen er under utredning av Norges Bank og Finanstilsynet. Finans Norge har angitt at omfattende bruk av kontanter i en beredskapsløsning er lite hensiktsmessig for bankene.

Som en del av myndighetenes vurderinger inngår også en klargjøring av bankenes plikt til å sikre tilbakebetaling til innlånskundene, også i en alvorlig beredskapssituasjon. Grupper i samfun-

[12] «The black swan theory» dreier seg om hendelser som kommer som en overraskelse og har betydelig negativ effekt, men som oppstår svært sjelden, slik at det er lite eller ingen hendelseshistorie å lære av det.

net kan også være mer avhengige av tilgang på kontanter som betalingsmiddel enn andre, så en vurdering av aktiv utfasing av kontanter har flere motstridende faktorer. Full overgang til digitale løsninger og dermed kun elektroniske penger kan ut fra en beredskapsmessig synsvinkel gi økt sårbarhet ut fra dagens status for beredskapsløsningene.

Utvalget mener dette er et eksempel på en stor sårbarhet med digitalt utspring som Norge må ha beredskap for. At det eksisterer kontanter, gir i seg selv flere muligheter i en krisesituasjon. Finansdepartementet bør ta initiativ til å se på hvordan dette best kan løses, blant annet gjennom å se til andre lands håndtering av lignende utfordringer.

Kapittel 17
Helse og omsorg

Nødvendig helsehjelp og omsorgstjenester til befolkningen er en vesentlig og kritisk samfunnsfunksjon for å redde liv, behandle sykdom og gi bistand til dem som trenger hjelp til dagliglivets nødvendige gjøremål. Helsesektoren består av et omfattende antall virksomheter i både offentlig og privat sektor – cirka 17 000 virksomheter og cirka 300 000 ansatte. Sektoren er komplekst organisert i administrative styringsnivåer, ulike nivåer for helsehjelp, ulike grupper helsepersonell og flere forsknings- og kunnskapsmiljøer. Det siste tiåret har sektoren vært igjennom omfattende reformer når det gjelder organisering av helseforetak og senere omfordeling av oppgaver mellom spesialisthelsetjenesten (sykehus) og primærhelsetjenesten (kommunal helse- og omsorgstjeneste). Reformene er gjennomført ved flere særlover. Styring, herunder effektivitets- og sikkerhetsmål ved bruk av IKT, er også en vesentlig del av de gjennomførte og pågående reformene. Sammenlignet med andre land var Norge tidlig ute med å ta i bruk IKT på mange områder i helsesektoren.[1]

Dokumentasjonsplikt, taushetsplikt og behovet for tilgang til nødvendige opplysninger til helsehjelpsformål er grunnleggende krav som stilles til det omfattende antallet IKT-systemer i sektoren. Kombinasjonen av taushetsplikt, tilgjengelighet og korrekt informasjon stiller høye krav til opplysningskvalitet og informasjonssikkerhet i pasientjournalsystemene og til sikker bruk av infrastrukturen som formidler pasientopplysninger mellom virksomhetene. Helsedirektoratet arbeider med løsninger som skal sikre mulighet for elektronisk kommunikasjon mellom lege og pasient og gi pasienter tilgang til egne helseopplysninger.

Deler av utvalgets sårbarhetsbeskrivelse er basert på oppsummering fra workshop om digitale sårbarheter i helsesektoren, se elektronisk vedlegg «Digitale sårbarheter i helsesektoren (SINTEF)».

[1] Meld. St. 9 (2012–2013) *Én innbygger – én journal.*

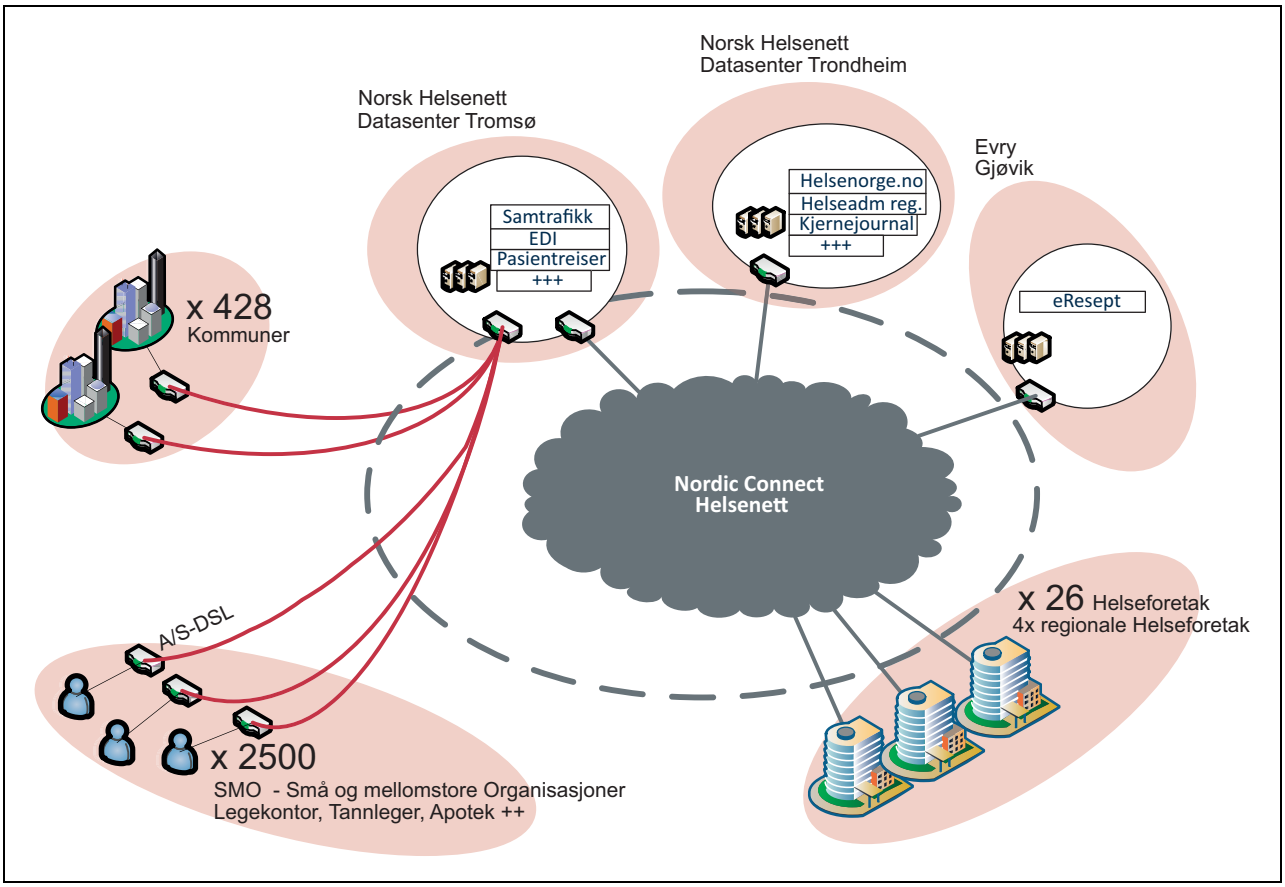
17.1 Infrastruktur

Infrastrukturen internt i sykehus kan være svært kompleks og består blant annet av systemer for pasientstyring (for eksempel elektroniske journaler), systemer for laboratoriestyring, radiologistyring, operasjonsstøtte og klinisk overvåking. Samtlige av disse består igjen av en rekke underliggende systemer. Oslo universitetssykehus oppgir at de anslagsvis har over 1 000 systemer.

Norsk Helsenett ble etablert i 2004 og fasiliterer blant annet et kommunikasjonsnett – helsenettet – som skal legge til rette for sikker utveksling av personopplysninger og kommunikasjon for øvrig. I tillegg skal selskapet levere basistjenester som støtter samhandlingen i hele helse- og omsorgssektoren. Norsk Helsenett eier ikke egen fiberinfrastruktur, men kjøper transmisjon fra tredjeparter, som Telenor. Med Neste Generasjons Kjernenett blir Broadnet leverandør av fiberinfrastruktur til helsenettet. Broadnet vil i tillegg til å benytte eksisterende fibernett etablere en ny infrastruktur for dette formålet.

Helsenettet er etablert for å sikre en felles standardisert infrastruktur for elektronisk samhandling i helse- og omsorgssektoren i Norge. Med et slikt nettverk blir det mulig å standardisere felles tjenester og sikkerhetsregimer.

Nasjonal kjernejournal, e-resept og IKT-systemer til støtte for pasientreiser er eksempler på nasjonale tjenester som tilbys gjennom helsenettet. Virksomheter som knytter seg til helsenettet, er forpliktet til å oppfylle kravene i Norm for informasjonssikkerhet i helsesektoren. Det er et krav at virksomheter som knytter seg til Norsk Helsenett, ikke har egen Internett-forbindelse fra sitt nettverk. Som medlem av helsenettet får virksomhetene tilgang til flere helseadministrative registre, blant annet Norsk Helsenetts adresseregister, Helsepersonellregisteret og Legestillingsregisteret. Norsk Helsenett administrerer på vegne av Skattedirektoratet en kopi av Folkeregisteret som sikrer medlemmene fri tilgang til rele-



Figur 17.1 Norsk Helsenett – dagens situasjon.

Kilde: Norsk Helsenett.

vante folkeregisterdata. Norsk Helsenett er forpliktet til å levere kommunikasjon 24/7.

Utbredelsen av helsenettet har vært i betydelig vekst. I 2014 inkluderte helsenettet over 2 500 helseaktører: offentlig og privat spesialisthelsetjeneste, nesten alle legekontorer, over 700 tannleger, alle norske kommuner, alle apoteker og de fleste av landets laboratorier og røntgeninstitutter. Norsk Helsenett har uttrykt en ambisjon om at alle som har behov for det, skal være tilknyttet helsenettet innen 2020. Samtidig ser de på muligheten for å kommunisere med utenlandske klinikker og sykehus som behandler norske pasienter.

På det meste går det 800 000 unike medisinske meldinger gjennom helsenettet i døgnet. Underleverandører til helsenettet må følge kravene i Norm for informasjonssikkerhet i helse- og omsorgstjenesten. Norsk Helsenett foretar en sikkerhetsvurdering før tilkobling innvilges, og i tillegg blir utstyr og tjenester levert av underleverandører testet for å forhindre uønsket eller skadelig funksjonalitet.

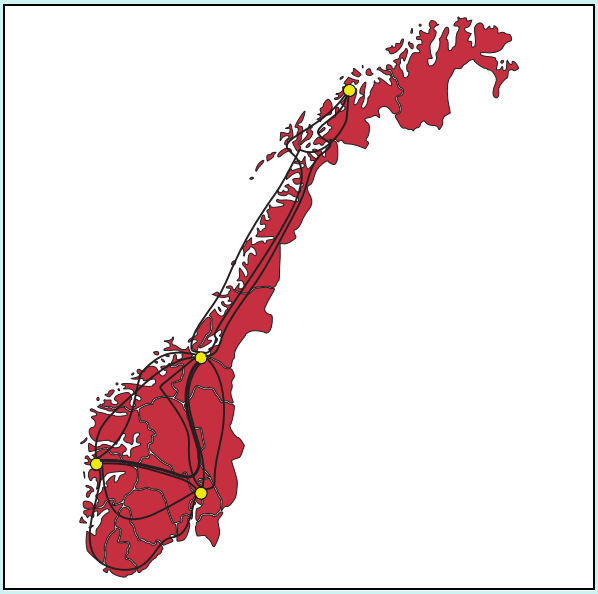
I tillegg til de nasjonale tjenestene som tilbys av Norsk Helsenett, inngår en rekke IKT-systemer i primærhelsetjenesten (kommunehelsetjeneste, fastlegekontorer med videre) og spesialisthelsetjenesten (regionale helseforetak). En komparativ studie fra 2014 viser hvilke IKT-systemer som er i bruk i den enkelte helseregion, og hvilke moderniseringsplaner som foreligger frem mot 2018. Av studien går det frem at kategoriene pasientstyring, spesialistsystemer og digitale tjenester er høyt prioritert. Innenfor kategoriene helseovervåking og beredskap er det ikke planlagt modernisering i perioden.[2]

17.2 Roller og ansvar

Sykehusreformen organiserer og regulerer, med hjemmel i helseforetaksloven og spesialisthelsetjenesteloven, roller og ansvar for spesialisthelsetjenesten (sykehusene). Samhandlingsreformen stiller krav til samarbeid mellom kommune og stat, og helse- og omsorgstjenesteloven tildeler roller og ansvar i primærhelsetjenesten.

[2] Helsedirektoratet (2014): *Utredning av «én innbygger – én journal», Komparativ analyse av de regionale helseforetakene på IKT-området.*

Boks 17.1 Neste Generasjons Kjernenett



Figur 17.2

Kilde: Norsk Helsenett.

I forbindelse med Norsk Helsenetts innføring av Neste Generasjons Kjernenett er det lagt betydelig vekt på høytilgjengelig høykapasitetsnett. Bakgrunnen for det nye helsenettet er behovet for å øke kapasiteten i nettet og gjøre det mer robust. I tillegg er det avgjørende at Norsk Helsenett mer effektivt skal kunne implementere nye tjenester. Dagens infrastruktur tar for eksempel ikke høyde for innføringen av Nasjonal kjernejournal. Norsk Helsenett er i ferd med å etablere georedundante løsninger, og har tilgang til tre eller flere optiske bølgelengder i minst tre uavhengige føringsveier mellom Oslo, Bergen, Trondheim og Tromsø. Den overordnede arkitekturmodellen inkluderer fire datasentre, som alle er likeverdige og kan fungere som backup for hverandre. Infrastrukturen til Neste Generasjons Kjernenett vil være på plass i løpet av 2015. Deretter skal kundene fases over på det nye nettet.

Helse- og omsorgsdepartementet (HOD) har det overordnede ansvaret for at befolkningen får gode og likeverdige helse- og omsorgstjenester, og har det strategiske ansvaret for IKT-utviklingen i helse- og omsorgssektoren.[3] HOD har overordnet ansvar for informasjonssikkerhet og objektsikkerhet i helse- og omsorgssektoren og styrer de regionale helseforetakenes arbeid med beredskap og sikkerhet. HOD gir oppdrag til Helsedirektoratet angående myndighetsoppgaver knyttet til informasjonssikkerhet, og til Norsk Helsenett angående drift av HelseCSIRT (Computer Security Incident Response Team).

Helsedirektoratet er underlagt HOD og har et overordnet ansvar for at de nasjonale strategiene for elektronisk samhandling og standardisering blir fulgt opp og realisert. Ansvaret for etablering av flere nasjonale IKT-prosjekter, som nasjonalt meldingsløft, e-resept, helsenorge.no, automatisk frikort og kjernejournal, ligger også til Helsedirektoratet. Helsedirektoratet iverksetter IKT-tiltak som omfatter hele helse- og omsorgssektoren, og ivaretar en faglig og koordinerende rolle på vegne av hele sektoren overfor sektorovergripende felleskomponenter som for eksempel ID-porten.

Direktorat for e-helse opprettes 1. januar 2016 basert på divisjon e-helse i Helsedirektoratet. Direktoratet skal være fagdirektorat for Helse- og omsorgsdepartementet når det gjelder IKT-politiske spørsmål. Sentrale oppgaver vil være ledelse og styring av nasjonale oppgaver knyttet til premisser, standarder og retningslinjer innen IKT-området, herunder innspill til politikkutforming innen e-helse. Direktoratet vil også få i oppgave å utvikle, implementere og drifte nasjonale felleskomponenter.

De regionale helseforetakene (RHF) (Helse Vest, Helse Midt-Norge, Helse Nord og Helse Sør-Øst) er eid og styrt av Helse- og omsorgsdepartementet. RHF-ene styres gjennom årlig budsjettildeling over statsbudsjettet med tilhørende oppdragsbrev og har «sørge-for»-ansvar og tilretteleggingsansvar for at helseforetakene kan yte helsetjenester. I tillegg mottar RHF-ene styringsføringer fra politiske mål og strategier, også for IKT-området. Hvert av de regionale helseforetakene har etablert en felles IKT-tjenesteleverandør for sin region: Sykehuspartner (Helse Sør-Øst), Helse Vest IKT (Helse Vest), Hemit (Helse Midt-Norge) og Helse Nord IKT (Helse Nord). I en rapport fra Helsedirektoratet i 2015 fremmes en anbefaling om å etablere en helhetlig og felles nasjonal leverandørfunksjon for helse- og omsorgssektoren som kan sørge for anskaffelse, utvikling, drift og forvaltning av nasjonale fellesløsninger.[4]

[3] Meld. St. 9 (2012–2013) *Digitale tjenester i helse- og omsorgssektoren*, kap. 5, s. 43–47.

Helseforetakene (sykehusene) representerer kjerneytelsen i spesialisthelsetjenesten, som er å gi adekvat helsehjelp poliklinisk og på døgnbasis. Helseforetakene er eid av RHF-ene, men er selvstendige rettssubjekter. Innen IKT er foretakene i stadig større utstrekning avhengige av RHF-enes IKT-enheter, som beslutter innkjøp, infrastruktur og drift av IT-systemene. Dette krever dialog og rapportering mellom foretaket og IKT-selskapet.

Primærhelsetjenesten dekker kommunale helse- og omsorgstjenester, som fastlege, sykehjem, legevakt med videre. Kommunenes ansvar for helse- og omsorgstjenester omfatter pasienter med behov for sammensatte og koordinerte tjenester, noe som krever involvering og kommunikasjon med flere kommunale enheter, samt med spesialisthelsetjenesten, i forbindelse med inn- og utskriving av pasienter. Kommunale helse- og omsorgstjenester har derfor et stort behov for sikker kommunikasjon. Kommunene følger nasjonale føringer og programmer for bruk og utvikling av IKT fra KS og Helsedirektoratet.

KommIT er et program for IKT-samordning i kommunesektoren. Hver kommune forvalter sine egne IKT-kjernesystemer, men enkelte samarbeider interkommunalt. Fastlegene er en del av den kommunale helsetjenesten, og har i svært stor grad sine egne IKT-systemer med liten eller ingen integrasjon med kommunenes IKT-systemer, med unntak av meldingsutveksling ved bruk av helsenettet.

Statens helsetilsyn har, sammen med Fylkesmannen, det generelle tilsynsansvaret i helsesektoren, og fører tilsyn med utførelse av helsehjelp og med helsepersonells skikkethet. Tilsynet fører også tilsyn med helseberedskapsloven og tilsyn i forbindelse med større uønskede hendelser.

Folkehelseinstituttet (FHI) er underlagt Helse- og omsorgsdepartementet og er en nasjonal kompetanseinstitusjon for myndigheter, helsetjeneste, rettsapparat, påtalemyndighet, politikere, media og publikum. Instituttets hovedoppgaver er helseovervåking, forskning, forebyggende helsearbeid og beredskap. FHI har ansvar for 10 av 17 sentrale helseregistre. De sentrale helseregistrene brukes til landsdekkende formål knyttet til helsestatistikk, beredskap, kvalitetsforbedring av helsetjenester, forskning, administrasjon og styring.

Norsk Helsenett SF er et statsforetak som styres med oppdragsbrev fra Helse- og omsorgsdepartementet. Oppdraget er å levere og videreutvikle en sikker, robust og hensiktsmessig nasjonal IKT-infrastruktur for effektiv samhandling mellom alle aktører i helse- og omsorgstjenesten, helsenettet. Norsk Helsenett utarbeider risikovurderinger for nye eller endringer av eksisterende tjenester, og gjennomfører en rekke sårbarhetskartlegginger i egen infrastruktur. Videre har de et opplegg for monitorering av løsninger og infrastruktur, både internt og i regi av HelseCSIRT.

Nasjonal IKT er spesialisthelsetjenestens hovedarena for samhandling innen informasjons- og kommunikasjonsteknologi. Det gjelder både samhandling innad i spesialisthelsetjenesten (mellom de ulike helseforetakene og de regionale helseforetakene) og samhandling med andre sentrale aktører, som kommunehelsetjenesten, Helse- og omsorgsdepartementet, Helsedirektoratet og Norsk Helsenett.

I tillegg kommer en rekke private aktører i helsesektoren. Flere av disse er tilknyttet Norsk Helsenett og/eller kjøper driftstjenester fra eksterne leverandører. Det er fragmenterte ansvarsforhold i helse- og omsorgssektoren, med mange selvstendige aktører som ikke er underlagt direkte statlig styring, unntatt gjennom lov.

17.3 Hjemmelsgrunnlag og tilsynsvirksomhet

Helsesektoren er sterkt lovregulert med bakgrunn i de store reformene som har vært førende siden helseforetaksreformen i 1999. Sektoren styres i stor grad av rettsregler fra 2000, med hyppige endringer og nye lover frem til i dag. Sentrale lovverk for helsetjenesten omfatter både organisering, beredskap, krav til ytelse av helsehjelp, herunder krav til å dokumentere helsehjelpen for senere bruk i pasientbehandlingen og for å kunne kontrollere at den helsehjelpen som ble gitt, var forsvarlig.

For bruk av IKT som verktøy i tjenestene er de mest sentrale lovene helsepersonelloven, pasientjournalloven, pasient- og brukerrettighetsloven, helseregisterloven og personopplysningsloven.

Lov om helsemessig og sosial beredskap (helseberedskapsloven) pålegger kommuner, fylkeskommuner og regionale helseforetak å utarbeide en beredskapsplan for de helse- og omsorgstjenestene eller sosialtjenestene de skal sørge for eller er ansvarlige for å tilby. Plikt til å etablere planverk fremgår også av spesialisthelsetjenesteloven, den kommunale helse- og omsorgstjenesteloven og folkehelseloven. Planplikten i helseberedskapsloven er utdypet i forskrift nr. 881 23. juli 2001 om krav til beredskapsplanlegging og bered-

[4] Helsedirektoratet (2015): *Styrket gjennomføringsevne for IKT-utvikling i helse- og omsorgstjenesten.*

skapsarbeid. Forskriften fastsetter at virksomheten gjennom risiko- og sårbarhetsanalyser skal skaffe en oversikt over hendelser som kan føre til ekstraordinære belastninger for virksomheten, og at det på bakgrunn av avdekket risiko og sårbarhet skal utarbeides en beredskapsplan. Verken loven eller forskriften nevner ekom eller IKT eksplisitt, men det forutsettes at dette er omfattet av pålegget om risiko- og sårbarhetsanalyser.

Lov om behandlingsrettede helseregistre, pasientjournalloven, regulerer adgangen til å registrere og bruke pasientenes helseopplysninger for å yte og administrere helsehjelp. Loven forener behovene for dokumentasjon til helsehjelpsformål og ivaretakelse av pasientenes krav på personvern. Lovens § 5 viser til at personopplysningsloven supplerer pasientjournalloven. For eksempel stilles det krav til informasjonssikkerhet i personopplysningsloven kapittel 2, som gjelder frem til HOD eventuelt benytter adgangen til å gi forskrift etter § 22 i pasientjournalloven.

Lov om helseregistre og behandling av helseopplysninger, helseregisterloven, gir hjemmel for å etablere helseregistre på tre forskjellige måter. Hvilken fremgangsmåte som skal benyttes, er avhengig av pasientens mulighet til å medvirke til å la seg registrere. Registre som må opprettes ved lov, omfattes av § 11, ved forskrift §§ 8 og 9 eller ved konsesjon fra Datatilsynet § 7. Datatilsynet har gitt konsesjon til cirka 20 nasjonale sykdomsregistre. Til nå er det lovvedtak for ni ulike helseregistre,[5] og det pågår et arbeid for å etablere et nasjonalt register for primærhelsetjenesten, tilsvarende Norsk pasientregister for spesialist-helsetjenesten, som registrerer alle pasientbehandlinger ved landets sykehus. Personopplysningslovens regulering av informasjonssikkerhet gjelder for både helseregisterloven og pasientjournalloven.

Norm for informasjonssikkerhet i helse- og omsorgstjenesten, heretter kalt Normen, er utarbeidet av aktørene i sektoren med sikte på å sørge for implementering av rettslige krav til informasjonssikkerhet i den enkelte virksomhet og i sektoren generelt. Dette skal bidra til å etablere gjensidig tillit til at samtlige virksomheter behandler helse- og personopplysninger på et forsvarlig sikkerhetsnivå. Normen omsetter lovkravene til behandling av helseopplysninger til praktiserbare funksjonelle krav som skal sikre gjennomføring i IKT-systemene.

Normen er i samsvar med bestemmelser som omhandler konfidensialitet, opplysningsplikt, dokumentasjonsplikt, pasientenes rett til innsyn, med videre. Videre omfattes virksomhetenes systemansvar, som skal sikre at helsepersonell kan ivareta sine lovpålagte plikter, herunder taushetsplikten. Ved eventuell motstrid mellom Normen og de til enhver tid gjeldende lover eller forskrifter vil lov og forskrift gå foran Normen.

Tilsyn

Det finnes ikke et eget sektortilsyn for informasjonssikkerhet på helseområdet. Helsetilsynet har som tidligere beskrevet det generelle tilsynsansvaret i sektoren. De fører også tilsyn med helseberedskapsloven og utfører tilsyn i forbindelse med større uønskede hendelser. Datatilsynet som generell tilsynsmyndighet fører tilsyn med at behandlingen av helseopplysninger er i samsvar med regelverket i både pasientjournalloven, helseregisterloven og personopplysningsloven. For to av de lovregulerte helseregistrene, Norsk pasientregister og Hjerte- og karregisteret, fører Datatilsynet forsterket tilsyn. Det innebærer årlig rapportering fra registrene med oppfølging fra tilsynet. For medisinsk utstyr, elektromedisinsk utstyr inkludert, er tilsynsansvaret delt mellom Statens helsetilsyn / Fylkesmannen, Helsedirektoratet og Direktoratet for samfunnssikkerhet og beredskap – dels for ulike typer helseinstitusjoner og dels ut fra type medisinsk utstyr.

17.4 Beredskap og hendelseshåndtering

De overordnede kravene til beredskap for kommuner, fylkeskommuner og regionale helseforetak går frem av flere regelverk, som beskrevet i punkt 17.3 «Hjemmelsgrunnlag og tilsynsvirksomhet». Nasjonal helseberedskapsplan er et nasjonalt rammeverk for helsesektorens beredskap. Planen beskriver lov- og plangrunnlag, aktørene i helseberedskapen og deres rolle, ansvar, oppgaver og ressurser når det gjelder forebygging, beredskapsplanlegging, kriser og katastrofer, og utgjør grunnlaget for helsesektorens håndtering av alle typer kriser og katastrofer.[6]

[5] De ni registrene som er opprettet i medhold av lov, er: Dødsårsaksregisteret, Medisinsk fødselsregister, Kreftregisteret, Meldingssystem for smittsomme sykdommer, System for vaksinasjonskontroll, Forsvarets helseregister, Norsk pasientregister, Nasjonalt register over hjerte- og karlidelser og System for bivirkningsrapportering.

[6] Helse- og omsorgsdepartementet (2014): *Nasjonal helseberedskapsplan*. Versjon 2.0.

Helse- og omsorgsdepartementet oppgir at IKT-hendelser var tema under Øvelse Østlandet 2013, der all infrastruktur ble utilgjengelig. Norsk Helsenett har også gjennomført flere øvelser.

Mange hendelser inntreffer som følge av manglende opplæring, holdninger og årvåkenhet. Det øves på nedetid av IKT-systemer, men som oftest ikke på redusert bemanning. Det er uttrykt at det trengs beredskapsplaner og øvelser med tanke på situasjoner der blant annet journalsystemer er ute av funksjon. Ifølge Norsk Helsenett anses nedetid på IKT-systemer ofte som mindre kritisk enn evnen til å yte helsehjelp i sektoren, noe som ofte gjenspeiles i beredskapsplanene. Ifølge Norsk Helsenett er dette et område som antas å få større oppmerksomhet i årene som kommer. Flere av de regionale driftsleverandørene har rapportert om IKT-hendelser som har medført utilgjengelighet i IKT-systemene og dermed redusert kapasitet til pasientbehandling i kortere perioder. Lav grad av standardisering og stor grad av arv av systemer medfører blant annet lang responstid når hendelser inntreffer.

HelseCSIRT[7] ble etablert i 2011 og driftes av Norsk Helsenett. HelseCSIRT er helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet. Senteret kan brukes av hele sektoren, og bistår blant annet de regionale helseforetakene ved IKT-hendelser. HelseCSIRT skal bidra til økt kompetanse om IKT-trusler og beskyttelsesmekanismer og kontinuerlig holde øye med trafikken i helsenettet. Målet er å forebygge, avdekke og håndtere trusler mot sikkerheten. Senteret er et viktig verktøy for å ivareta informasjonssikkerheten og kartlegge sårbare systemer i sektoren. Støtten HelseCSIRT gir de regionale helseforetakene og driftsleverandørene, blir betraktet som svært nyttig av sektoren. Det er likevel avgjørende for en effektiv håndtering at det er tilstrekkelig sikkerhetskompetanse til stede lokalt.

HelseCSIRT har et eget sensornettverk, Nasjonalt beskyttelsesprogram for helse- og omsorgssektoren (NBP). NBP består av sensorer plassert i helsenettet som oppdager uønskede hendelser og uønsket trafikk ved at all trafikk skannes i sanntid. Det er etablert varslingsrutiner for å informere deltagerne i beskyttelsesprogrammet om hendelser, trusler og sårbarheter. Per 1. oktober 2015 var det utplassert 26 sensorer på sentrale steder i helsenettet.

HelseCSIRT er tilknyttet Varslingssystem for digital infrastruktur (VDI), og samarbeider med NSM NorCERT og øvrige sektorvise CERT-er i Norge. Norsk Helsenett har et forpliktende samarbeid med alle aktører som er tilknyttet helsenettet, og gjennom Nasjonalt beskyttelsesprogram (NBP).

Det finnes ingen rapporteringsplikt om IKT-hendelser i helsesektoren. De regionale helse-

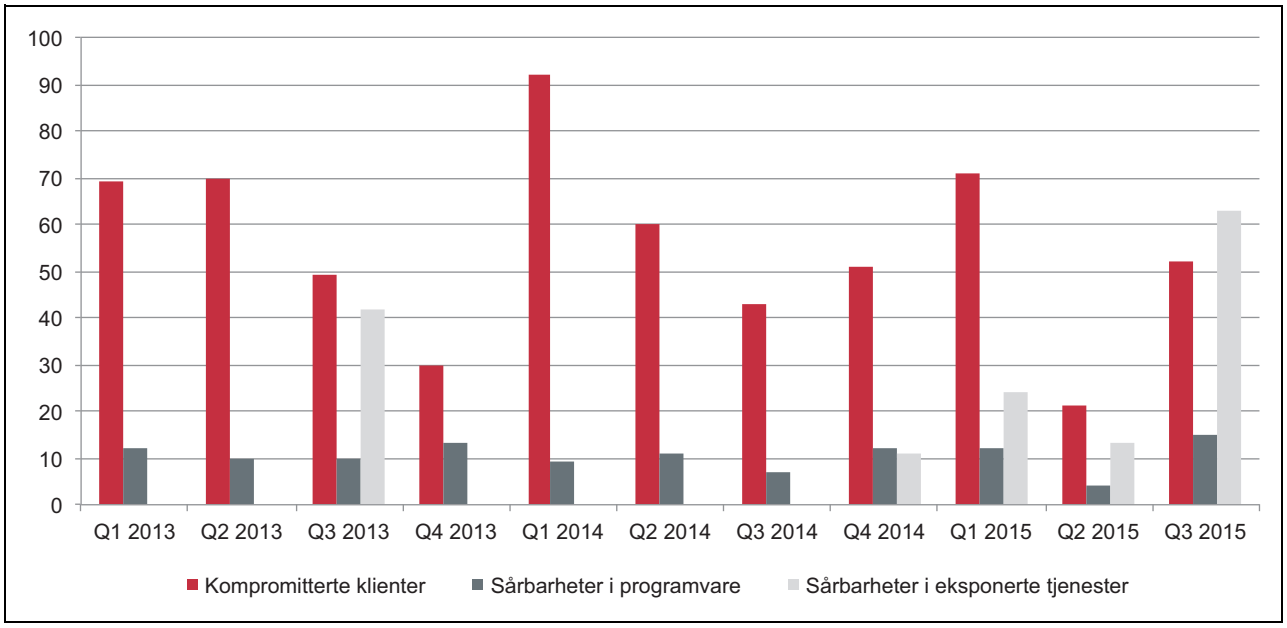
[7] I forslag til statsbudsjett for 2016 har HOD foreslått at HelseCSIRT skal gå over til en fullverdig CERT. HelseCSIRT har vært godkjent for det i tre år allerede. Uttrykket HelseCERT vil dermed kunne benyttes fremover.

Boks 17.2 Økende utfordringer knyttet til løsepengevirus i helsesektoren

I helsesektoren har det vært hendelser knyttet til løsepengevirus som krypterer filene lokalt og på nettverksområder som det får tilgang til, og der trusselutøveren i etterkant krever bitcoins som løsepenger for å dekryptere filene. Helse Sør-Øst har opplevd til dels alvorlige hendelser der flere hundre tusen filer har blitt kryptert i én og samme infeksjon. Dette har medført at dokumenter, databaser eller andre filer på delte filområder har blitt uleselige, og at personell som har blitt rammet av dette – noen ganger i flere timer – ikke får tilgang til ressurser for å utføre arbeidsoppgavene sine. Ved et annet tilfelle ble et registreringssystem tilknyttet sykehusets blodbank rammet.

Konsekvensen av løsepengevirusene i Helse Sør-Øst har i betydelig grad blitt mitigert av gode manuelle rutiner for kontinuerlig drift, mens det på teknisk nivå har vært implementert god enterprise-backup. Likevel har angrep ført til at produksjon i forskjellige deler av helseforetaket midlertidig har stoppet opp, frem til filområdene som er blitt kryptert, er blitt gjenopprettet fra frisk backup. Filer som har blitt opprettet eller endret i tidspunktet mellom siste backup og kompromittering fra løsepengeviruset, har måttet gjenopprettes manuelt.

Ingen av løsepengevirusene ved Helse Sør-Øst har medført noen direkte fare for liv eller helse. Likevel har løsepengevirusene i stor grad vist hvor viktig det er med sikkerhetskontroller som sikkerhetsoppgraderinger, beskyttelse mot ondsinnet kode, logganalyse og deteksjon, og hvilket skadepotensiale mer destruktive ondsinnede virus kan ha innenfor sektoren.



Figur 17.3 Hendelser og sårbarheter varslet fra HelseCSIRT.

Kilde: Norsk Helsenett.

foretakene rapporterer inn til HelseCSIRT ved behov for støtte, men det er ingen fast sentral rapportering. Etter HelseCSIRTs mening er det behov for tydeligere krav til rapportering. Figur 17.3 viser statistikk fra HelseCSIRT knyttet til hendelser og sårbarheter de har registrert og varslet sektoren om.

Kompromitterte klienter er klienter der HelseCSIRT med sikkerhet vet at det er kjørt ondsinnet kode og klienten kommuniserer eller forsøker å kommunisere med en ekstern maskin. Dette tallet viser hvor mange varsler som er sendt ut til aktører som er innrullert i Nasjonalt beskyttelsesprogram angående slike hendelser. Klienter som mistenkes å være kompromittert, men der HelseCSIRT ikke kan bekrefte det med 100 prosent sikkerhet, er ikke med i statistikken. *Sårbarheter i programvare* omfatter antall varsler HelseCSIRT har sendt ut angående sårbarheter i programvare som er utbredt i sektoren. Et slikt varsel kan inneholde varsler om mange sårbarheter i forskjellige typer programvare. *Varsler om sårbarheter i eksponerte tjenester* refererer til antall sårbare tjenester HelseCSIRT har oppdaget i sektoren. Flere sårbarheter i én tjeneste teller som én. Et varsel vil typisk inneholde varsel om flere sårbare tjenester.

Norsk Helsenett etablerte høsten 2015 et nasjonalt kompetanseforum for å dele kompetanse og erfaringer på tvers av regioner. HelseCSIRT vil fungere som fasilitator for denne møtearenaen. I tillegg finnes det ulike regionale samarbeidsstrukturer innen informasjonssikkerhet og beredskap.

17.5 Digitale sårbarheter i helsesektoren

Det er mange avhengigheter mellom aktørene i helsesektoren. Sentrale utfordringer er tilgjengelighet av IKT-systemer og beredskap mot nedetid. Helsevesenet har så små marginer at liv kan gå tapt som følge av bortfall av IKT. Det finnes visse manuelle rutiner og muligheter for utskrifter på papir som gjør at sykehusene kan opprettholde driften noen timer, men ikke dager. Sektoren består av mange selvstendige aktører og systemer og lite teknisk integrasjon.

Medisinsk-teknisk utstyr er på vei inn i private hjem, og påliteligheten til dette utstyret kan variere. Fremover vil private hjem i større grad være behandlingsstedet, og dette innebærer nye sårbarheter. Infrastrukturen er privateid og kanskje delt med mange private og offentlige aktører, eksempelvis leverandører av helsetjenester, vaktselskaper, strømleverandører med flere. Dette gir et uoversiktlig bilde med mange ulike tjenesteleverandører, i tillegg til data som skal integreres og lagres. Økt bruk av privat utstyr for medisinsk personell og pasienter er én problemstilling, konsekvensene av «det utvidede legekontoret» som blir brakt hjem til folk, en annen.

17.5.1 Avhengighet av elektronisk kommunikasjon og øvrige infrastrukturer

Helsesektoren er svært sårbar for bortfall av elektronisk kommunikasjon (ekom), energi og vannforsyning. Avhengigheten av vann og avløp er stor, og sykehus må stenge etter få timer om dette bortfaller. Tilgjengelig ekom er nødvendig for de fleste tjenestene og fremheves som en av de største sårbarhetene. Nødvendige kommunikasjonskanaler for å tilkalle helsepersonell, kommunikasjon mellom sykehusene og mellom sykehus og fastleger vil stoppe opp. I de fleste tilfeller er for eksempel tilgang til pasientjournaler avhengig av fungerende IKT-systemer. Uten pasientjournaler vil det være svært vanskelig å opprettholde en forsvarlig drift. Akuttfunksjonene vil imidlertid kunne fortsette å behandle pasienter selv om den digitale samhandlingen opphører.

I DSBs nasjonale risikobilde for 2014 synliggjøres det hvilke konsekvenser for liv og helse det vil ha dersom ekomtjenester skulle falle bort i fem døgn. Det anslås blant annet at 50 flere enn normalt vil dø som følge av at det ikke er mulig å ringe etter ambulanse og varsle nødetatene ved akutte hendelser. I tillegg regner man med 200–300 alvorlige skadde og syke som følge av utsatt behandling eller feilbehandling. Det er imidlertid stor usikkerhet knyttet til anslagene, ettersom sektoren hittil ikke har erfart slike langvarige bortfall. Bortfall av ekom vil også kunne medføre mangelfull kommunikasjon og koordinering mellom nødetatene, ettersom Nødnett bare fungerer lokalt. For nærmere omtale av Nødnett, se kapittel 20 «Styring og kriseledelse».

Digitale kjølesystemer er viktig for drift av sykehus. Slike systemer styres over nettet og er dermed sårbare for angrep og hendelser. Dersom man mister evnen til å kontrollere temperaturen i et sykehus, vil det gå ut over evnen til å behandle pasienter.

Helse- og omsorgsdepartementet understreket i etterkant av Riksrevisjonens rapport at det skal foreligge konkrete beredskapsplaner for bortfall av IKT, vann og strøm i alle helseforetakene. Planene skal testes ved reelle hendelser, og også inngå i regionale og nasjonale fellesøvelser. I tillegg må beredskapsplanene ta høyde for ekstreme hendelser eller hendelser som oppstår svært sjelden.[8]

Boks 17.3 Massiv IKT-svikt ved Ahus

I juni 2011 førte en feil i en svitsj til at hele Akershus universitetssykehus (Ahus) var uten telefoni- og datatilgang i 14 timer før feilen ble rettet. All telefoni på sykehuset er IP-basert og falt dermed ut – både internt og eksternt – siden både telefoni og data ligger på samme fysiske WLAN-løsning. De ansatte kunne benytte private mobiltelefoner, men alle relevante telefonnumre lå på et ikke-fungerende datasystem. Det gjorde også kriseplanen, som det ikke fantes papirkopi av. Også laboratorietjenester, medisin- og journaltilganger ble rammet, da tilgang til disse tjenestene er avhengig av samme IKT-system. Konsekvensen av hendelsen var blant annet at det tok fire og en halv time å hente ut medisiner til pasientene, og at journaler måtte skrives ut ved å koble en printer rett på en server, noe som også tok lang tid. Mellom 10 og 20 pasienter måtte overføres til andre sykehus, og det var ikke mulig å ta inn nye akuttpasienter. Hendelsen fikk ingen direkte konsekvenser for liv og helse.

Boks 17.4 Tidligere påpekte mangler

I selskapskontrollen for 2013 påpekte Riksrevisjonen følgende mangler ved helseforetakenes beredskap innen IKT, vann og strøm:[1]

- Helseforetakene mangler eller har mangelfulle risiko- og sårbarhetsanalyser og beredskapsplaner for IKT, vann og strøm.
- Helseforetakene gjennomfører få øvelser i forbindelse med innsatsfaktorene vann, strøm og IKT.
- Ledelsen i helseforetakene følger i liten grad opp beredskapsarbeidet.
- Helse- og omsorgsdepartementet og de regionale helseforetakene har lagt til rette for beredskapsarbeidet, men oppfølgingen har vært svak.

[1] Riksrevisjonen (2014): *Riksrevisjonens kontroll med forvaltningen av statlige selskaper for 2013*, Dokument 3:2 (2014–2015).

[8] Riksrevisjonen (2014): *Riksrevisjonens kontroll med forvaltningen av statlige selskaper for 2013*, Dokument 3:2 (2014-2015).

17.5.2 Infrastruktur og tjenester

Det gjennomføres sikkerhetstesting i helsenettet for å avdekke eventuelle svakheter i infrastrukturen. I 2013 gjennomførte Norsk Helsenett 19 sikkerhetsrevisjoner fordelt på 13 kommuner, to helseforetak og fire tredjepartsleverandører. Ifølge Norsk Helsenett har disse testene gitt gode resultater, og påviste avvik er lukket.

Det ligger en generell sårbarhet i IKT-tjenester som ikke er høytilgjengelige, og som kjører fra kun én bestemt geografisk lokasjon. Dette medfører at tjenestene kan bli utilgjengelige i enkelte landsdeler, og at tjenestene som sådanne kan bli redusert eller lammet på grunn av infrastruktursvikt som følge av ulykker, ekstremvær eller andre utilsiktede hendelser. Flere av disse tjenestene mangler i dag automatiske og velprøvde muligheter for reservelegging og parallelldrift. Som beskrevet i punkt 17.1 «Infrastruktur» er det satt i gang et arbeid med et nytt høytilgjengelig høykapasitetsnett. Det strategiske målet er at kjernetjenestene – fra et brukerståsted – skal være 100 prosent tilgjengelige, gitt at brukeren har kontakt med helsenettet.

Ifølge Norsk Helsenett fremstår tilknytningsløsningene til helsenettet, spesielt for mindre organisasjoner som legekontorer, tannlegekontorer og mindre kommuner, som uhensiktsmessige og unødig kostbare. De har derfor utviklet en enklere, men like sikker, tilknytning til helsenettet som gir kundene større frihet i valg av nettleverandør.

Erfaring viser at IKT-utstyr i sektoren ofte er utenfor support og ikke lar seg oppdatere. Utfasing og sanering av systemer kan være krevende. I tillegg påpekes det som en sårbarhet at oppdateringer tar tid, siden disse må testes på infrastrukturen først. Et stort antall eldre IKT-systemer i sektoren er utviklet uten evne til å beskytte seg mot trusler fra nettet, direkte eller indirekte, og utgjør dermed en sikkerhetsrisiko. Dette krever særskilte sikringstiltak som gjerne øker kompleksiteten i totalsystemet, noe som igjen bidrar til å gjøre systemene mindre pålitelige og robuste. I flere risikovurderinger fra helseforetakene fremgår det at det er et høyt antall kritiske feil i flere IKT-applikasjoner.

Stor grad av variasjon i tekniske løsninger medfører utfordringer for meldingsutveksling mellom helseforetakene og primærhelsetjenesten. Dette er også tidligere påpekt av Riksrevisjonen.

Helsetilsynet kjenner til eksempler på at henvisninger og prøvesvar er blitt borte, noe som kan forårsake forsinket diagnostisering av alvorlige tilstander. Svikt i elektroniske systemer og/eller menneskelige feil er påpekt som mulige årsaker. Helsetilsynet har sammenlignet arbeidsmetodene i Norge med måten svenske myndigheter analyserer sine situasjoner på. Det går frem av sammenligningen at den svenske havarikommisjonen blant annet legger større vekt på å «avdekke mulig svikt i teknisk utstyr som kan ha hatt betydning for hendelsen, enn det som er praksis i Norge».[9]

Elektronisk pasientjournal (EPJ) er avhengig av kommunikasjon mellom mange systemer og omfatter pasientinformasjon som for eksempel røntgenbilder, laboratoriesvar og annen pasientdokumentasjon. Alle landets sykehus og de fleste allmennleger har installert EPJ-systemer, og det foregår en gradvis overgang fra papirjournaler til elektronisk lagrede journaler. Det er ikke entydig om man for eksempel i forbindelse med fritt sykehusvalg på en enkel måte eller automatisk kan ta med egne data fra ett sykehus til et annet.

I Meld. St. 9 (2012–2013) *Én innbygger – én journal* påpekes det blant annet at de teknologiske mulighetene elektronisk pasientjournal gir, ikke blir utnyttet. Dette begrunnes blant annet med at det er mange selvstendige aktører og mange systemer. Det pågår et omfattende arbeid som følge av denne stortingsmeldingen, og det foreligger ulike konsepter. Valget av konsept vil skje i løpet av 2015.

Hensiktsmessig tilgangsstyring og sporing av brudd på taushetsplikt er utfordrende. Riksrevisjonen har påpekt følgende: «Ansatte i helseforetak har tilgang til helseopplysninger utover tjenestebehov, og kontrollen av tilganger til elektronisk pasientjournal er mangelfull.» Én av årsakene som oppgis, er at helseforetakene ikke i tilstrekkelig grad har implementert gjeldende regelverk om informasjonssikkerhet og behandling av helseopplysninger.[10] Det pågår imidlertid et systematisk arbeid i de regionale helseforetakene for å rette opp dette. Samtidig må det erkjennes at dette er et vanskelig område fordi det er svært mange ulike systemer med innbyrdes ulike oppsett.

---

9 Helsetilsynet (2015): Med *tilsynsblikk på alvorlige og uventede hendelser i spesialisthelsetjenesten. Status og erfaringer 2014 fra Undersøkelsesenheten i Statens helsetilsyn.*

10 Riksrevisjonen (2014): *Riksrevisjonens kontroll med forvaltningen av statlige selskaper for 2013*, Dokument 3:2 (2014-2015).

Boks 17.5 Digitale sårbarheter på tvers av sektorer og bransjer

Vi omgir oss med elektronikk, digitaliserte styringssystemer og apper. Store internasjonale selskaper leverer industrikontrollsystemer og medisinsk-teknisk utstyr til en rekke bransjer globalt, inklusiv norske virksomheter. Forskning har vist at samme type sårbarheter går igjen i industrikontrollsystemer og i medisinsk-teknisk utstyr på tvers av bransjer.

Forskerne testet blant annet røntgenmaskiner ved hjelp av fuzzing[1] og sjekket ut en app som leger kan bruke for å overvåke pasienter. Appen viste seg å dele en konto på App Store, noe som viser at det ikke har vært tenkt mye på sikkerhet, mens det medisinsk-tekniske utstyret hadde innebygde hardkodede passord som representerte sårbarheter. Slike innebygde passord i programvare blir brukt til intern eller ekstern autentisering av enheter og programmer og representerer digitale sårbarheter som kan utnyttes. Hardkodede passord er vanskelige å oppdage av systemadministratorer og vanskelige å rette opp hvis de blir oppdaget.[2] Sårbarhetene viste seg i produkter som benyttes til operasjoner, anestesi, ventilatorer, medisinpumper, pasientovervåking, laboratorieanalyse og hjertestartere. Totalt gjaldt dette 300 medisinske enheter og 40 leverandører.

[1] En testteknikk innenfor programvareutvikling.
[2] CWE-259: Use of Hard-coded Password.

17.5.3 Styring og samhandling

Erfaring viser at mange uønskede IKT-hendelser i helsesektoren skyldes underleverandører, blant annet feil på strømleveranse og brudd på kommunikasjonslinjer. Tre av de regionale helseforetakene har rapportert til Lysneutvalget at henholdsvis 17–20 prosent, 26 prosent og 50 prosent av hendelsene skyldes svikt hos underleverandører. Ett av helseforetakene oppgir at de ikke har oversikt over dette. Norsk Helsenett anslår at omkring 80 prosent av større uønskede IKT-hendelser innenfor deres ansvarsområde er forårsaket av underleverandører. En stor andel av disse skyldes kommunikasjonsbrudd som har rammet større eller mindre grupper av kundene.

Flere av de samme utfordringene kommer også til uttrykk i en rapport fra Gartner i 2014, der det konkluderes med at norske og nordiske IKT-leverandører ikke leverer den funksjonaliteten som er påkrevd.[11] Det er store forskjeller mellom de regionale helseforetakene med hensyn til løsninger og valg av teknologi, og det er ingen felles prosess for samordning av krav til leverandører. Helsedirektoratet har imidlertid i en rapport fra 2015 foreslått en rekke virkemidler for å styrke gjennomføringsevnen for IKT-utvikling i helse- og omsorgssektoren og for å redusere disse sårbarhetene.[12]

Kommunene i samspill med leverandører og sektoren. Manglende virksomhetsstyring når det gjelder digitalisering og IKT-utvikling, vil kunne medføre «skygge-IKT», det vil si IKT-prosjekter som etableres med manglende kontroll i virksomhetene. Ifølge Ikomm er det vanskelig å finne gode digitaliseringsstrategier både i kommunene og i helse- og omsorgssektoren for øvrig. Manglende digitalisering kan også i mange tilfeller være en digital sårbarhet – for eksempel ved at det blir innført elektroniske verktøy uten at arbeidsprosesser endres eller gevinstene ved investeringen hentes ut. En uheldig konsekvens av manglende digitalisering og manglende utnyttelse av digitale verktøy kan være svekket pasientsikkerhet.

Helsepersonell har et stort behov for effektive og funksjonelle IKT-systemer, noe som er uttrykt i flere rapporter. Flere av dagens systemer er tungvinte for brukerne, for eksempel ved at de har lang innloggingstid og lite strukturerte pasientjournaler. En suksesshistorie som skiller seg ut med hensyn til involvering av helsepersonell i utviklingsarbeidet, er innføringen av e-resept og utarbeidelsen av Norm for informasjonssikkerhet. Norm for informasjonssikkerhet blir i hovedsak ansett som et godt tiltak for sektoren. Likevel oppleves enkelte forslag til tiltak som utdaterte, og det etterlyses mer konkrete forslag til hvordan man skal forholde seg til IKT-sikkerhet. For de minste helseforetakene oppleves normen som for omfattende, noe som medfører at de ikke har ressurser til å følge den opp.

Helsesektoren er gjenstand for et stort antall revisjoner og utredningsarbeider. Flere har

[11] Gartner (2014): *Gartner survey of EHR suppliers and systems in the Norwegian market.*
[12] Helsedirektoratet (2015): *Styrket gjennomføringsevne for IKT-utvikling i helse- og omsorgstjenesten.*

uttrykt bekymring over all tiden som går med til å svare på henvendelser, noe som fører til økt sårbarhet for personellet, ettersom mindre tid benyttes direkte til primæroppgavene, nemlig å yte helsehjelp.

Flere aktører etterlyser en sterkere styring fra Helse- og omsorgsdepartementet når det gjelder digitalisering av helsesektoren. Aktørene er videre bekymret for at informasjon fra HOD og Helsedirektoratet ofte ikke når frem til de relevante miljøene i helseforetakene, eller at informasjonen kommer for sent frem til at man rekker å svare på den.

I alle sektorer finnes kommunikasjonsutfordringer mellom IKT-ansvarlig personell og personell som er ansvarlig for sektorens primæroppgaver. Innen helsesektoren er dette spesielt fremhevet. Uheldige beslutninger som følge av manglende forståelse for hverandres ansvarsområde og arbeidshverdag er påpekt av flere aktører i sektoren.

Det kommer også frem at det er utfordringer knyttet til kommunikasjon med andre helseaktører, for eksempel når det gjelder utvikling og bruk av fellesløsninger, elektronisk meldingsutveksling, tilgangsstyring og så videre. I tillegg klarer ikke de tekniske systemene å ivareta de kravene lovene stiller til behandling av helseopplysninger, i tilstrekkelig grad.

17.5.4 Kompetanseutfordringer når det gjelder IKT-sikkerhet

Behovet for opplæring anses som viktig, da det er mye turnover i sektoren. Det har blitt nevnt at helsepersonell sliter med å forstå systemer, blant annet på grunn av økende kompleksitet. Som et eksempel nevnes utfordringer ved at brukerne ikke forstår konsekvenser av handlinger med bruk av verktøy. Ulik bruk av verktøy medfører varierende datakvalitet.

Norsk Helsenett har uttrykt at nærheten til teknologimiljøet i Oslo og Tromsø, og i Trondheim spesielt, har vært avgjørende for å rekruttere og beholde teknisk sikkerhetskompetanse i organisasjonen, inkludert HelseCSIRT. Høy kompetanse, både på overordnet og detaljert teknisk nivå, er svært kritisk for evnen til å forebygge og håndtere uønskede IKT-hendelser. Som andre sektorer rapporterer enkelte av de regionale helseforetakene at det er utfordringer med rekruttering av IKT-sikkerhetskompetanse, og at kompetansebehovet stadig øker.

Som nevnt i blant annet kapittel 15 «Vannforsyning» og 20 «Styring og kriseledelse» er det en betydelig svikt i sikkerhetskunnskap i kommunene. Et eksempel er en dagsaktuell sak knyttet til at en eksisterende PKI-leverandør endret rot-sertifikatet sitt, noe som satte et stort antall legekontorer ut av spill, da de ikke var i stand til å oppdatere dette hos seg selv.

Få akademiske miljøer i Norge forsker på IKT i helsesektoren (helseinformatikk). Samtidig er det i liten grad forskning på konsekvensene av de IKT-tiltakene som innføres, og store IKT-prosjekter blir i liten grad evaluert. Det er uttrykt et behov for en mer akademisk tilnærming til helseinformatikk, i tillegg til at det trengs mer forskning på dataflyt, dataeierskap og tilgangsstyring. Det blir etterlyst en tettere involvering av helsepersonell, slik at de som har forståelse for arbeidsprosesser, strukturering av informasjon, og så videre, inkluderes.

Små og mellomstore private helseforetak har ofte begrensede ressurser til IKT-drift, og mange har lagt for liten vekt på å utarbeide og implementere styringssystemer for informasjonssikkerhet. Mange mindre helsevirksomheter har servere stående i eget hus, og de mangler ofte gode backup-rutiner. De er også svært sårbare når det gjelder kompetanse i egen IKT-drift. Ikomm mener det er behov for at systemeierne og virksomhetsledelsen i større grad tar grep om informasjonssikkerhet og digitalisering i egen virksomhet og ikke lar dette være opp til IKT-ansvarlig eller systemansvarlig å håndtere.

En mulig sårbarhet som kan oppstå, er at klinisk skjønn «digitaliseres bort» som følge av heldigitaliserte helsesystemer (for eksempel strukturerte pasientjournaler). At all informasjon er tilgjengelig ved hjelp av noen få tastetrykk, vil kunne medføre at den diagnostiske, analytiske kompetansen som leger i dag bygger opp, blir borte. Risikoen for at utredningen av pasienter ikke blir god nok fordi pasienten ikke passer inn i en standard sjekkliste, kan oppstå. På den annen side kan innebygget sikkerhet, det vil si at datasystemene «spør mer» og kontrollerer at tiltak er gjennomført, være en støtte for forsvarlig pasientbehandling.

17.5.5 Særskilte personvernutfordringer

Helsesektoren er av åpenbare grunner avhengig av å benytte helserelaterte personopplysninger når de yter helsehjelp til pasienter. I dag er de fleste pasientjournaler elektroniske. Helseopplysninger er juridisk klassifisert som sensitive personopplysninger, jf. personopplysningsloven § 2. Styring av hvilket personell som skal ha tilgang til

opplysningene, er et viktig tiltak for å beskytte pasientenes helseopplysninger mot innsyn fra personell som ikke har tjenestebehov for opplysningene.

Mangelfull styring av tilgang er en problemstilling som sist ble påpekt av Riksrevisjonen i 2013, og som tidligere er påpekt i forbindelse med Datatilsynets kontroll av flere sykehus i 2008. Det er imidlertid viktig å bemerke at etablering av en forsvarlig tilgangsstyring i sykehusene er spesielt krevende, selv om det ikke kan frita for å etablere tilgangsstyring i samsvar med lovgiverens krav. I korthet omfatter kravene respekt for at pasienten i fortrolighet må formidle nødvendige opplysninger til behandlende helsepersonell for å kunne få helsehjelp, og respekt for helsepersonells taushetsplikt.

Kontroll i ettertid av logger som viser hvordan helsepersonell aksesserer personopplysninger, kan ha preventiv effekt, men kan ikke veie opp for manglende forebyggende tiltak i form av bedre styring med tilgangskontrollen.

Samhandlingsreformen og planen om å realisere «én innbygger – én journal» gjør at den enkelte pasients opplysninger blir tilgjengelige for flere grupper av helsepersonell. En betydelig utvidelse av grupper av helsepersonell som skal ha tilgang til pasientjournaler, understreker viktigheten av en forsvarlig tilgangsstyring som er i samsvar med helsepersonells taushetsplikt, og som tar vare på tillitsforholdet mellom pasient og behandler.

Det er flere nasjonale helseregistre som er basert på helsepersonells plikt til å rapportere helseopplysninger fra en pasients journal. Helseregistrene benyttes for sekundære formål, for eksempel til forskning og styring av helsesektoren. Når det ikke skal ytes helsehjelp, er behovet for å kunne identifisere den enkelte pasient annerledes enn i en helsehjelpssituasjon. I helseregistrene er det fullt mulig å beskytte pasientenes identitet ved hjelp av ulike former for anonymisering, men dette er i liten grad sørget for.[13] At det overveiende flertallet av helseregistre som ikke er knyttet til konkret pasientbehandling, er basert på full identifikasjon av den enkelte pasient, kan se ut til å stride mot det som anses nødvendig. Det skal likevel fremheves at et av de store registrene, Norsk pasientregister, har etablert en forsvarlig forvaltning av pasientenes identitet, der denne behandles både teknisk og fysisk isolert fra helseopplysningene.

Personvernkommisjonen viet helsesektoren mye oppmerksomhet og foreslo et moratorium for opprettelse av nye helseregistre frem til de eksisterende registrene var gjennomgått og utredet. Kommisjonen anbefalte å vurdere pseudonymisering av pasientenes identitet i registrene.[14] Kommisjonens forslag er ikke tatt til følge, og det er opprettet ytterligere nasjonale helseregistre. Et nytt nasjonalt helseregister over alle pasienter i primærhelsetjenesten er nå under utvikling. Dermed er enhver medisinsk konsultasjon og behandling av den enkelte pasient i befolkningen kartlagt. Summen av helseopplysninger om befolkningen fra fødsel til død blir dermed altomfattende, og ethvert sykdomsforløp hos enhver pasient kan spores i registrene.

Høsten 2013 gjennomførte Datatilsynet 15 brevkontroller av fastleger, spesialister og helseforetak som utleverer helseopplysninger til de sentrale helseregistrene. En forutsetning for pasientenes mulighet til å ivareta sitt personvern er at de blir informert om at helseopplysningene om dem videreformidles slik regelverket krever. Kontrollene viste at pasienten generelt ikke blir informert om at helseopplysninger blir utlevert til sentrale helseregistre som for eksempel Norsk pasientregister og Kreftregisteret.

En særskilt problemstilling innen helsesektoren er den teknologiske muligheten som foreligger til å lagre hele gensekvensen til enkeltindivider. Når dette skrives er det begrenset hvilke egenskaper ved personen det er mulig å lese ut fra en slik sekvens. Likevel foregår det en betydelig utvikling på dette området, og man bør utvise varsomhet når det gjelder tillatelse til innsamling, lagring og bruk av slikt materiale. Det er anerkjent at dette er spesielt sensitiv informasjon, og at den derfor må forvaltes slik at den ikke blir misbrukt. Vi har idag et strengt regelverk for bruk av genetiske analyser til behandlingsformål i helsetjenesten,[15] og utredningen av et nytt regelverk pågår. Bruk av biologisk materiale har skapt internasjonale debatter, og det er vedtatt konvensjoner[16] som også Norge har forpliktet seg til å følge.

Utfordringer knyttet til velferdsteknologi i en personvernkontekst

Velferdsteknologi kan være inngripende overfor enkeltindividet ettersom teknologien kan inne-

[13] NOU 2009: 1 *Individ og integritet – Personvern i det digitale samfunnet.*

[14] Ibid.

[15] Lov om humanmedisinsk bruk av bioteknologi -2003-12-05-100.

[16] Oviedokonvensjonen og Helsinkideklarasjonen.

Boks 17.6 GE-sakene

I Personvernnemdas årsmelding fra 2013 går det frem at mange av de sakene som har vært prinsipielle, angår helsesektoren. Et eksempel fra 2013 er de såkalte GE-sakene, der situasjonen var at en type medisinsk utstyr som flere sykehus benyttet til diagnostisering av pasienter, var tilknyttet nettet. Gjennom nettet kunne GE i USA, som drev service på maskinen, hente ut norske personopplysninger. Det at maskiner er tilknyttet nettet på denne måten, vil antagelig bli mer vanlig fremover. Det var ingen som var klar over at personopplysningene ble sendt til USA, det skjedde automatisk. Da GE selv oppdaget overføringene, ble de norske sykehusene orientert, og spørsmålet var da om man skulle orientere pasientene om hva som hadde skjedd, eller ikke. Datatilsynet fattet vedtak om at de berørte pasientene skulle informeres om hendelsen. Flere av sykehusene ønsket ikke dette og klaget saken inn for avgjørelse i Personvernnemnda. Nemndas flertall konkluderte med at det forelå rettslig grunnlag for å pålegge sykehuset en informasjonsplikt. Rettslig sett var situasjonen at det ville foreligget en informasjonsplikt overfor pasientene dersom sykehuset på forhånd hadde vært klar over at dataene ville bli overført til USA, og det ville være en lite balansert situasjon dersom en tilsvarende informasjonsplikt ikke forelå når overføringen skjedde i strid med avtale med sykehuset. Et av hovedprinsippene innen personvern er retten til å kontrollere opplysninger om seg selv, og hvis det ikke er mulig, vite hvordan opplysninger om en selv blir behandlet. Nemnda antok at den teknologiske utviklingen gjør at lignende situasjoner kan tenkes å oppstå på flere samfunnsområder fremover, og at saken kan få betydning også for disse.

bære en omfattende kartlegging av den enkeltes privatliv, men dette avhenger av hvordan teknologien fungerer, og hvordan den settes opp. I mange tilfeller vil teknologien og bruken av dataene den generer, berøre personvernet.

I tillegg til de ordinære helsetjenestene samler en rekke andre næringsaktører inn helseopplysninger via apper. Hjemmelsgrunnlaget overfor pasienten er ofte en avtale der brukeren samtykker til bruken av opplysningene. En undersøkelse av apper som Datatilsynet foretok i mai 2015, viser at to tredjedeler av alle apper ber om tilgang til personopplysninger, uten å informere om hva opplysningene skal brukes til, og hvorfor de samles inn. Dette er problematisk. Flere aktuelle saker viser at eksempelvis Google og andre aktører kan bygge opp helseinformasjon om enkeltpersoner, basert på den enkeltes søk på Internett. En undersøkelse fra 2015 viste at over 90 prosent av helserelaterte nettsider initierer http-forespørsler til en tredjepart.[17]

Gratistjenester som måler treningsaktivitet og helsetilstand, er attraktive, men brukeren «betaler» ofte med personlige data som kan brukes i reklame og til andre formål. Det kan imidlertid være uoversiktlig for den jevne nettbrukeren å vite hvor helsedataene befinner seg, om de lagres trygt og sikkert, hvem som har tilgang til dem, og hva de eventuelt brukes til. Som vist til i Datatilsynets undersøkelse, er det en risiko for at informasjonen brukes til andre formål enn brukeren opprinnelig ga tillatelse til. Det kan også være vanskelig å få slettet dataene, fordi den enkelte sjelden har oversikt over alle aktørene dataene er delt med.

I sum er det høyst betenkelig at helsetjenestene og næringsaktører ikke alltid informerer pasienter og brukere om hvordan opplysningene deres videreformidles og behandles for nye formål. Det kan være fare for at økende høsting av helseopplysninger kan undergrave den nødvendige tilliten til helsetjenestene og føre til at deler av befolkningen unngår å oppsøke det alminnelige helsehjelpstilbudet. Alternativt kan det føre til at det oppstår et «grått» marked for behandlingstilbud som unnlater å registrere pasientene eller fører «skyggejournaler» som ikke rapporterer til de lovpålagte registrene.

Dagens systemer (IKT-systemer, organisering og kompetanse) har åpenbare mangler når det gjelder å understøtte innbyggernes rett til personvern. Helsepersonell gis for omfattende tilgang i forhold til hva de reelt sett har tjenstlig behov for. Det er avdekket store mangler i logging av tilganger som gis, hvilket gjør det vanskelig å gjennomføre etterkontroller for å avdekke urettmessig tilegning av opplysninger. Det er implementert for lavt sikkerhetsnivå i henhold til Normen på noen av de mest brukte digitale innbyg-

[17] «Privacy Implications of Health Information Seeking on the Web». *Communications of the ACM.* Mars 2015.

gertjenestene i dag. Dette øker risikoen for at uvedkommende får tilgang til helseinformasjonen.[18]

På den annen side gir digitalisering muligheter for styrket personvern, og disse mulighetene må utnyttes. Selv om dagens løsninger og dagens rutiner i sektoren innebærer kjente svakheter, mener Helse- og omsorgsdepartementet at dagens IKT-løsninger lokalt i sektoren må videreutvikles for å oppnå styrket personvern og økt digitalisering.

17.6 Fremtidige problemstillinger og trender

Utvikling og bruk av velferdsteknologi og mobil helseteknologi er økende. Ifølge statistikk fra Forbes fra 2015 topper helseteknologi listen over de mest lønnsomme industriene.

Helsetjenester vil i stadig større grad utføres i hjemmet. For eksempel vil mange undersøkelser og konsultasjoner kunne gjøres uten at man fysisk oppsøker en lege. Målet er en helsesektor som er tilpasset fremtidens økte behov, men utviklingen kan på mange måter karakteriseres som teknologidrevet. Ifølge Norsk Helsenett er det naturlig å se for seg at for eksempel enheter som smarttelefoner og nettbrett blir «hub-er» for velferdsteknologi.

Offentlig helse- og omsorgssektor vil sannsynligvis miste kontrollen over deler av den digitale tjenesteleveransen til innbyggerne, blant annet fordi den enkelte brukeren selv har råderett hjemme og der tar aktivt initiativ til innføring og bruk av ny teknologi. Det vil kreve stor innsats før sentrale systemer med strenge krav til sikkerhet og personvern kan gi tilfredsstillende integrasjon mot infrastruktur i utstyr, applikasjoner og data fra innbyggernes private hjem. På veien vil nye sårbarheter introduseres, samtidig som det er fare for at gamle sårbarheter vil gjøre seg ytterligere gjeldende.

Personer med spesielle omsorgsbehov kan bruke en mer avansert trygghetsalarm med for eksempel GPS-sporing, fallalarm og andre alarmer for å bli fulgt bedre opp hjemme. Pasienter med kroniske sykdommer kan følge opp helsen sin ved å utføre egenmålinger av for eksempel KOLS selv. Offentlige og private helse- og omsorgstjenester vil da ta imot og følge opp egenmålinger og alarmer. Brukere av velferdsteknologi og mobile helseløsninger blir avhengige av at disse tjenestene er tilgjengelige døgnet rundt. Samfunnet blir sårbart for at utstyret ikke virker, eller at IKT-infrastrukturen mellom privatpersoner og helsetjenestene blir utilgjengelig. Norsk Helsenett mener en annen potensiell stor sårbarhet vil være at et høyt antall falske alarmer kan bli et økende problem.

Lav integritet for medisinsk utstyr brukt til innsamling av helsedata kan bli en sårbarhet i en tid da selvdiagnostisering er utbredt og pasienter kan insistere på at deres data skal brukes. Stadig rimeligere medisinsk utstyr vil øke graden av privatisering. Det er for eksempel allerede mulig å måle parametre som puls, blodtrykk, søvnrytme med mer med mobilen. Helsedata og private data blandes når data integreres fra hjemmet, og det blir et spørsmål hvor grensen går for hva som skal inn i en journal, og hva skal som skal holdes utenfor. Private enheter og applikasjoner vil være sårbare for datalekkasje. Systemene skal også integreres mot grensesnitt som til slutt ender opp i en elektronisk journal, men også gjerne lagres flere steder på veien, inkludert hos globale – potensielt dominerende – aktører der brukerens kontroll over lagringen og prosesseringen av dataene er liten, med mindre det foreligger særlig gode avtaler. Dersom det er helsetjenesten som eier utstyret, kan de til en viss grad sikre utstyret i henhold til egne policyer og innkjøpsavtaler. Det er imidlertid grunn til å tro at folk vil anskaffe mye av dette utstyret selv. I disse tilfellene har ikke helsetjenestene den samme kontrollen over kvaliteten på utstyret. Det vil aldri være mulig å stille samme sikkerhetskrav i et privat hjem som på en helseinstitusjon.

Videokommunikasjon for konsultasjon og lignende må nødvendigvis gå over Internett via standardiserte åpne protokoller, som igjen må sikres mot avlytting ut fra innholdet som potensielt kan kommuniseres her. Teknisk oppsett på brukersiden vil samtidig kreve sitt av brukervennligheten til tilbudet og kan være sårbart for feilkonfigurasjoner og bortfall.

Nedetid/avbrudd utenfor helsetjenestens kontroll kan i tilknytning til private hjem ta ekstra lang tid å fange opp og kartlegge omfanget av. Det kan også ta lang tid å involvere ansvarlig leverandør, varsle pasienten/sluttbrukeren og gjennomføre og kvalitetssikre utbedringen.

Overføring av sensitive data til nettskyer kan introdusere ytterligere trusler mot personvernet. Slike overføringer kan for eksempel skje ved stordata-analyse der man leier regnekraft fra eksterne nettskyleverandører. Dette kan medføre at globale kommersielle aktører vil kunne få tilgang til infor-

[18] Helsedirektoratet (2014): *Utredning av «en innbygger – én journal», IKT utfordringsbilde i helse- og omsorgssektoren.*

masjon og til en viss grad overta kontrollen over denne. I tillegg kan det bli utfordrende å avklare ansvar på tvers av landegrenser dersom leverandøren opererer globalt. Se også punkt 23.7 «Utkontraktering og skytjenester».

17.7 Vurderinger og tiltak

Helsesektoren er en svært kompleks sektor, som består av mange organisatoriske enheter, komplekse styringsmodeller og verdikjeder som på overordnet nivå ikke lar seg beskrive på en enkel måte. Utvalget har ut fra en begrenset tidsramme bare sett på et lite antall problemstillinger og tjenester innenfor dette komplekse bildet.

Utvalget mener at etableringen av Norsk Helsenett har vært et nyttig grep for å samle nasjonale løsninger og sikre enhetlige krav og styring. Gitt den kompleksiteten helsesektoren består av, hadde det vært utfordrende å opprettholde tilstrekkelig kompetanse til å ivareta sikkerheten i de tjenestene som etableres, dersom alle skulle opprettholdt regionale løsninger. HelseCSIRT er et annet initiativ som fungerer godt i sektoren, og som er en viktig ressurs for de regionale helseforetakene. Norge er det eneste landet som har etablert et statlig kompetansemiljø for sikkerhet i helsesektoren i form av HelseCSIRT. Utvalget mener det er viktig at disse ordningene forvaltes på en god måte også fremover.

Utvalget foreslår følgende tiltak:

17.7.1 Sterkere styring av IKT-sikkerhet fra Helse- og omsorgsdepartementet

Flere aktører etterlyser en sterkere styring fra HOD. Utvalget stiller spørsmål ved hvorfor styringsmuligheten som departementet har til å samkjøre mellom de regionale helseforetakene, ikke benyttes i større utstrekning.

Utvalget mener det er behov for sterkere nasjonal styring for å identifisere og styrke felles behov og for å unngå divergerende løsninger i regionene. I helsesektoren er det et sterkt behov for beslutningsevne hos HOD og for at det gis klare føringer for hvilke standarder som skal gjelde, hvilke IKT-områder RHF-ene må samkjøre, og så videre. Dette kan gjøres gjennom Direktoratet for e-helse, men det må legges til rette for at de får tilstrekkelige virkemidler og myndighet til å bistå HOD i utøvelsen av rollen. Dette inkluderer også tilgang på nødvendig IKT-faglig kompetanse der det er nødvendig. Videre må HOD sikre god samhandling med de ulike fagmiljøene.

Opprettelsen av Direktoratet for e-helse gir en mulighet for å utarbeide en samlet styringsstruktur som dekker både primær- og spesialisthelsetjenesten, med ansvar for å implementere og følge opp løsningene knyttet til e-helsesamarbeid. En slik løsning vil, spesielt i kommunesektoren, være til støtte for mange mindre aktører som kan ha vansker med å rekruttere og vedlikeholde tilstrekkelig egenkompetanse. Sikkerhetskrav i innkjøpsprosessene kan for eksempel i større grad samkjøres med større vekt på leverandøransvar.

Utvalget har gjennom sitt arbeid registrert at det er utgitt en stor mengde utredninger som omhandler IKT i helsesektoren, de siste årene. Flere av disse ser ut til å beskrive dagens utfordringer på en god måte, og det synes å være stor bevissthet i sektoren om hvilke forbedringstiltak som er nødvendige. Utvalget stiller spørsmål ved hvorfor ikke flere av tiltakene er fulgt opp, og om mengden utredninger i seg selv er til hinder for en effektiv iverksetting av tiltakene. Flere har uttrykt at evnen til å lære av tidligere utredninger ikke alltid er til stede, og at man i stor grad «finner opp hjulet på nytt». Utvalget har ikke vurdert hvorvidt dette skyldes manglende gjennomføringsevne, økonomi, eller styringsevne og -vilje. *Utvalget mener imidlertid at det er viktig med en tydeligere prioritering av forebyggende tiltak for å redusere de identifiserte sårbarhetene, og at det sikres gjennomføringskraft for disse. Som en del av dette foreslår utvalget at det nye Direktoratet for e-helse utarbeider en årlig statusrapport om tilstanden for IKT-sikkerhet i helsesektoren.*

Helsefaglig personell, som best kjenner sine egne arbeidsprosesser, må være med på å sette premissene for sikkerhetstiltak, slik at disse blir tilstrekkelig forankret i virksomheten. Sterk involvering av helsepersonell vil ikke stå i motsetning til sterkere nasjonal styring. Utvalget anerkjenner at kompleksiteten i sektoren, samt lang historikk med systemer som arves og lappes på, gjør at dette er en utfordring.

Utvalget observerer at Normen er ønsket velkommen av sektoren, og at den i all hovedsak fungerer bra. Normen gjør at helseforetakene tør å stille krav, og leverandørene blir mer oppmerksomme på temaet ved anskaffelser. Prosessen med å utvikle Normen har hatt en god effekt i seg selv og økt kompetansen i bransjen. Utvalget er orientert om at det er laget minimumskrav beregnet for små enheter. *På bakgrunn av innspill mener utvalget likevel det bør vurderes forenklinger i Normen for de minste helseforetakene i den grad det er mulig uten at det bidrar til å øke sårbarheten.*

17.7.2 Mer forskning på IKT-sikkerhet innenfor ny helse- og velferdsteknologi

Den raske utviklingen av helse- og velferdsteknologi gir en rekke nye muligheter, men kan også føre til økt sårbarhet dersom det ikke tas nødvendige forholdsregler. Dette kan være både sårbarheter innad i helseforetakene og sårbarheter knyttet til bruk av helsetjenester utenfor helseforetakenes kontroll i privathjem. Behovet for kontroll av utviklingen understrekes av de tidligere beskrevne sårbarhetene knyttet til velferdsteknologi, som et økt antall angrepsflater, uklarheter omkring databehandleransvar og manglende digitaliseringsstrategi.

Etter utvalgets vurdering bør helse- og velferdsteknologi som i stor grad endrer samfunnet, utredes og følges opp av en offentlig debatt før implementering. Utvalget mener det er behov for en mer spisset forskningsinnsats for å se på sikkerhetsaspektene ved teknologien, samtidig som man ivaretar de mulighetene og utfordringene som ny helse- og velferdsteknologi vil gi. Forsøk som pågår med ny helse- og velferdsteknologi, bør videre samordnes nasjonalt for å sikre kompetanseoverføring. Det nye Direktoratet for e-helse bør sikre at disse initiativene samordnes.

17.7.3 Etablere løsninger for å imøtekomme utviklingen innenfor helse- og velferdsteknologien

Ved innføring av helse- og velferdsteknologi bør hovedregelen være at tjenesteeieren av slike løsninger tar et overordnet ansvar for sikkerheten i hele verdikjeden og ikke utelukkende baserer seg på at sikkerheten er ivaretatt av underliggende tjenester som for eksempel ekom-tilbydere. Også på dette området er leverandørkjeder og verdikjeder viktig. Se for øvrig omtale av verdikjeder i punkt 23.1 «Etablere nasjonalt rammeverk for å ivareta en helhetsvurdering av verdikjeder».

Utvalget støtter Norsk Helsenetts forslag om at helsenettet, i samarbeid med sektoren, bør vurdere om det er sentrale felleskomponenter (innen kommunikasjon mot Internett) som sektoren behøver for å fremme en trygg innføring av velferdsteknologiske løsninger.

17.7.4 Gjennomføre flere IKT-øvelser der kritiske systemer er ute av funksjon

Det er behov for å ha en beredskap for bortfall av IKT i helsesektoren, enten dette skyldes tilsiktede eller utilsiktede IKT-hendelser. Mindre grad av manuelle rutiner å falle tilbake på kan i fremtiden gi nye og økte sårbarheter. *Utvalget mener det bør gjennomføres flere IKT-øvelser der kritiske systemer er ute av funksjon.* Se også kapittel 20 «Styring og kriseledelse». I tillegg kreves det at sentrale helsetjenester kan opprettholdes uavhengig av IKT-støtte. Utvalget stiller spørsmål ved om man ved fremtidens heldigitaliserte helsesystemer (eksempelvis strukturerte pasientjournaler) vil ha mulighet og evne til å gå tilbake til manuelle systemer, og om vi med dette påfører oss en ny sårbarhet.

Kapittel 18
Transport

Transportsektoren har en sentral plass i det moderne samfunnet, og velfungerende transport er nødvendig for verdiskapingen. Transportsektoren kan deles inn i fire transportgrener, som hver har sine særegenskaper. Det blir investert mye i IKT i transportsektoren for å effektivisere sektoren og for å øke sikkerheten.

Samferdselsdepartementet har det overordnede ansvaret for IKT-sikkerhet innen luftfart, sjøtransport, veitrafikk og jernbane. Departementet har blant annet etatsstyring av Statens vegvesen, Vegtilsynet, Jernbaneverket, Luftfartstilsynet, Kystverket, Statens havarikommisjon for transport og Statens jernbanetilsyn.

Både Sårbarhetsutvalget og Infrastrukturutvalget omhandlet transportsektoren. Lysneutvalget vil peke på at de vurderingene fortsatt står seg. I tiden etter at disse rapportene ble utgitt, har digitaliseringen kommet mye lenger, og tendensene er derfor styrket. Kompleksiteten i transportsektoren har økt.

IKT-systemer i transportsektoren har effektivisert informasjonsflyten betydelig og blant annet bidratt til bedre utnyttelse av veikapasiteten. Men dette gjør også at sårbarheten blir større, ettersom transportsektoren blir kritisk avhengig av ekom, satellittbaserte tjenester og elektrisitet og en svikt i disse tjenestene vil redusere kapasiteten og effektiviteten betydelig.

Utvalget har valgt å se grundigere på sjøtransport, særlig på grunn av denne sektorens avhengighet av satellittbaserte tjenester. De øvrige transportgrenene behandles på et overordnet nivå, og utvalget har valgt å se på noen utvalgte sårbarheter.

18.1 Veitrafikk

IKT-systemer blir stadig mer integrert og koblet sammen. Som tidligere beskrevet vil det i følge estimater være mellom 25 milliarder og 50 milliarder enheter koblet til Internett gjennom tingenes Internett. Denne trenden treffer også veitrafikken. Statens vegvesen ser at det er en utfordring å sikre disse enhetene, da teknologien utvikles svært raskt. Nye løsninger for nasjonal reiseplanlegging og elektronisk billettering er under gjennomføring for kollektivtransporten i hele landet. Over en og en halv million kunder benytter seg av elektronisk reisekort eller mobiltelefon når de kjøper billett på båt, buss eller bane, og antallet brukere stiger raskt.[1]

Statens vegvesen er et myndighetsorgan og en vei- og trafikkforvalter, og består av Vegdirektoratet og fem regioner. Statens vegvesen drifter fem regionale veitrafikksentraler (VTS), som gjør det mulig å overvåke trafikken. Fra disse sentralene styres blant annet lyskryss, trafikkbommer, datastyrte friteksttavler og fjernstyrte skilt via fjernstyringssystemer. Sentralene har mulighet til å avlaste hverandre. Vegtrafikksentralen i Oslo har et landsansvar når det gjelder nasjonale kriser og veimeldinger. VTS-ene samarbeider med nødetatene, og spesielt politiet, når dette er naturlig, for eksempel ved trafikkulykker, ras og lignende. VTS-ene har muligheten til å bryte gjennom radiosendinger for å gi viktige beskjeder. I tillegg har Statens vegvesen ansvar for tre viktige registre: motorvognregisteret, førerkortregisteret og Nasjonal vegdatabank (som inneholder teknisk informasjon om veinettet).

Vegtilsynet er direkte underlagt vegdirektøren, og er organisatorisk og styringsmessig skilt fra Statens vegvesen. I årsrapporten for 2014 går det frem at Vegtilsynet driver risikobasert systemtilsyn. Ingen av tilsynene var rettet mot IKT-sikkerhet.

Etablering av et felles sektor-responsmiljø for håndtering av hendelser har vært diskutert for transportsektoren. Aktørene konkluderte med ikke å opprette et sektorvis responsmiljø på grunn av ulikhetene mellom transportgrenene. Høsten 2014 ble det imidlertid etablert en egen IKT-sikkerhetsenhet i Statens vegvesen, og etaten

[1] Meld. St. 26 (2012–2013) *Nasjonal transportplan 2014–2023.*

ble tilknyttet NSM NorCERT. Etaten har hittil hatt lite erfaring med IKT-hendelser.

Intelligente transportsystemer (ITS) vil i fremtiden kunne bidra til mer effektiv bruk av transportmidlene og bedre utnyttelse av kapasiteten i infrastrukturen. ITS omfatter løsninger som i en eller annen form benytter informasjons- og kommunikasjonsteknologi (IKT) i et trafikk- eller transportsystem. ITS kan blant annet brukes som del av en anleggsfase på store utbyggingsprosjekter for å ivareta trafikksikkerhet og fremkommelighet. ITS kan også inngå som elementer i nye transportsystemer for å legge til rette for styring, informasjon og beredskapssituasjoner. For nødetatene og andre beredskapsaktører vil bruk av ITS være avgjørende for å kunne bidra i beredskaps- og nødssituasjoner.[2] Innovasjonstakten på dette området er høy. Et stadig viktigere trekk er den økende integrasjonen mellom infrastruktur og transportmiddel. Nye ITS-løsninger utvikles i et internasjonalt miljø. ITS-direktivet er en del av EØS-avtalen.[3]

Statens vegvesens strategi for bruk av ITS inneholder en rekke tiltak. Eksempler på tiltak for bedre trafikksikkerhet på vei er streknings-ATK, automatisk kjøretøykontroll og dynamiske fartsgrenser. På litt lengre sikt kan elektroniske kant- og midtlinjevarslere være aktuelt. Innenfor kjøretøyteknologi finnes ulike kjørestøttesystemer og systemer for passiv sikkerhet. Statens vegvesen tar også sikte på å etablere et nasjonalt trafikk- og transportdatasystem for alle offentlige veier.[4]

Bompenger utgjør en viktig inntektskilde for veiutbyggingen. En egen infrastruktur for bompengeinnkreving er drevet av cirka 60 ulike bompengeselskaper. AutoPASS Grindgut er en ny nasjonal IKT-løsning som skal erstatte det eksisterende sentralsystemet for bompengebetaling. Sentralsystemet er det administrative systemet bomselskapene benytter for å kreve inn bompenger. Systemet håndterer i dag nær 500 millioner passeringer i bomstasjoner hvert år.

18.1.1 Sårbarhet i kjøretøy og digitale trafikkstyringssystemer

Den teknologiske utviklingen går i retning av selvgående kjøretøy, samt at kjøretøy blir tilkoblet Internett. Det finnes cirka 23 millioner biler som er koblet direkte til Internett, og dette tallet er forventet å stige til 152 millioner i løpet av 2020. Amerikanske myndigheter har opplyst at fire av 48 selvkjørende biler over en periode på åtte måneder har vært involvert i ulykker. Bilprodusentene har avvist at de selvkjørende bilene var årsak til ulykken.[5] Beregninger fra Transportøkonomisk institutt har vist at teknologiske tiltak kan bidra til å oppnå en nedgang i antall drepte eller hardt skadde i trafikken.

SINTEF[6] har påpekt flere aktuelle sikkerhetsutfordringer knyttet til kjøretøy som følge av den økende graden av tilknytning til Internett. Noen av disse knyttes til masseprodusert elektronikk, der det hittil ikke har vært investert tilstrekkelig i sikkerhet. Løsningene er ofte proprietære og med manglende standarder. Selv standardiserte protokoller har vist seg å være uten sikkerhetsmekanismer. Dette kan blant annet gjøre det mulig å overstyre styre- og bremsesystemene via tilgang til underholdningssystemet i bilen. I tillegg er kjøretøy utstyrt med komponenter med lang levetid, noe som gjør at disse blir hengende etter i forhold til trusselbildet. Eksempelvis er det vist til tilfeller i bilindustrien der det ikke er implementert mekanismer for softwareoppdatering. Konsekvensen av dette er at det vil ta lang tid å rette opp i sårbarheter selv om de blir kjent.

Boks 18.1 Hacking av trafikklys

En gruppe amerikanske forskere tilknyttet University of Michigan utførte et hackingangrep på ekte, operative trafikklys. Lysene i det aktuelle området brukte trådløse 5,8 GHz-nettverk, som ligner på den vanlige 802.11-standarden, til å kommunisere med. Det forskerne raskt fant ut, var at de dermed enkelt kunne se nettverks-ID-en (SSID) til hvert lyskryss bare ved hjelp av vanlige, umodifiserte PC-er og smarttelefoner. De brukte i stedet en spesiallaget radio. Forskerne fant ut at kommunikasjonen til kontrollerne som styrer lyskryssene, heller ikke var kryptert, noe som satte dem i stand til å analysere systemarkitekturen og lage sine egne kommandoer.

2 Direktoratet for samfunnssikkerhet og beredskap (2012): *Samfunnets sårbarhet som følge av bortfall av elektronisk kommunikasjon.*

3 Meld. St. 26 (2012–2013) *Nasjonal transportplan 2014–2023.*

4 Ibid.

5 Walton, Mark (2015): *Google's quirky self-driving bubble car hits public roads this summer.*

6 Moe, Marie (2015): *Informasjonssikkerhet og personvern: Hva må vi tenke på ved tilgjengeliggjøring av data?* Sintef IKT, Systemutvikling og sikkerhet.

Sikkerheten i de digitale trafikkstyringssystemene er en utfordring. Systemene styrer pumpesystemer mellom undersjøiske tunneler, lyssignaler, variable skilt med videre. Statens vegvesen har ikke hatt IKT-hendelser (hacking eller tjenestenektangrep) så langt.

Internasjonale avtaler og internasjonal transportpolitikk stiller en rekke betingelser og gir bindinger og muligheter når det gjelder utviklingen av Norges transportsystem på vei. Det setter rammer for norsk transportpolitikk, og særlig gjelder dette tekniske standarder og krav til kjøretøy. Når for eksempel kjøretøy blir produsert med Internett-forbindelse, gjelder dette også kjøretøy på norske veier.

18.1.2 Trafikkstyringens avhengighet av elektronisk kommunikasjon og satellittbaserte tjenester

Staten vegvesen har virksomhet i hele landet og er avhengig av tilgjengelig elektronisk kommunikasjon (ekom) for at ulike systemer skal kunne snakke med hverandre. Pinseflommen (se kapittel 20 «Styring og kriseledelse») illustrerer hvilke konsekvenser bortfall av elektronisk kommunikasjon kan ha. Trafikkavvikling og trafikkstyring vil bli rammet ved ekombrudd og gi redusert informasjonsflyt til/fra veitrafikksentralene, noe som hemmer informasjon til trafikantene og fremkommeligheten, spesielt i de større byene med mange tunneler. Ekom er særlig viktig for å opprettholde tunnelsikkerheten. Ved langvarig brudd i ekom vil trafikkavviklingen kunne bli treg eller stoppe opp, og de samfunnsmessige konsekvensene vil bli store.[7] Statens vegvesen har jobbet med reservekommunikasjon, og har både satellitt-telefoner, nødnett og prioritert mobilsamband. De vurderer også VHF for helt lokal bruk. IKT-avdelingen har startet en utredning for å se på det totale kommunikasjonsbehovet.

Mye av kommunikasjonen som Statens vegvesen er avhengig av, skjer via trådløse nett. Dersom kommunikasjon blir jammet i et område, vil det kunne sette viktige funksjoner ut av spill, for eksempel pumpestasjoner, trafikkstyring med videre. Statens vegvesen har uttrykt bekymring for politiets ønske om å få mulighet til å jamme trådløse nett.

I tråd med utviklingen av ITS, der en blant annet er avhengig av posisjoneringsdata, øker også avhengigheten av GPS og satellittbaserte tjenester. Se kapittel 12 «Satellittbaserte tjenester».

Boks 18.2 Bruk av ITS i nødsituasjoner

ITS vil være avgjørende for å kunne bidra i beredskaps- og nødssituasjoner. Et eksempel på bruk av ITS i nødsituasjoner er *eCall*.[1] Tjenesten eCall er tenkt å virke slik at en teknisk innretning i bilen automatisk ringer nødnummeret og opplyser om bilens posisjon ved ulykker, slik at nærmeste nødsentral raskt kan sende assistanse til riktig sted. Systemet er planlagt å bli en felleseuropeisk alarmtjeneste for kjøretøy, bygd på alarmnummeret 112. Det er satt som mål at alle biler som blir solgt i EU-området, skal være utstyrt med satellittposisjonering og kommunikasjon via mobiltelefonnettet. Det er anslått at 2 500 liv kan reddes hvert år i Europa når eCall blir ferdig utviklet og utbredt. Systemet vil dermed være et viktig bidrag til trafikksikkerheten gjennom å redusere konsekvensene av ulykker.

[1] Direktoratet for samfunnssikkerhet og beredskap (2012): *Samfunnets sårbarhet som følge av bortfall av elektronisk kommunikasjon.*

18.1.3 Særskilte personvernutfordringer innen veitrafikken

Digitalisering i transportsektoren utfordrer personvernet. Hensynet til personvern skal være en viktig del av planleggingen og videreutviklingen av ITS.[8] De fleste innsamlede opplysninger er ikke sensitive, men sammenstilt med andre kilder og mulige nye anvendelsesområder kan de endre risikoen for personvernet.[9] En rekke initiativer er satt i verk for å imøtekomme dette. Blant annet har Datatilsynet og Statens vegvesen sett på tekniske løsninger for økt anonymitet i bompengesystemet og vurdering av unntak for lagring av opplysninger om passeringer etter bokføringsloven.[10] Det vises også til arbeidet med en nasjonal bransjenorm for elektronisk billettering. Der del-

[7] Samferdselsdepartementet (2010): *Krisescenarioer i samferdselssektoren – KRISIS.*

[8] Meld. St. 26 (2012–2013) *Nasjonal transportplan 2014–2023.*

[9] Øvstedal, L., Lervåg, L.E. og T. Foss (2010): *Personvern og trafikk: Personvernet i intelligente transportsystemer.* SINTEF.

[10] Meld. St. 26 (2012–2013) *Nasjonal transportplan 2014–2023.*

tok både Datatilsynet, Statens vegvesen og transportaktører for å nå frem til en enighet om hvordan reise med kollektivtrafikk kan skje ved hjelp av elektroniske billetter samtidig som retten til personvern, fri ferdsel og anonymitet blir ivaretatt.[11]

Trafikkregistrene inneholder informasjon om blant annet folk med hemmelig adresse og kjøretøy som tilhører politiet og Forsvaret. Dette er informasjon som ikke skal offentliggjøres. Statens vegvesen har påpekt at de mange innsynsbegjæringene fra eksterne som ønsker kopi av hele registeret, er en utfordring ettersom registrene ikke er laget for å gi delvis tilgang. Det er satt i gang et arbeid for å se på nye løsninger for bedre å kunne strukturere og skille ut sensitive data.

18.2 Jernbane

Jernbanen står overfor store investeringer og digitalisering i årene som kommer. Det samlede jernbanenettet i Norge er på om lag 4 000 km, hvorav om lag 1 400 km ikke er elektrifisert. Hver dag frakter jernbanen i snitt mer enn 160 000 passasjerer og 80 000 tonn gods. Som de andre transportgrenene er jernbanen en del av et internasjonalt system, riktignok begrenset til våre naboland. Med innføringen av ERTMS (European Rail Traffic Management System) vil norsk jernbane få samme signalsystem som europeisk jernbane.

ITS-løsninger vil bli viktige innen trafikantinformasjon og trafikkstyring. Ny teknologi gjør det enklere å identifisere og registrere hendelser gjennom bruk av sensorer eller kameraovervåking og kontroll, og slik bidra til å gi bedre og løpende informasjon om tilstanden i infrastrukturen. Dette vil kunne bidra til å identifisere feil i infrastrukturen og løse problemet før det påvirker togtrafikken. På sikt kan det også tenkes å påvirke behovet for henholdsvis korrektivt og forebyggende vedlikehold av infrastrukturen.

Jernbaneverket skal på vegne av staten drifte, vedlikeholde og bygge ut statens jernbaneinfrastruktur med tilhørende anlegg og innretninger. Jernbaneverket har ansvaret for trafikkstyringen på det nasjonale jernbanenettet.

Statens jernbanetilsyn (Jernbanetilsynet) er en selvstendig etat underlagt Samferdselsdepartementet, og er tilsynsmyndighet for blant annet jernbane, trikk og T-bane. Statens jernbanetilsyn fører kontroll og tilsyn med blant annet 33 jernbanevirksomheter. En forskrift om sikkerhet trådte i kraft 1. juli 2015, og Jernbanetilsynet fikk med den hjemmelsgrunnlag for å føre tilsyn mot tilsiktede hendelser. Jernbanetilsynet har få ressurser til oppfølging av IKT-sikkerheten.

NSB er et nordisk transportkonsern der godstrafikk og persontransport med tog utgjør en viktig del av virksomheten. Ansvarsforholdene vil bli endret med den kommende jernbanereformen, der det er besluttet å etablere et eget jernbanedirektorat. Dette skal blant annet ha en koordinerende rolle overfor aktørene i både egen sektor og øvrig kollektivtransport.

Som tidligere beskrevet er det ikke etablert et felles responsmiljø innenfor samferdselssektoren. De mest sentrale aktørene har valgt å inngå som medlemmer av VDI-samarbeidet med NSM NorCERT.

Flere aktører innenfor sektoren har blitt utsatt for utilsiktede IKT-hendelser, uten at disse har fått konsekvenser for den operative driften. En av hendelsene i 2015 ble opplevd som så alvorlig at Jernbaneverket for første gang satte krisestab med hele ledelsen til stede. I dette tilfellet mente Jernbaneverket det var avgjørende med fysisk nærhet til underleverandøren for effektivt å håndtere hendelsen.

18.2.1 Sikkerhetsutfordringer i skinnegående trafikk

Skinnegående transport er avhengig av at en rekke systemer er tilgjengelige. *Systemer i transportmiddelet* omfatter systemer som støtter operasjon og drift av transportmiddelet, samarbeid med andre systemer og informasjon til passasjerer. *Systemer langs kjøreveien* styrer uavhengige soner og overlevering av kjøretøy fra en sone til en annen. De styrer også alle elektromekaniske enheter i sin sone inklusiv energikontroll. *Stasjonsystemene* styrer infrastrukturen på stasjonene – alt fra heiser til systemer for passasjerinformasjon. *Kontrollsentralsystemene* styrer transportnettverket og samarbeider med systemene på toget, langs kjøreveien, med mer. *Administrative systemer* støtter transportoperatøren i forretningsvirksomheten, som transportplan, vedlikeholdsplan, regnskap, HR med videre.

ERTMS (European Rail Traffic Management System) vil være det nye signal- og sikringssystemet for jernbanen. ERTMS er et automatisk togkontrollsystem, men det er ikke laget for førerløse tog. I løpet av de kommende årene vil byggingen av ERTMS medføre store endringer for den norske jernbanen. Den mest synlige endringen er at

[11] Statens Vegvesen, Vegdirektoratet (2014): *Bransjenorm for personvern og informasjonssikkerhet i elektronisk billettering.*

de ytre signalene som i dag står langs sporet og regulerer togtrafikken, erstattes med overføring av signalinformasjon direkte til det enkelte toget via jernbanens eget mobilnett GSM-R. Videre vil togene fritt kunne trafikkere andre lands infrastruktur uten å være flerdobbelt utrustet med hvert enkelt lands spesielle system for automatisk togkontroll. ERTMS kan karakteriseres som et meget stort, sikkerhetskritisk, distribuert programvarebasert system basert på felles europeiske standarder. Dersom mobilnettet GSM-R får utfall, vil konsekvensen for trafikken på jernbanenettet være stor.

Ifølge Jernbaneverket vil innføringen av ERTMS skape en mer pålitelig jernbane enn med dagens signalanlegg, som er basert på sårbar reléteknologi. Det er forventet at antall tekniske feil knyttet til signal- og sikringsanleggene vil bli redusert. Samtidig er det fra flere hold uttrykt bekymring for at dette vil introdusere nye sårbarheter, ettersom IKT-systemer vil styre kritisk sikkerhetsinformasjon, som blant annet hastighet og bremselengde for togene.

Jernbaneverket har uttrykt at de vil rette oppmerksomheten mot dette fremover. Arbeidet med å sikre tilgang og kapasitet på nøkkelkompetanse innenfor signalområdet og øvrige spesialiserte jernbanefag har høy prioritet.[12]

18.2.2 Sårbarheter i systemer knyttet til togfremføring

FIDO (Filtrert distribusjon av operative kunngjøringer) er Jernbaneverkets nye distribusjonssystem for informasjon ved togfremføring og arbeid i spor. Med dette distribusjonsverktøyet kan jernbanen sende ut automatisert og målrettet informasjon til den det gjelder, i stedet for å distribuere papirer og dokumenter manuelt. Jernbaneforetak kan også motta data direkte og implementere disse i sine egne systemer, samt skrive ut informasjon dersom det er ønskelig. Systemet har en modell av jernbaneinfrastrukturen og en ruteplan som grunndata. Disse dataene behandles i systemet og settes sammen til en visning basert på hvem man er, og hva man skal gjøre. FIDO er kritisk ettersom man må kvittere ut informasjon per avgang for å få lov til å kjøre toget.

FIDO vil på sikt være kilden for ruteinformasjon til andre fagsystemer internt i Jernbaneverket, men også til eksterne systemer hos jernbaneforetak og entreprenører. FIDO har mange brukere: togførere, jernbaneselskaper, sikkerhetsvakter, entreprenører, operative ruteplanleggere og driftskoordinatorer. En feil i dette systemet førte til togstans i hele landet i mai 2015.

18.2.3 Avhengighet av ekom

De største sårbarhetene innen skinnegående transport er hittil knyttet til avhengigheten av andre samfunnsfunksjoner som energiforsyning og elektronisk kommunikasjon (ekom). En stor del av den skinnegående transporten er elektrifisert, og driften av infrastrukturen og sikkerhetssystemene krever tilgjengelig ekom.

Jernbaneverket jobber aktivt med å fase ut gamle systemer. Det linjesvitsjede systemet som bærer av fasttelefon fases ut og erstattes av IP-telefoni. Transmisjonsnettets betydning fremover vil øke, ettersom det binder sammen det nye signalsystemet, systemet med tilstandsovervåking, med videre. De gamle systemene har kjente sårbarheter som eksponerer Jernbaneverket for angrep. Ifølge Jernbaneverket konkurrerer fornyelse av IKT-systemer med andre driftsoppgaver. En annen utfordring er de ulike tidskonstantene i investeringer. Jernbaneverket bygger jernbane for 100 år og signalanlegg for 40 år, mens IKT-systemer har en mye kortere levetid enn dette og dermed krever jevnlig fornyelse. Analog teknologi går til sikker tilstand ved feiltilstand. Ved innføring av digitale systemer er det usikkerhet knyttet til hvilken mulighet utenforstående har til å manipulere systemene, slik at de ikke går til sikker tilstand. I dag må en være fysisk til stede for å manipulere systemet. Jernbaneverket har gjennomført en verdivurdering av informasjon om signalanleggene, og skadepotensialet er høyt. Som for andre sektorer er det utfordrende å håndtere sensitiv informasjon, særlig med hensyn til problematikken med underleverandører.

18.3 Luftfart

Luftfarten i Norge har en desentralisert lufthavnstruktur som gir god tilgang til passasjertransport og flyfrakt i hele landet. Luftfarten er blant annet sentral for helsesektoren, som benytter rutefly til pasientreiser, og i form av akuttberedskap for ambulansefly og -helikoptre. Luftfarten har en lang tradisjon med sterk vekt på sikkerhet, blant annet ved hjelp av prosedyrer for å kunne håndtere «enhver» situasjon. Pilotene og mannskapet om bord er blant sikkerhetsbarrierene mot svikt i tekniske systemer. Dersom det

[12] Meld. St. 26 (2012–2013) *Nasjonal transportplan 2014–2023.*

oppstår teknisk svikt eller feil, skal de manuelle prosedyrene ta over. Til tross for dette har også luftfarten med økt digitalisering flere utfordringer med hensyn til IKT-sikkerhet.

Luftfartsinfrastruktur består forenklet av luftfartøy, lufthavner og flysikringstjenester. Inn under flysikringstjenester kommer blant annet kontrollsentraler og luftromsreguleringer, og inn under lufthavner kommer blant annet bakketjenester som bagasjehåndtering og catering. Flyselskapenes elektroniske systemer for håndtering av passasjerer (innsjekk, bag-drop og så videre) er et eksempel på avhengighet mellom lufthavnoperatør og flyselskap. Alle enheter i infrastrukturen er avhengige av fungerende kommunikasjon, spesielt digital kommunikasjon (IKT), for å kunne levere en sikker og effektiv tjeneste til passasjerene.

Luftfartstilsynet har hovedansvaret for tilsynet med norsk sivil luftfart. Dette inkluderer tilsyn med blant annet luftfartøy, flyselskaper, flyplasser, verksteder, flysikringstjenester, personell, utdanningsinstitusjoner med mer. Luftfartstilsynet skal også sikre luftfarten mot terror og sabotasje (security) og ivareta helse, miljø og sikkerhet for flygende personell. Videre skal Luftfartstilsynet utvikle og oppdatere regelverk og påvirke utviklingen av internasjonale regler på luftfartens område. Luftfartstilsynet har begrenset hjemmelsgrunnlag for å føre tilsyn med IKT-sikkerhet i luftfartssektoren. Luftfartsloven § 4-1 stiller krav om luftdyktighet for luftfartøy og viser til en EU-forordning. I forordningen, som tar for seg de flyoperative systemene, er IKT-sikkerhet ikke nevnt. Det stilles krav til design av luftfartøy. I EASA Certification Specification (CS) 25.1309 fastslås det at luftfartøy skal designes slik at ingen enkeltsystemer i seg selv skal kunne forårsake katastrofale feil. Innenfor flysikringstjenesten slås det fast i en EU-forordning (1035/2011) at operasjonelle data skal være sikret slik at kun autorisert personell har tilgang. Forordningen gjennomføres i norsk rett i forskrift om felles krav for yting av flysikringstjenester (BSL G 2-2). Forordningen er veldig generell, og for tilsynsmyndigheten er det utfordrende å gjennomføre tilsyn basert på veiledninger.

Avinor AS er et statlig eid aksjeselskap der eierskapet forvaltes av Samferdselsdepartementet. Selskapet har ansvaret for å eie, drive og utvikle et landsomfattende nett av lufthavner for den sivile luftfarten og en samlet flysikringstjeneste for den sivile og militære luftfarten.

Avinor Flysikring AS er sertifisert som tjenesteyter for leveranser av flysikringstjenester. Avinor Flysikring AS har som et ledd i barrierebyggingen mot den stadig økende IKT-trusselen etablert et eget nettverk som ikke er koblet opp mot andre nettverk. Dette nettverket driftes og monitoreres av Avinor Flysikring AS som leverandør av lufttrafikktjenester i Norge.

Som tidligere beskrevet er det ikke etablert et felles responsmiljø innenfor samferdselssektoren. Det er heller ikke gjennomført nasjonale øvelser i samordning og håndtering av IKT-hendelser i luftfarten. Avinor har egen CSIRT-funksjon og er tilknyttet ekstern CERT. Luftfartstilsynet fører ikke særskilt statistikk over IKT-hendelser, men slike hendelser tas inn i den ordinære rapporteringsstatistikken. Statens havarikommisjon har statistikk over hendelser og ulykker innenfor luftfarten, men ikke over IKT-hendelser spesielt.

18.3.1 Internasjonale avhengigheter – globale premissgivere

Luftfart er en global industri der verdensomspennende regler og standarder setter betingelser for godkjenning av luftfartøy, krav til IKT-sikkerhet og prosedyrer for flygning, avgang og landing. Dagens systemer innen luftfart aldres, og flytrafikken øker. Økt trafikk øker behovet for utnyttelse av luftrommet, sammen med krav til pålitelighet, sikkerhet, komfort og miljø. Den globale luftfarten vil de nærmeste årene gjennomgå en betydelig modernisering på IKT-området, med NextGen i USA og Single European Sky i Europa som de store initiativene.[13] Slike globale initiativer gir også rammebetingelser for hva Norge selv kan og må gjøre som nasjon.

Sammen med Samferdselsdepartementet deltar Luftfartstilsynet i internasjonale organisasjoner for å ivareta norske interesser. To av disse organisasjonene er europeiske EASA (European Aviation Safety Agency) og FNs organisasjon for sivil luftfart, ICAO (International Civil Aviation Organization). ICAO arbeider for internasjonal standardisering og beste praksis innenfor luftfart. ICAOs standarder er folkerettslig bindende for statene som har ratifisert Chicagokonvensjonen. Anbefalinger i vedleggene til Chicagokonvensjonen er ikke bindende, men fungerer som beste praksis. Det er i EU-forordning 1035/2011 inkludert spesifikke krav innen IKT for tjenesteytere.[14]

---

[13] Sampigethaya et al. (2011): *Future E-Enabled Aircraft Communications and Security: The Next 20 Years and Beyond, Proceedings of the IEEE* | Vol. 99. No. 11.

[14] EU (2011): *Commission implementing regulation (EU) No 1035/2011.*

European Aviation Safety Agency ble etablert i 2002. Hovedaktivitetene er strategiutvikling og sikkerhetsledelse (safety), sertifisering av produkter og oversikt over godkjente organisasjoner og EU-medlemsland. Det internasjonale forbundet av flyselskaper (IATA) legger stor vekt på sikkerhet og tilbyr også en rekke verktøy for IKT-sikkerhet.

Utvalget er kjent med at det har vært en rekke personvernmessige utfordringer knyttet til tvungen overføring av passasjerlister, såkalte PNR-data, til USA. Opplysningene blir lagret i databaser og sammenlignet med andre databaser før reisende tillates innreise til USA. Det er flere eksempler på at personer feilaktig har blitt ført opp på «no fly»-lister i USA som følge av ukorrekte lister. I EU pågår det arbeid med å få på plass en tilsvarende ordning i Europa. Der diskuteres blant annet krav som skal ivareta passasjerenes rettigheter bedre, som for eksempel at de skal være informert om hvilke data som samles inn.

Boks 18.3 Trådløse passasjernettverk sårbare for inntrenging

I en rapport skrevet for amerikanske luftfartsmyndigheter påpekes det at fly med trådløst passasjernettverk kan være sårbart for inntrenging.[1] Dette kan gjøre det mulig for en angriper å få tilgang til og kompromittere flyets kontrollsystem. Som en respons på rapporten har FBI og TSA varslet flyselskaper om å være oppmerksomme på mistenkelig aktivitet. Et viktig spørsmål, som det er uenighet om mellom flyfabrikanter og sikkerhetsforskere, er om tilgang til flyoperative systemer kan oppnås via passasjernettverket.

[1] United States Government Accountability Office (2015): *Air Traffic Control. FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen.*

18.3.2 Sårbarheter om bord i fly

Et luftfartøy har avansert elektronikk og IKT-systemer om bord. Systemene i luftfartøy kan klassifiseres i tre nett etter kritikalitet: 1) De flyoperative systemene om bord. Systemene er lukket og kommuniserer med støttesystemer på bakken. Kun pilotene er brukere av de operative kontrollsystemene. 2) Tjenestenett som ivaretar behovet for vedlikehold og drift for flyselskapet. Mannskapets enheter, for eksempel nettbrett, kan kobles til dette tjenestenettet. 3) Passasjerenes underholdningssystemer om bord i luftfartøyet. Disse systemene er adskilt fra de andre to. Det er bare krav om logisk adskillelse og ikke fysisk separasjon mellom nettet til passasjerene og de andre systemene i flyet. Det er identifisert sårbarheter knyttet til underholdning og velferdstilbud om bord, se boks 18.3.

Flyselskapene tar i bruk nettbrett som verktøy (Electronic Flightbag) i cockpiten. Dette kan medføre at sårbarheten for inntrenging fra utenforstående i flyoperative data blir en ny problemstilling. I stedet for den tidligere pilotkofferten med kart, prosedyrer og reiserute får pilotene nå med seg et nettbrett med den informasjonen de trenger for å gjennomføre flyturen. Det er et spørsmål hvordan nettbrett-tilkoblingen er sikret, og i hvilken grad nettbrettet for eksempel er tilgjengelig for andre. Flyselskaper har etablert strenge rutiner for bruk av Electronic Flightbag. Rutinene beskriver blant annet bruk av nettbrettet slik at informasjon ikke kommer på avveier, ikke blir infisert av virus, og så videre. Det er likevel en kjensgjerning at mennesket er den siste barrieren også her, og det er ikke nødvendigvis alltid slik at rutinene følges.

Sårbarheter i programvare kan slå ut på ulike måter. Kart og kartoppdateringer er en kritisk funksjon. Det har vært ett tilfelle av svikt i kartoppdateringen som medførte at en person fysisk måtte dra rundt til alle flyene for å oppgradere kartene manuelt ved hjelp av minnepinne. Denne hendelsen fikk ikke kritiske konsekvenser.

Landing kan skje automatisk i dag. Det er krav om landing på autopilot dersom værforholdene er spesielt dårlige. En forutsetning for å kunne lande på autopilot under dårlige værforhold er at flyplassen er utstyrt med avansert teknologi som støtter bruk av autopiloten. Avgang skjer alltid manuelt. Når luftfartøyet når en viss høyde, kan autopiloten kobles inn. I de fleste tilfeller vil det være slik at styrmannen (flygende pilot) både tar av og lander manuelt. Pilotene og flygelederne anses som de viktigste barrierene i Air Traffic Management (ATM). Pilotene kan fly manuelt hele tiden, men det er en uttrykt bekymring blant piloter i dag hvorvidt de reelt sett er i stand til å håndtere uforutsette problemer, gitt den teknologiske avhengigheten. Dette gjelder spesielt store luftfartøy. Rutinene de skal følge finnes på nettbrettet. I ytterste konsekvens må de fly tilbake til utgangspunktet.

I mai 2015 styrtet et militært transportfly under testing i Sevilla. Flyselskapet sendte varsel til kundene sine om mulige problemer og instru-

erte dem til å kjøre kontroll på elektroniske kontrollenheter på motoren (Electronic Control Units). En programvarefeil gjorde at tre av fire motorer stoppet opp.

18.3.3 Systemkompleksitet i operative systemer og på lufthavnene

Elektronisk informasjonsflyt er viktig og skal sikre at samspillet mellom leverandører av bakketjenester, flyselskaper og lufthavnoperatører fungerer. Det er mange IKT-systemer på lufthavnene som er koblet sammen i nettverk. Avinor har fysisk adskilt det operative nettet fra det administrative nettet. Det er også fysisk adskilt fra lufthavnnettet, som mange systemer på lufthavnene er avhengige av.

Ifølge Luftfartstilsynet er de operative systemene stabile. Det har vært bortfall av redundans, men det har ikke medført bortfall av tjenester. Luftfartstilsynet har likevel uttrykt bekymring knyttet til den reelle sikkerheten i systemene, ettersom de til nå har operert i et lukket system. Økt tilsynsaktivitet kan gi bedre grunnlag for å si noe mer kvalifisert om sikkerheten.

I 2015 førte en teknisk feil til stans i flytrafikken ved Sola og Flesland. Feilen ble rettet etter cirka en halv time, men trafikken gikk da en stund med 50 prosent kapasitet. Luftkontrollsentralene kan i dag ikke uten videre ta over oppgavene for hverandre.

For lufthavnsystemet er det mange systemer som skal virke sammen, og selv svikt i «ikke-kritiske» systemer, som for eksempel bagasjebånd, kan få konsekvenser for passasjerene. I mai 2015 stoppet bagasjebåndene på Gardermoen opp, noe som medførte at reisende ble forhindret fra å sjekke inn. Svikten medførte forsinkelser på rundt tre timer.

EUs etablering av et felleseuropeisk luftrom (Single European Sky) er tuftet på fire forordninger og vil føre til store endringer for flysikringstjenesten i Norge. Hovedformålet med initiativet er å legge til rette for et europeisk luftrom som har økt kapasitet og er mindre oppstykket enn det som er tilfellet i dag. Avinor vil vurdere fjernstyrte tårn som et alternativ. En vellykket test av dette ble gjennomført i 2014 med sentral fjernstyring fra Bodø kontrollsentral for lufthavnene Værøy og Røst.

Den økende utbredelsen av droner åpner luftrommet for mange typer ny bruk og nye brukere. Det kan føre til økt risiko og sårbarhetsutfordringer som følge av utilsiktede hendelser og ved at aktører kan ha som hensikt å gjøre skade. Droner utfordrer luftfartssikkerheten ved at de kan komme i konflikt med andre fartøy eller skade mennesker og verdier på bakken. Styringssystemer og kommunikasjonslinjer har vist seg å være sårbare for feil, og det finnes en mengde eksempler på at operatører har mistet kontrollen over droner på grunn av IKT-svikt eller mangel på ferdigheter.

18.3.4 Luftfartens avhengighet av ekom og satellittbaserte tjenester

Luftfartstjenesten er svært avhengig av velfungerende elektronisk kommunikasjon og IKT-systemer for øvrig. Det er mulig å drive trafikkavvikling selv om enkelte av funksjonene skulle svikte, blant annet ved å operere via forhåndsplanlagte prosedyrer, men effektiviteten i trafikkavviklingen vil da kunne bli svært lav.

Hendelsen 23. mai 2011 som medførte kabelbrudd i viktige forbindelser i Telenors nett, gjorde at flytrafikken mellom Bodø og henholdsvis Trondheim lufthavn, Værnes og flyplassene i Møre og Ørland måtte settes på vent. Etter en times tid fikk Avinor satt i gang sitt reservesystem, og luftrommet kunne åpnes igjen. Isolert sett førte ikke hendelsen til større samfunnsmessige problemer, men denne type hendelser kan få konsekvenser for næringslivet, det offentlige og den enkelte. Skjer en svikt på et uheldig tidspunkt i en pågående trafikkavvikling, kan utfallet bli svært alvorlig. Avinor har redundante føringsveier og kjøper ekomtjenester fra ulike leverandører.

Det er en stor og økende avhengighet av GPS-baserte tjenester og satellittkommunikasjon. I dag er det ikke alle luftfartøy som har aktive antikollisjonsmekanismer, derimot har de passive varslingssystemer. I fremtiden vil dette bildet kunne endre seg. Den gradvise innføringen av satellittbasert flynavigasjon i Europa skjer innenfor rammen av Single European Sky (SES). SESAR (Single European Sky ATM Research) er EUs forsknings- og utviklingsprosjekt for innføring av nye administrative, operative og teknologiske konsepter for en mer effektiv utnyttelse av europeisk luftrom. I SESAR vil posisjonsdata fra satellittsystemer brukes til navigasjon, trafikkovervåking og tjenester ved lufthavnene. I tillegg vil satellittsystemer bli brukt som tidsreferanse for synkronisering av systemer for flykontroll (Air Traffic Management, ATM) og flybåren avionikk.[15] USA og EU samarbeider om å harmonisere moderniseringen av

[15] Norsk Romsenter (2013): *Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur.*

ATM. Sammenlignet med aldrende radarsystemer og gammeldags luftkontroll vil en ny infrastruktur basert på GPS, automatisk kringkasting av posisjon (ADS-B) og IP-basert telekommunikasjon for luftfarten kunne bidra til bedre integrasjon mellom luftfartøy og bakkebaserte systemer. Forstyrrelser av GPS-signaler eller forfalskning av lokasjonsinformasjon vil imidlertid kunne degradere overvåkingsnøyaktigheten, og den økte integrasjonen gjør det mulig å spre skadevare og utføre tjenestenektangrep.[16]

18.4 Sjøtransport

Maritim sektor har oppnådd en vesentlig rasjonalisering og forbedring av tjenestene ved å ta i bruk digital teknologi. Et moderne skip er avhengig av en rekke digitale systemer for navigasjon, motorkontroll, lastkontroll, sikkerhet og kommunikasjon. Offshoreflåten er for eksempel avhengig av kompliserte systemer for dynamisk posisjonering. Logistikk knyttet til vare- og passasjertransport er helt avhengig av sentrale IKT-systemer og kommunikasjon mellom et stort antall aktører. Fiskeri- og kystdepartementet har utpekt 5 av totalt 32 stamnetthavner som anses som særlig viktige for å utvikle en effektiv og sikker sjøtransport av personer og gods. Transport av varer med skip og import/eksport av disse varene via landets havner utgjør en kritisk funksjon i samfunnet.

Det transporteres store mengder farlig last, og ulykker med for eksempel eksplosiv last kan gi store skader på helse og miljø. De verst tenkelige tilfellene er kollisjon mellom skip der menneskeliv går tapt, eller der store miljøødeleggelser er konsekvensen.

Maritim sektor har investert i sikkerhet og beredskap med tanke på ulykker som grunnstøting, brann, eksplosjon med mer. Det er investert i fysisk sikring av blant annet havneområder, men mindre i sikkerhet med tanke på digitale sårbarheter.

Utvalgets omtale av sjøtransport er i sin helhet basert på rapporten «Digitale Sårbarheter Maritim Sektor (DNV GL)», se elektronisk vedlegg.

18.4.1 Roller og ansvar

Ansvaret for implementering av det internasjonale regelverket for maritim sikring i Norge er delt mellom Samferdselsdepartementet (SD) og Nærings- og fiskeridepartementet (NFD). Kystverket har ansvar for havner og havneanlegg, og Sjøfartsdirektoratet har ansvar for skip og personell om bord. Det er et stort antall aktører i sektoren, og med ulik IKT-infrastruktur. Noen rederier har tilstrebet like IKT-løsninger på sine skip for å forenkle bruken og vedlikeholdet.

Det finnes en rekke interesseorganisasjoner som blant annet er involvert i samarbeidet mellom næring og myndigheter. *Norges Rederiforbund* er en interesse- og arbeidsgiverorganisasjon for norsktilknyttede bedrifter innen skipsfart og offshore entreprenørvirksomhet. Rederiforbundets medlemmer sysselsetter over 55 000 sjøfolk og offshorearbeidere fra mer enn 50 forskjellige nasjoner. Rederiforbundet har en sentral rolle i samarbeidet mellom rederi og myndigheter. *Norsk Havneforening* er en medlems- og interesseorganisasjon med 47 medlemshavner langs hele norskekysten. Foreningen arbeider med havnenes rammevilkår ved å jobbe med myndigheter og næringsaktører, samt ved å samarbeide med andre organisasjoner og aktører.

18.4.2 Hjemmelsgrunnlag og tilsynsvirksomhet

Det internasjonale regelverket for maritim sikring er gjort gjeldende i norsk rett gjennom forskrift om sikring av havneanlegg, forskrift om sikring av havner og forskrift om sikkerhet, pirat- og terrorberedskapstiltak og bruk av maktmidler om bord på skip og flyttbare boreinnretninger (sikkerhetsforskriften fra Sjøfartsdirektoratet).

De nevnte forskriftene gjennomfører EU-forordning 725/2004, om forbedret sikkerhet for fartøyer og havneanlegg. Forordningen gjelder fullt ut som norsk forskrift, og brukerne må derfor forholde seg til kravene i denne direkte. SOLAS-konvensjonen[17] kapittel XI-2 og ISPS-koden (International Ship and Port Facility Security Code) er vedlegg til forordning 725/2004. Forordningen gjør ISPS-koden del A obligatorisk i alle EUs medlemsland, i tillegg til at enkelte av bestemmelsene i del B også gjøres obligatoriske.

ISPS er en utvidelse av SOLAS-konvensjonen om sikkerhet for personell og skip på sjøen. ISPS-koden trådte i kraft i 2004 og angir hvilke ansvarsområder forskjellige parter har for å detektere og

[16] Sampigethaya et al. (2011): *Future E-Enabled Aircraft Communications and Security: The Next 20 Years and Beyond, Proceedings of the IEEE* | Vol. 99. No. 11.

[17] Titanic-ulykken for over 100 år siden satte søkelyset på sikkerhet innen maritim sektor. Dette var forløperen til at den første internasjonale konvensjonen om sikkerhet til sjøs, SOLAS (Safety of Life at Sea), ble utarbeidet.

hindre sikkerhetstrusler mot skip og havner som brukes til internasjonal handel. Regelverk etter ISPS-koden gjelder uavhengig av flagg, farvann, eier med mer.

Forskrift nr. 538, om sikring av havneanlegg, og forskrift nr. 539, om sikring av havner, etablerer et begrep om sikringsnivå for havner og havneanlegg. Tilsvarende etablerer forskrift nr. 972, om sikkerhet og terrorberedskap om bord på skip, et tilsvarende begrep om beredskapsnivå for skip. Denne graderingen gjør det mulig å tilpasse sikringstiltak til den gjeldende trusselsituasjonen. Myndighetene kan beslutte å sette i verk et forhøyet beredskapsnivå. Kystverket fastsetter det maritime sikringsnivået som havner og havneanlegg skal operere på. Skip som befinner seg i disse eller i norsk farvann, må forholde seg til dette sikringsnivået uavhengig av flagg. Sjøfartsdirektoratet fastsetter sikringsnivået for skip under norsk flagg, gjerne knyttet til spesielle farvann. Ingen av forskriftene nevner digitale sårbarheter eller IKT-sikkerhet spesielt.

Sikkerhetsforskriften fra Sjøfartsdirektoratet krever at det skal utarbeides en sårbarhetsvurdering (Ship security assessment, SSA) som beskrevet i ISPS-koden del A seksjon 8, og en sikkerhets- og terrorberedskapsplan (Ship security plan, SSP) som beskrevet i ISPS-koden del A seksjon 9. Når det er verifisert at fartøyet oppfyller kravene i forskriften og i den godkjente sikkerhets- og terrorberedskapsplanen, utsteder Sjøfartsdirektoratet eller klasseinstitusjonen (såkalt RSO) et internasjonalt sikkerhets- og terrorberedskapssertifikat (ISSC). Dette har en gyldighet på fem år med forutsetning om en mellomliggende verifikasjon mellom andre og tredje år.

Et minstekrav til sikkerhetsvurderingen i henhold til ISPS-kodens del A, seksjon 8 er at den skal identifisere: eksisterende tiltak, operasjoner det er særlig viktig å beskytte, mulige trusler og deres sannsynligheter, samt sårbarheter. ISPS koden nevner ikke digitale sårbarheter spesielt, men kravene til en sikkerhetsvurdering er formulert generelt slik at digitale sårbarheter også omfattes av forskriften. Dette kravet om sårbarhetsvurdering og sikringsplan gjelder også for havner og havneanlegg.

Kystverket og Sjøfartsdirektoratet fører ikke tilsyn med IKT-sikkerhet i maritime selskaper. Rederiene har uttrykt at de ikke ønsker et detaljert regelverk og tilsynsregime for digitale sårbarheter, men foretrekker en risikobasert tilnærming.

18.4.3 Beredskap og hendelseshåndtering

Det er ikke kjent at norsk maritim sektor har vært berørt av alvorlige hendelser knyttet til digitale sårbarheter, men flere mindre hendelser er identifisert, og alvorlige hendelser har inntruffet i andre land. Det er kjent hvordan ondsinnet modifikasjon av navigasjonssignaler og identifikasjonssignaler kan medvirke til grunnstøting og kollisjon.

Maritim sektor er en foregangssektor når det gjelder beredskapsplaner og øving av beredskap. Offshoreskip ligger kanskje lengst fremme på dette området innenfor skipsfarten. Dette arbeidet fokuserer på utilsiktede hendelser som grunnstøting, havari og brann. Disse planene har i liten grad innarbeidet digitale sårbarheter, og det er ikke identifisert øvelser som involverer slike hendelser. Det er etablert globale rutiner for varsling av hendelser eller systembortfall som kan gi fare for navigasjonssikkerhet (NAVTEX- og NAVAREA-meldinger).

Det øves på å styre skip «manuelt» ved bortfall av industrielle automasjons- og kontrollsystemer, men systemene blir mer og mer avhengige av slike systemer. Det er tvilsomt om en flytende oljeplattform lar seg styre uten et funksjonelt DP-system (dynamiske posisjoneringssystemer). Det øves på utfall av elektroniske navigasjonssystemer, og enkelte rederier opplyser at de har beredskapsplaner for noen kritiske systemer.

18.4.4 Digitale sårbarheter innen sjøtransport

Ettersom maritim sektor i stor grad benytter IKT, er sektoren også eksponert for digitale sårbarheter. Det benyttes i stor grad trådløse datanett i sektoren, sektoren er global, og det kan forventes industrispionasje, jf. hendelsen mot Ulstein Gruppen. Sjøtransporten er avhengig av en rekke systemer basert på digital teknologi:

- globale posisjoneringssystemer (GNSS)
- elektroniske kart og informasjonssystemer (ECDIS)
- automatisk identifisering av skip (AIS/LRIT)
- nettverksbaserte kontrollsystemer om bord for blant annet styring og fremdrift
- radiokommunikasjon (satellitt, MF/HF, VHF, UHF, mobiltelefon, kabel (i havn))
- datakommunikasjon (primært via satellitt)
- administrative systemer (rapportering til myndigheter, rederi, lasteier med flere)
- landbaserte systemer for administrasjon av havneanløp, last, passasjerer med mer

Underholdning og velferdstilbud om bord på skip medfører nye sårbarheter. Noen skip har fysisk adskilte nett, mens andre har virtuelt adskilte nett. Det er varierende kvalitet på separasjonsmekanismene, ofte er det bare enkle brannveggfunksjoner. Se for øvrig omtale i punkt 18.3 «Luftfart».

18.4.4.1 Navigasjons- og posisjoneringssystemer

Navigasjonsulykker (kollisjon, grunnstøting, kontaktskade) utgjør omtrent 50 prosent av alvorlige skipsulykker. Slike ulykker kan få store konsekvenser, spesielt ved passasjertransport og ved transport av farlig last. Norskekysten har mange leder som er trange og krever presis navigering med hyppige kursendringer. Det er også betydelig transport av farlig eller forurensende last, blant annet i forbindelse med oljevirksomheten. Seilaser i Norge med forhøyet risiko er generelt underlagt losplikt, noe som reduserer mulige konsekvenser av sårbarheter i digitale systemer.

Globale posisjoneringssystemer spiller en stor rolle ved navigasjon. Det amerikanske GPS-systemet har flere kjente sårbarheter. Signalene kan forstyrres (jamming), signalene kan modifiseres (spoofing), og amerikanske myndigheter kan degradere ytelse eller i spesielle tilfeller slå av tjenesten. Passasjerer kan med enkelt og rimelig utstyr forstyrre GPS-signaler om bord. Tester med GPS-blokkering (jamming), utført av The General Lighthouse Authorities of the United Kingdom and Ireland, viser at utfall av GPS-tjenester har betydelige konsekvenser for maritim sikkerhet.

Konsekvensene av utfall av eller feil på globale posisjoneringssystemer kan være store for eksempelvis offshorefartøy som holder posisjon tett inntil oljeinstallasjoner. For navigasjon i ledene langs kysten i god sikt er konsekvensene mindre. Undersøkelser blant seilende navigatører viser at observasjon av land og navigasjonsinnretninger visuelt eller ved hjelp av radar, eventuelt også med los, er den viktigste navigasjonsmetoden. Denne metoden brukes oftest i kombinasjon med elektronisk stedfesting på elektroniske kart. Navigasjon basert på informasjon fra to separate kilder som kontinuerlig verifiseres opp mot hverandre, anses som «best practice». Det er da viktig at begge kildene fungerer, men det blir ikke sikkerhetsmessig kritisk før begge kildene svikter samtidig.

I et eksperiment fra 2013 viste forskere ved University of Texas (Austin) hvordan GPS-modifikasjon (spoofing) kan påvirke et fartøys navigasjon. Om bord i skipet ble en innretning på størrelse med en koffert brukt for å sende falske signaler til skipets GPS-mottakere. Skipets navigasjonssystem var ikke i stand til å avsløre at signalene var falske. Mannskapet ble lurt til å korrigere kursen i henhold til de falske GPS-signalene, og skipet kom ut av kurs uten at det ble oppdaget. Utstyret som ble brukt, kostet cirka 20 000 kroner å produsere.

GPS-sporsystemer benyttes til lokalisering og overvåking av last (containere) i transportkjeden. Dette gir forutsigbare ankomsttider og kan virke avskrekkende på potensielle tyver. Sporsystemet inneholder også informasjon om type last. En jammer kan «gjemme» containeren.

Det finnes flere eksempler på at overdreven tillit til digitale navigasjonssystemer kan medvirke til å svekke årvåkenheten hos navigatøren eller skipsføreren. Dette forsterker konsekvensen av angrep rettet mot slike systemer. En mulig fare er at operatørene enten ikke merker at et system er satt ut av spill, eller at de ikke er godt nok forberedt til å ta i bruk alternative navigasjonsmidler. For ytterligere omtale av sårbarheter knyttet til satellittbaserte tjenester, se kapittel 12 «Satellittbaserte tjenester».

18.4.4.2 Elektroniske kart- og informasjonssystemer

Electronic Chart Display and Information System (ECDIS) er et navigasjonsinformasjonssystem som oppfyller krav fastsatt av Den internasjonale sjøfartsorganisasjonen (IMO). ECDIS kan benyttes som lovlig erstatning for papirkartet dersom

Boks 18.4 USS Guardian

Den 17. januar 2013 grunnstøtte minesveiperen USS Guardian på Tubbataha-revet ved Filippinene. En granskingsrapport fant ingen enkeltårsak til hendelsen, men konkluderte med at ulykken kunne vært unngått og var et resultat av «poor voyage planning, poor execution and unfortunate circumstances». Spesielt påpekes det at for stor tillit til elektroniske kart var en medvirkende årsak: «The leadership and watch teams relied primarily on an inaccurate Digital Nautical Chart (DNC)® coastal chart during planning and execution of the navigation plan.» Selv om denne hendelsen skyldtes menneskelig svikt og ikke ondsinnede handlinger, viser den at den store tilliten til slike systemer er en risikofaktor.

Boks 18.5 Digitale kart og ECDIS

En ECDIS-arbeidsstasjon tar inn navigasjonsdata fra en rekke sensorer som sammen med elektroniske kart gir et kraftig navigasjonsverktøy. Siden ECDIS er et knutepunkt som kobler sammen mange navigasjonssystemer, vil en angriper som får tilgang til ECDIS, ha mange muligheter til å villede navigatøren: modifisering av sensordata slik at operatøren får et feilaktig bilde, manipulasjon/tyveri av elektroniske kart eller bruk av ECDIS som et tilgangspunkt for videre inntrenging. Sikkerhetsfirmaet NCC Group har vist at man kan trenge inn i ECDIS-systemer ved hjelp av enkle teknikker.

det brukes offisielle kartdata som er produsert etter gitte internasjonale standarder og kravspesifikasjoner. I tillegg må en ha et godkjent backupsystem. Det betyr at man må ha to ECDIS-er om bord som er tilknyttet hver sin strømkilde. Det stilles også krav om at et ECDIS skal være typegodkjent.

Et ECDIS skal vise all sjøkartinformasjon som er nødvendig for sikker og effektiv navigasjon, og data skal være levert og godkjent av en autorisert sjøkartmyndighet. I Norge er Kartverket sjøkartmyndighet, og deres sjødivisjon leverer og godkjenner sjøkartdataene.

Elektroniske kart- og informasjonssystemer må holdes løpende oppdatert. Dette skjer ved bruk av minnepinner, CD-er, e-post eller nettbaserte tjenester. Under oppdatering kan det spres virus, og det kan bli lagt inn tilsiktede og utilsiktede feil i kart og informasjon. I ett kjent tilfelle manglet nye nedlastede kart dybdeinformasjon.

18.4.4.3 Identifikasjonssystemer

Automatisk identifikasjonssystem (Automatic Identification System, AIS) er et antikollisjonshjelpemiddel for skipsfarten. Fartøyer som har utstyr for AIS om bord, sender ut og utveksler informasjon om sin identitet, posisjon, fart, kurs og så videre over frekvenser på VHF-båndet. AIS brukes også av maritime trafikksentraler for å holde oversikt over skipstrafikken innen egne ansvarsområder.

Rekkevidden varierer, men kan være på opptil 40 nautiske mil. Etter krav fra IMO skal fartøyer over 300 brutto registertonn i internasjonal fart ha utstyr for sending og mottak av AIS-signaler. Med visse unntak har de aller fleste skip i dag AIS, og det anslås at over 40 000 skip har AIS-utstyr klasse A om bord.

En kjenner ikke til tilfeller der modifiserte AIS-signaler har ført til ulykker, men manipulerte AIS-signaler kan medføre kollisjonsfare selv om en bemannet bro skal reagere på slike hendelser. Trafikksentraler benytter informasjon om dypgang i AIS-signalene for å dirigere fartøy. Modifiserte data om dypgang kan føre til grunnstøting. Modifiserte AIS-signaler er ikke lett synlige for brukeren og kan gi feilaktige vurderinger av den aktuelle kollisjons- og/eller grunnstøtingsrisikoen og derigjennom bidra til en gal beslutning. Falske AIS-signaler kan brukes til å skjule identiteten til

Boks 18.6 Digitale sårbarheter ved AIS

AIS er sårbart fordi systemet i liten grad er designet med tanke på digitale sårbarheter. Det er ingen kontroll av autentisiteten til meldinger og heller ingen kryptering. I en sikkerhetsevaluering utført av Trend Micro i 2013 ble det vist hvordan AIS kan angripes. Med enkelt utstyr kunne en angriper blant annet

- endre all AIS-informasjon som sendes ut fra et fartøy
- forfalske fartøysinformasjon, slik at ikke-eksisterende skip blir oppfattet av andre som faktiske fartøy, eller for å igangsette operasjoner med søk- og redningsfartøy (SAR), herunder helikoptre
- generere falske værmeldinger
- utløse falske kollisjonsvarsler (CPA)
- utgi seg for å være sjøfartsmyndigheter for å kunne manipulere mannskapet på fartøyet
- sende ut falske mann-over-bord-meldinger (SAR) for å lure et fartøy inn i et fiendtlig område
- iverksette ulike former for tjenestenektangrep for å hindre legitim AIS-trafikk

Realisering av én av disse handlingene eller flere i kombinasjon kan ha ulike og omfattende konsekvenser.

et skip. AIS-data er tilgjengelige på åpne websider og fra mobile applikasjoner (apper). Dette utgjør en sårbarhet ved at «alle» kan kjenne til et skips identitet, dimensjoner, hastighet med mer.

Den viktigste egenskapen til AIS er en veldig nøyaktig tidssynkronisering som muliggjør en selvorganiserende datalink mellom alle AIS-mottakere. Tidssynkroniseringen til AIS baserer seg på GPS' atomklokker. Bortfall av GPS-tid (UTC) vil dermed også stenge ned AIS. I dag er det kun VHF og radar som er alternativene for identifikasjon av fartøyer i antikollisjonsøyemed, med LRIT som «strategisk» ID-kilde for myndighetene. For ikke-landnære områder ble et satellittbasert langdistansesystem for identifisering og sporing av fartøy (LRIT) innført i Norge i 2009. Et alternativt (redundant) identifikasjonssystem blir tilgjengelig hvis/når infrastrukturen «Maritime Cloud» blir implementert.

18.4.4.4 Industrielle automasjons-, kontroll- og sikkerhetssystemer

Tradisjonelt har skip vært bygd med enkeltstående og autonome kontroll- og sikkerhetssystemer, der skipets viktige hovedfunksjoner (for eksempel fremdrift, styring, kraftproduksjon, dynamisk posisjonering, kran, ROV-systemer og ballastering) var kontrollert og overvåket av enkle, ikke-programmerbare systemer. Slike skip var i liten grad utsatt for fellesfeil som kunne påvirke flere hovedfunksjoner samtidig. Gjeldende internasjonale regelverk er basert på at skipets mannskap skal ha kapasitet, kunnskap og mulighet til å styre skipets hovedfunksjoner med enkle lokale og manuelle metoder dersom en feil skulle oppstå.

Som et resultat av den teknologiske utviklingen er imidlertid dagens skip høyteknologiske installasjoner som er avhengige av programmerbare og nettverksbaserte systemer. I tillegg blir skipets viktige automasjons-, kontroll- og sikkerhetssystemer i økende grad integrert med nettverksløsninger. Dette innebærer økt risiko for at digitale feil, skadeprogrammer og angrep vil kunne slå ut enkelte eller flere av skipets viktige funksjoner samtidig. Selv om skipet fremdeles skal kunne styres og kontrolleres lokalt/manuelt, vil dette i mange tilfeller være en krevende oppgave på grunn av manglende kunnskap, manglende øvelse, begrenset mannskap, kompliserte brukergrensesnitt, og så videre.

Næringen bruker systemer som i dag i stor grad er basert på kommersielt tilgjengelige komponenter som for eksempel PC-er med Microsoft Windows operativsystem. Det innebærer at kjente sårbarheter for slike kommersielle standardprodukter også vil være eksponert i sektoren. For å sikre seg mot slike sårbarheter må systemene løpende oppdateres med rettelser fra produsentene. Dette er utfordrende i maritim sektor fordi datakommunikasjonen til skipene kan ha begrenset kapasitet, og fordi oppdateringer som kan påvirke systemer som er i drift, må planlegges nøye og kanskje utføres når skipet ikke er i normal drift. Mange skip benytter digitale systemer som ikke har oppdaterte sikkerhetsrettelser.

18.4.4.5 Kommunikasjon

Logistikk-kjeden ved transport av varer og personer involverer et stort antall aktører og utstrakt bruk av usikret e-post. Blant annet utveksles passasjerlister, og ved en ulykke vil informasjon om skadede personer utveksles. Skadeinformasjon er sensitiv personinformasjon, og usikret e-post er ikke et medium som er egnet til dette.

Et stort antall aktører utveksler mye informasjon på e-post om skip, last og passasjerer.

Systemer for sikring av e-post har vært tilgjengelige over lang tid, men er i liten grad tatt i bruk, da systemene krever elektronisk ID og anskaffelse og bruk av slik ID oppfattes som svært tungvint. Løsningene har også primært vært tilrettelagt for person-til-person-kommunikasjon. Det arbeides med løsninger for selskap-til-selskap-kommunikasjon («Digipost for selskaper»).

Åpen kommunikasjon gjennom VHF har en sikkerhetsfunksjon som gjør at det er mulig å initiere kommunikasjon uten nærmere kunnskap om identiteten til den man vil kommunisere med, og ved at alle fartøy som er involvert i en trafikksituasjon, får tilgang til lik informasjon ved å overhøre kommunikasjon mellom andre skip eller mellom andre skip og vessel traffic service (VTS). Dette innebærer utfordringer med tanke på personvern, men også i forbindelse med utveksling av sikkerhetsinformasjon i havner, og så videre. I dag kommuniseres sensitiv informasjon mellom skip og aktører på land i stor grad ved hjelp av mobiltelefoni når fartøy er nær land, eller ved hjelp av satellittbasert telefoni til havs. Med utviklingen av små, håndholdte VHF-enheter har det oppstått en ny sårbarhet, nemlig at disse enhetene kan bli «liggende på sendeknappen» og dermed jamme oppkallings- og nødkanalen.

18.4.4.6 Kommandoforhold om bord kan medføre sårbarheter

Dersom en kaptein beordrer sammenkobling av systemer eller nett, er det vanskelig for en elektriker/servicetekniker å motsette seg dette ut fra sikkerhetsbetraktninger. Næringen har i liten grad IKT-teknisk personell ombord, og ofte gjøres IKT-teknisk vedlikehold av ikke-IKT-faglige personer. Skipene er derfor i stor grad avhengige av fjernarbeid utført av leverandører og landbaserte IKT-teknikere. De digitale systemene om bord muliggjør fjernvedlikehold, diagnostikk og oppdateringer over nett. Det betyr ofte at systemene åpnes for tilgang fra Internett, noe som også åpner for en rekke digitale sårbarheter. Det varierer hvor sterkt sikring mot dette blir vektlagt. Noen rederier har innført nøkkelbrytere for å kontrollere slik tilgang, men sektoren har i liten grad innført dedikerte systemer for kontroll. Ved et tilfelle resatte personell som utførte vedlikehold via en nettforbindelse, digitale systemer på feil skip.

Når skip ankommer havner, kommer det ofte servicepersonell og inspeksjonspersonell om bord. Kontrollen med identitet og kompetanse hos slikt personell varierer. Disse har ofte med seg minnepinner og lignende, som utgjør en sårbarhet ved at de kan installere feil programvare, spre ondsinnet kode eller utføre feilkonfigurasjon av systemer. Det er varierende fysisk sikring av serverrom, kommunikasjonsrom og kablingsskap på skip. Det er også varierende grad av merking av kabling. Spesielt på eldre skip kan datakabling for kritiske nett være tilgjengelig for mannskap og passasjerer. Dersom uautoriserte datamaskiner kobles til slike segmenter, innføres en rekke sårbarheter.

18.4.4.7 Sentrale systemer

Det benyttes i stor grad overvåkingssystemer (CCTV) både om bord i skip, i trange passasjer og i havn. Slike systemer samler mye informasjon som kan ha betydning både for personvern og for ondsinnede handlinger. Systemene kan settes ut av drift, og de kan benyttes til å innhente informasjon. Slike systemer er brukt for å stjele brukeridentiteter og passord. Det er varierende praksis for sikring av data og sletting.

Kystverket utvikler og drifter SafeSeaNet Norway som en felles nasjonal meldeportal for skipsfarten. Dette systemet er basert på det europeiske Single Window-konseptet, som anbefaler utviklingen av en nasjonal portal der fartøy, rederier og operatører kan sende inn rapporteringspliktig informasjon til nasjonale myndigheter kun én gang. Informasjonen skal videreformidles automatisk til nasjonale myndigheter for å forenkle og øke kvaliteten på den offentlige saksbehandlingen overfor maritime brukere. Informasjon om farlig eller forurensende last blir videreformidlet til det sentrale europeiske SafeSeaNet-systemet.

SafeSeaNet har en stor og variert brukermasse, og det er utfordrende å sikre god brukerautentisering. En utenforstående kan lage seg en falsk konto og både hente ut og registrere feilaktig informasjon. Blant annet ligger sikkerhetsinformasjon om skip i systemet. SafeSeaNet spiller en viktig rolle ved losformidling, meldinger om farlig gods, trafikkontroll, tollkontroll og grensekontroll. Bortfall av systemet eller feilaktig informasjon kan føre til at viktig informasjon ikke er tilgjengelig når kritiske situasjoner oppstår.

Barents Watch er et norsk overvåkings- og informasjonssystem som gir et oversiktsbilde av aktiviteter og tilstand i kyst og havområder. En åpen løsning finnes allerede og det arbeides med en adgangsbegrenset løsning. Barents Watch adgangsbegrensede del skal tjene som et system for utveksling av informasjon mellom etater med operativt ansvar i kyst- og havområdene.

18.4.4.8 Globale utfordringer

Etter angrepet på Twin Towers 11. september 2001 har det vært økt oppmerksomhet omkring mulige angrep som involverer passasjerskip og skip med farlig last. Den amerikanske kystvakten har en pågående vurdering av om de skal sette «cybersecurity»-krav til skip som anløper amerikanske havner.

EU fikk i 2011 utført en analyse som munnet ut i rapporten *Cyber Security Aspects in the Maritime Sector*. Noen av hovedfunnene i denne rapporten var at maritim bevissthet om informasjonssikkerhet («cyber security awareness») er lav og til dels ikke-eksisterende, og at eksisterende maritimt regelverk og policy kun fokuserer på fysisk sikkerhet og ikke tar informasjonsaspektet i betraktning. Dette kan overføres til norske forhold. Videre anbefales det at IMO og EU sørger for en harmonisering av regelverket, og at man bør forsøke å bygge plattformer for bedre informasjonsutveksling mellom medlemsstatene for dette domenet.

IMOs sjøsikkerhetskomité (Maritime Safety Committee) har satt i gang et arbeid for å se på behovet for retningslinjer for maritim cybersikkerhet under det stående agendapunktet «Measu-

res to enhance maritime security» etter initiativ fra Canada og USA. Maritim industri ved Intertanko, Intercargo, BIMCO og ICS arbeider med en egen industriveiledning for risikobasert håndtering av informasjonssikkerhet. Arbeidet med veilederen er gjort kjent for IMO, og MSC holdes informert og vil bli presentert det endelige dokumentet. Et lignende arbeid er satt i gang av IMOs Facilitation Committee.

IMO er en stor og tung organisasjon der utarbeidelse av nye retningslinjer tar lang tid. IMOs intensjon er å lage frivillige retningslinjer, mens EU gjør disse retningslinjene til obligatoriske krav.

18.4.5 Fremtidige problemstillinger og trender

IMO har vedtatt en strategiplan (MSC94) for implementering av e-navigasjon. Planen påpeker behovet for en autorisert kommunikasjonsinfrastruktur om bord i skip, mellom skip, mellom skip og land og mellom myndigheter og andre maritime interessenter. Denne «maritime skyen» («Maritime Cloud») er definert som «en kommunikasjonsinfrastruktur for effektiv, pålitelig og sømløs digital informasjonsutveksling mellom alle autoriserte maritime interessenter på tvers av alle tilgjengelige kommunikasjonssystemer».

Virtuelle seilingsleder erstatter bøyer og andre fysiske navigasjonsinnretninger med motsvarende virtuelle objekter som fremvises om bord på beslutningsstøttesystemer som ECDIS og RADAR. IALA/IEC har allerede utarbeidet standarder for presentasjon av virtuelle navigasjonsinnretninger (ikoner) på navigasjonsutstyr. Kystverket, som har ansvar for merking av ledene i dag, legger ikke opp til en slik utvikling i Norge.

Autonome og ubemannede skip anses som et element i en bærekraftig og konkurransedyktig (skips)industri i fremtiden. EU-prosjektet MUNIN undersøker både konseptet og teknologien som kreves for å operere et «industrielt autonomt skip» både kosteffektivt og sikkert i et reelt og kommersielt miljø.

Reassuransemarkedet innførte etter 11. september 2001 et unntak for bruk av datateknologi i skadelig hensikt, den såkalte Cyber Attack-klausulen (CL 380). I det internasjonale forsikringsmarkedet for maritime enheter (skip, rigger og så videre) gjelder CL 380 tilnærmelsesvis uten unntak.

Under krigsdekningen hos Den Norske Krigsforsikring for Skib dekkes tap og skade som oppstår på basis av bruk av datateknologi i skadehensikt, altså det CL 380 i hovedsak søker å ekskludere. Slik sett er norske skip og rigger bedre beskyttet enn resten av verdensflåten. Det er imidlertid en risiko for at norske skip og rigger kan bli utsatt for skadeverk gjennom hacking eller lignende som ikke omfattes av krigsforsikringen fordi angrepet ikke kan betegnes som sabotasje eller politisk motivert skadeverk. Skal skadeverket henføres til sivildekningen, vil det være et hull i dekningen. Med den praksis at denne risikoen ekskluderes under sivil kasko, vil det være en ikke ubetydelig udekket risiko for rederne/sikrede, ettersom slike risikoer bare i spesielle tilfeller vil være å regne som krigsfare etter CL 2-9.

18.5 Vurderinger og tiltak på tvers av transportsektoren

Samferdselssektoren har de siste årene blitt mer avhengig av IKT, og kompleksiteten i IKT-systemer og nett har økt. Utviklingen har ført til at sektoren er blitt mer sårbar overfor svikt og brudd i systemer og nett. Bortfall av IKT-tjenester kan få store konsekvenser for transportsikkerhet og pålitelighet, og utvalget mener at IKT-sikkerhet og -beredskap må være et grunnleggende innsatsområde innenfor sektoren.

Transportsektoren står blant annet overfor store og omfattende investeringer innen IKT. Disse prosjektene kjennetegnes av grenseoverskridende føringer, høy kompleksitet og store kostnader. Investeringer i dag skal være levedyktige i mange år fremover i tid, noe utvalget mener er utfordrende på et område der teknologien utvikler seg svært raskt samtidig som anskaffelsesregime og lovverk har en vesentlig lengre endringstakt.

Utvalget merker seg at sentrale trafikkstyrings- og kontrollsystemer innen vei, bane, luft og sjø kan svikte på grunn av både tilsiktede og utilsiktede hendelser. Dette vil kunne medføre konsekvenser for trafikkavvikling og kan i noen tilfeller true sikkerheten, spesielt hvis noen får kontroll over eller manipulerer styringssystemene.

Utvalget mener at transportsektoren derfor bør vie eksisterende og kommende digitale sårbarheter enda større oppmerksomhet, og at innsatsen, som følge av sektorens globale karakter, også må rettes mot internasjonale samarbeidsfora.

Nye, publikumsvennlige digitale løsninger for utførelse av offentlige tjenester vil i de fleste tilfeller inneholde personopplysninger samt kunne åpne for en tettere kobling mellom forskjellige

registre med ulike formål. Utvalget mener det er behov for å vurdere personvernspørsmål knyttet til sektorens systemer. Området er relevant i forhold til Den europeiske menneskerettighetskonvensjons (EMK) bestemmelser om fri bevegelse. Dette avhenger av om det blir obligatorisk å benytte systemene i praksis. Ikke å kunne bevege seg uten å legge igjen spor representerer et inngrep i borgernes rettigheter og friheter. Det er også nødvendig å se på hvem som har tilgang til opplysningene som lagres. Anonymiseringsmuligheter må vurderes ettersom mange hensyn kan ivaretas uten at man knytter opplysningene til person. Problemstillingene må ses i sammenheng med utkontraktering, i og med at mange av «eierne» av informasjonen (transportselskaper, billettselskaper og så videre) hører hjemme i andre jurisdiksjoner. Formålsglidning er en sentral problemstilling jf. kapittel 11 «Elektronisk kommunikasjon».

Utvalget foreslår følgende tiltak:

18.5.1 Styrke IKT-tilsyn og samarbeid mellom transportgrenene

Samtlige transportgrener opplever en trend der digitaliseringen skyter fart og sektoren skal igjennom store endringer. Utvalget ser blant annet med bekymring på økende systemintegrasjon og kompleksitet, som også rammer styringssystemer. Utvalget er gjort kjent med eksempler på manglende kontroll av kritiske styringssystemer, blant annet knyttet til fysisk skille («air gap») mellom et kritisk IKT-system og kunderettede tjenester, for eksempel om bord i fly eller skip. Dette er en internasjonal problemstilling, og det forutsettes at tilsynsmyndighetene har tilstrekkelig kompetanse og kapasitet til å kunne påvirke i relevante internasjonale fora.

Transportbransjen kjennetegnes av en pågående og økende privatisering og internasjonalisering, noe som medfører en rekke utfordringer, særlig for myndighetenes krisehåndtering. Eie- og leieavtaler er i kontinuerlig endring. Det er en utfordring for krisehåndtering at tjenesteproduksjonen i stor grad håndteres av underleverandører og dermed styres gjennom kommersielle avtaler.[18] *Utvalget vil anbefale at sektoren går igjennom beredskapsplanene og sjekker disse opp mot digitale sårbarheter og reserveløsninger. Beredskapsplanverket må også ha planer for å håndtere digitale kriser der leverandører befinner seg utenfor Norges grenser.*

Samferdselssektoren gjør et omfattende arbeid med risikoanalyser. Utvalget har observert at IKT og digitale sårbarheter i mindre grad er inkludert i dette arbeidet. Utvalget er imidlertid kjent med at det pågår diskusjoner om etablering av et samarbeidsforum mellom transportetatene.

Det er behov for ressurssterke tilsynsmyndigheter som kan følge med på den internasjonale utviklingen og gi norske innspill. Dette forutsetter at myndighetene har hjemmel og makt i tilsynsarbeidet sitt. I tilfeller der tilsynsmyndigheten mangler hjemler, bør det settes i gang et arbeid med å gi myndigheten dette der det er mulig. Et slikt initiativ er blant annet gjort innenfor skinnegående transport. Utvalget vil også fremheve myndighetenes veiledningsrolle som vesentlig, samt samarbeid og informasjonsutveksling både internt i sektoren og med andre tilsynsmyndigheter på IKT-området.

Utvalget anbefaler at Samferdselsdepartementet styrker tilsynsmyndighetene innenfor transportsektoren innen IKT-sikkerhet. Tilsynsmyndighetene må ha kapasitet og kompetanse til å føre tilsyn med og veilede virksomheter på norsk territorium, samt bidra i internasjonale fora.

18.5.2 Etablere en felles rapporteringskanal for IKT-hendelser innen transportsektoren

Utvalget vurderer at det er behov for en felles rapporteringskanal både fra myndighetene til sektoren og fra sektoren til myndighetene når det gjelder IKT-hendelser. Når for eksempel NSM NorCERT detekterer en økning av Internett-baserte angrep mot sektoren, må alle relevante aktører i sektoren kunne varsles.

Et alternativ kan være at sektoren etablerer en egen CERT-tjeneste, men det er uklart hvem som eventuelt skal etablere og finansiere denne, også gitt den globale dimensjonen for flere av transportgrenene. Utvalget observerer at Samferdselsdepartementet hittil har overlatt denne diskusjonen til underlagte etater. *Utvalget mener at Samferdselsdepartementet bør utrede hvordan rapportering av IKT-hendelser bør ivaretas for sektoren.*

18.5.3 Særskilte tiltak for sjøtransport

Den maritime sektoren er svært avhengig av digitale systemer for å ivareta sjøsikkerhet og effektivitet. Maritim sektor omfatter mange aktører, også et globalt arbeidsmarked der utenlandske

[18] Samferdselsdepartementet (2010): *Krisescenarioer i samferdselssektoren – KRISIS.*

sjøfolk arbeider på skip som seiler i norske farvann. Maritim sektor er en global industri underlagt internasjonale konvensjoner og regelverk. Dette setter rammer for hva norske myndigheter selv kan gjøre. Utvalget observerer at ulike myndigheter har et ansvar i en kompleks verdikjede i sjøfarten, samtidig som det mangler en myndighet med et helhetsblikk på digitale sårbarheter i hele verdikjeden.

Etablere helhetsoversikt over IKT-sikkerheten i maritime verdikjeder

Utvalget vil anbefale at Kystverket gis et overordnet ansvar for å ha en helhetsoversikt over IKT-sikkerheten i maritime verdikjeder og gi råd til departementet om prioriteringer som gjelder digitale sårbarheter i verdikjeden. Det inkluderer en digitalisert maritim infrastruktur langs kysten og i farleder og IKT-sikkerhet om bord i fartøy og for maritimt personell. Rollen tilsvarer den som Petroleumstilsynet er gitt på petroleumsområdet. Rollen endrer ikke ansvaret Sjøfartsdirektoratet har for skip og maritimt personell, eller Nkoms ansvar for elektronisk kommunikasjon.

Tilrettelegge for sikring av identitet

Det er en uløst problemstilling internasjonalt knyttet til sikret digital utveksling av passasjer- og mannskapsinformasjon, last- og kundedata. *Utvalget anbefaler Samferdselsdepartementet, i samarbeid med andre relevante myndigheter, å ta initiativ for å finne en løsning på dette internasjonalt.*

Del IV
Tverrsektorielle forhold

Kapittel 19
Kompetanse

For å kunne delta i en stadig mer digital hverdag er det en forutsetning å ha grunnleggende kunnskap om bruk av IKT. Dette gjelder først og fremst kjennskap til funksjonalitet, men også hvordan man forholder seg i møte med digitale trusler og sårbarheter. Selv om dagens IKT-systemer har en økende grad av innebygde løsninger som skal ivareta brukerens integritet og sikkerhet, har dette liten verdi dersom brukeren enten ikke vet hvordan slike løsninger skal brukes, eller bevisst velger å omgå dem.

Dette kapittelet omhandler kunnskap og ferdigheter som må utvikles, videreformidles og fordeles i samfunnet for å sikre tryggest mulig bruk av IKT. Hva slik kunnskap skal inneholde, vil avhenge av hvem mottageren er. For eksempel må befolkningen i sin alminnelighet vite hvordan man bruker IKT på en sikker måte, både privat og i jobbsammenheng, mens fagarbeidere og spesialister innen IKT må ha spesifikk kunnskap om hvordan man forebygger og håndterer digitale trusler. Slik kunnskap inkluderer også spisskompetanse innenfor utvalgte og særlig kritiske områder. Samtidig må ledere og beslutningstagere i bedrifter og etater ha tilstrekkelig kompetanse til å kunne allokere nødvendige ressurser for å sikre at IKT-sikkerheten blir ivaretatt i egen organisasjon.

Kunnskap om IKT blir blir først og fremst formidlet gjennom opplæring og utdanning. Utvalget har primært fokusert på den offentlige utdanningsdelen som er ment å dekke disse behovene. Utdanningsløpet starter i barnehage og grunnskole og går gjennom videregående utdanning og opp til både generelle IKT-utdanninger og spesialistutdanninger innenfor IKT-sikkerhet. Den grunnleggende utdanningen er primært vurdert med tanke på innhold, mens det for de mer spesialiserte utdanningene også er vurdert om volumet er tilstrekkelig til å dekke nåværende og fremtidige behov. Siden opplæring av eksperter innen IKT-sikkerhet er nært knyttet til forskning og utvikling (FoU), behandler dette kapittelet også den nasjonale FoU-aktiviteten innenfor området. Utvalget avgrenser mot sektorspesifikke utdanningsbehov i dette kapittelet. Øvelse er et vesentlig element i kompetanseoppbygging i virksomheter, og er behandlet under samfunnsfunksjonene i del III «Sårbarheter i kritiske samfunnsfunksjoner».

IKT-sikkerhetskompetanse omtales i det følgende som et samlebegrep som dekker både kunnskap om hvordan man gjør IKT-system robuste mot utilsiktede hendelser, samt også hvordan man beskytter slike system mot tilsiktede angrep.

IKT-sikkerhetskompetanse bygger på flere fagdisipliner: Teknisk IKT-sikkerhet bygger på generell teknisk basisforståelse[1] og kan for eksempel være en spesialisering i programvaresikkerhet, nettverkssikkerhet, kryptografi, kartlegging av sårbarheter over nettverk og skadevareanalyse. IKT-sikkerhet innenfor ledelse og administrasjon kan for eksempel være kompetanse innen hendelseshåndtering og digital risikostyring. Innen juss og kriminalitetsbekjempelse har vi datatekniske undersøkelser, forvaltningsinformatikk og medierett, og innen samfunnsfagene står digital rettsstatsutvikling, overvåking og personvern sentralt.

19.1 Sentrale dokumenter

Sårbarhetsutvalget[2] fra 2000 omhandlet det norske samfunnets sårbarheter med utgangspunkt i et ønske om å styrke samfunnets sikkerhet og beredskap. Utvalget hevdet at Forskningsrådet, som er ansvarlig for strategisk rådgivning overfor departementene, ikke hadde tatt ansvaret for å kanalisere offentlige midler til sikkerhetsfors-

1 Som for eksempel matematikk og logikk, forståelse for kretser, mikroprosessorer, operativsystemer, programmering, databaser og nettverksprotokoller. Inngår i fagretninger som teleteknikk, datateknikk og informatikk (computer science).

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

kning. Konsekvensen av dette var at sikkerhetsforskningen rundt årtusenskiftet var kortsiktig og fragmentert, og at fornyelse og nytenkning ut fra blant annet IKT-revolusjonen ble forhindret.

Sårbarhetsutvalget mente videre at både næringsliv, forvaltning og utdanningsinstitusjoner raskt ville kunne havne i en kompetanse- og rekrutteringskrise på sikkerhetsområdet dersom det ikke kom en ny satsing på sikkerhetsforskning. Utvalget anbefalte blant annet at ett departement måtte ta ansvaret for sikkerhetsforskning i stort og for prioritering av privat–offentlige sektorovergripende forskningsprogrammer.

Infrastrukturutvalget[3] leverte i 2006 en utredning som kartla virksomheter med betydning for rikets sikkerhet og vitale nasjonale interesser (kritisk infrastruktur), og fulgte opp Sårbarhetsutvalget med å si: «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.»

Nasjonal strategi for informasjonssikkerhet, med tilhørende handlingsplan, fra 2012 angir retninger og prioriteringer som skal ligge til grunn for myndighetenes informasjonssikkerhetsarbeid. «Høy kompetanse og fokus på forskning om informasjonssikkerhet» er angitt som ett av de fire overordnede målene. To av de sju strategiske prioriteringene er særlig relevante: «kontinuerlig innsats for bevisstgjøring og kompetanseheving» og «høy kvalitet på nasjonal forskning og utvikling innenfor informasjons- og kommunikasjonssikkerhet». I den tilhørende handlingsplanen er Samferdselsdepartementet bedt om å videreføre nettvett.no, Justis- og beredskapsdepartementet er bedt om å videreføre tilskuddet til Norsk senter for informasjonssikring (NorSIS), Kunnskapsdepartementet skal følge opp at det gis støtte til personvern og informasjonssikkerhet i grunnopplæringen, og Kommunal- og moderniseringsdepartementet fikk i oppgave å etablere et kompetansemiljø for informasjonssikkerhet i statsforvaltningen. Det var også tiltak knyttet til Forskningsrådets nye IKT-satsing IKTPLUSS, som er en videreføring av VERDIKT-programmet.

Nasjonal strategi for IKT-forskning og -utvikling[4] er utarbeidet av det tidligere Forbruker- og administrasjonsdepartementet, nå Kommunal- og moderniseringsdepartementet, på vegne av regjeringen. Strategien gjelder for perioden 2013–2022. Informasjonssikkerhet er nevnt som én av tre store samfunnsutfordringer innen IKT-forskning og -utvikling: «Regjeringa meiner det er av særskilt nasjonal interesse at vi har innanlands kompetanse og eigne forskingsmiljø innanfor informasjonstryggleik». Strategien viser til små og fragmenterte forskningsgrupper innen offentlig IKT-forskning i Norge og manglende langsiktig forskningsstøtte. Regjeringen ønsket at Forskningsrådet skulle fortsette med en sterk satsing innen IKT, og at Norge skulle delta i EUs rammeprogram Horisont 2020 som fullverdig medlem.

Digitutvalget[5] mente i 2013 at digitale ferdigheter i grunnskole og videregående skole i liten grad har blitt et mål i seg selv, men fremstår som et virkemiddel for å oppnå de andre læringsmålene. Med det menes at vekten nesten ensidig er på kommunikasjon og presentasjon, fremfor utvikling, programmering, beregning og teknisk forståelse.[6] For å sikre verdiskaping mente Digitutvalget at nye generasjoner må settes i stand til å skape, ikke bare forbruke, teknologi. Digitutvalget foreslo derfor å utvide definisjonen av digitale ferdigheter til også å innebære beregning, analyse og generell teknologiforståelse. I tillegg ønsket de å innføre programmering som valgfag i grunnskolen. Det var etter Digitutvalgets mening for lenge å vente til videregående utdanning tilbyr formell undervisning i programmering. Tiltak for å bygge kompetanse blant lærerne ble foreslått, blant annet basert på «skolens digitale tilstand».[7]

For høyere utdanning pekte Digitutvalget på manglende formelle krav til digital kompetanse eller ferdigheter, og at slike krav må klarere inn i læringsmål i alle studieprogram. De mente at forståelse for teknologi er viktig også for generalister, som jurister, økonomer, leger og sykepleiere. Helsepersonell må for eksempel kunne ivareta sikkerhet, personvern og menneskeverd. Økonomer må forstå nettbaserte forretningsmodeller. Journalister må kunne bearbeide store mengder rådata og krysskoblinger i databaser for å drive

---

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

4 Kommunal- og moderniseringsdepartementet (2013): *Nasjonal strategi – IKT-forsking og -utvikling. Strategi 2013-2022.*

5 NOU 2013: 2 *Hindre for digital verdiskaping.*

6 Med teknisk forståelse menes å få innsyn i de bakenforliggende mekanismene for hvordan datamaskiner fungerer og snakker sammen, og hva Internett er.

7 Senter for IKT i utdanningen (2012): *Monitor 2011 – Skolens digitale tilstand.* Det vises til at det er store mangler i elevers og læreres operative digitale ferdigheter. Eksempler er bruk av regneark, kunnskap om opphavsrettighet og bruk av Wikipedia som kilde. Undersøkelsen ser ikke på situasjonen knyttet til forståelse av hvordan «datamaskiner fungerer».

oppsøkende journalistikk. Lærere må kunne knytte IKT til sine fagfelt.

For IKT-spesialistene mente Digitutvalget at det var viktig å få frem studietilbud rettet mot entreprenørskap der den digitale skaperkompetansen rendyrkes. Dette begrunnet i manglende fokus på kommersialisering av produkter og tjenester.

I 2015 ble det levert en utredning kalt *Fremtidens skole – Fornyelse av fag og kompetanser*[8], som vurderte grunnopplæringens fag opp mot krav til kompetanse i et fremtidig samfunns- og arbeidsliv. Utvalget skrev:

> «Verktøykompetanse og kompetanse knyttet til sikkerhet er eksempler på digital kompetanse[9] som ikke har en umiddelbar tilknytning til noen av dagens skolefag».

Videre står det:

> «Teknologiutviklingen fører til endringer i alle fag. Samtidig er det deler av digital kompetanse som ikke er knyttet til et bestemt fag, for eksempel det å lære generelle sider ved bruk av datamaskiner som verktøy. En konsekvens av dette kan være uklarheter i skolehverdagen om hvilke fag som skal ta ansvar for elevenes læring og utvikling av grunnleggende 'operasjonelle' digitale ferdigheter.»

Utvalget anbefalte at «de ulike sidene ved digital kompetanse uttrykkes som del av kompetansen i alle fag, men uten at dagens ordning med grunnleggende digitale ferdigheter videreføres».

Digidel 2017 er Kommunal- og moderniseringsdepartementets program for økt digital deltakelse, i samarbeid med private aktører. Hensikten er å styrke samarbeidet og øke innsatsen som i dag gjøres av ulike offentlige virksomheter, IKT-næringen og frivillige organisasjoner på området digital kompetanse og deltakelse. Digidel 2017 vil tilby opplæringsmateriell og arenaer for erfaringsutveksling og kunnskapsheving for instruktører og kursledere som driver med undervisning innen digital kompetanse. EU har en tilsvarende satsning på digital inkludering i sin digitale agenda.

Justis- og beredskapsdepartementet har utgitt *FoU-strategi for samfunnssikkerhet 2015–2019.*[10] Trygg digitalisering av samfunnet er ett av flere prioriterte temaer i strategien. Justis- og beredskapsdepartementet vil bidra til forskning innen informasjonssikkerhet og personvern gjennom Forskningsrådets IKTPLUSS og delta aktivt for å koordinere EU-forskningen i Horisont 2020.

19.2 Roller og ansvar

Kunnskapsdepartementet har ansvaret for barnehager, grunnskole, kulturskole, videregående opplæring, fagskoleutdanning og høyere utdanning. Kunnskapsdepartementet utformer den nasjonale utdanningspolitikken som er vedtatt av Stortinget. Departementet har også ansvar for voksnes læring og forskning.

Justis- og beredskapsdepartementet har samordningsansvaret for forebyggende IKT-sikkerhet i sivil sektor. Nasjonal sikkerhetsmyndighet (NSM) er det nasjonale fagmiljøet for IKT-sikkerhet.

Utdanningsdirektoratet følger opp og iverksetter den nasjonale utdanningspolitikken, blant annet gjennom veiledning, tilsyn og undersøkelser.

Senter for IKT i utdanningen skal bidra til økt kvalitet på opplæringen innen bruk av IKT for barn i barnehager, elever i grunnskole og videregående opplæring og studenter i barnehage- og lærerutdanningene. Senteret har blant annet ansvar for personvernskolen.no, undervisningsopplegget «Du bestemmer», og FEIDE i grunnopplæringen.

Nasjonalt organ for kvalitet i utdanningen (NOKUT) har ansvaret for kvalitetssikringen av høyere utdanning og fagskoleutdanning i Norge. Høyere utdanninger tilbys på bachelor-, master- og doktorgradsnivå, og skal være forskningsbaserte. Fagskole er et kortvarig, yrkesrettet alternativ til høyere utdanning. NOKUT fører tilsyn for å utvikle kvaliteten ved utdanningsinstitusjonene. NOKUT har også ansvaret for å godkjenne utenlandsk høyere utdanning og skal bidra til god informasjon når det gjelder sammenligning av norsk og utenlandsk kompetanse.

Norges Forskningsråd (Forskningsrådet) er et nasjonalt forskningsstrategisk og forskningsfinansierende organ som skal møte samfunnsutfordringer og forskningspolitiske målsettinger.

---

8 NOU 2015: 8 *Fremtidens skole – Fornyelse av fag og kompetanser.*

9 Verktøykompetanse handler om praktisk bruk av universelle digitale enheter og systemer som bruk av datamaskin og etablerte programmer for behandling av tekst, tall, presentasjoner og bilder. Sikkerhet er å lære å beskytte egen informasjon som ligger digitalt.

10 Justis- og beredskapsdepartementet (2015): *FoU-strategi for samfunnssikkerhet 2015–2019.*

Forskningsrådet finansierer forskningsprosjekter, gir basisfinansiering til institutter og sentre, i tillegg til investeringer i nasjonal forskningsinfrastruktur, kurs og konferanser. Budsjettet for 2014 var på 8 046 millioner kroner.[11] Rådet skal medvirke til samspill mellom forskning og næringsliv.

19.3 Kompetansesituasjonen i samfunnet

DAMVAD og Samfunnsøkonomisk analyse har tidligere fått i oppdrag av Kommunal- og moderniseringsdepartementet å undersøke behovet for avansert IKT-kompetanse frem mot 2030.[12] Analysen viser at etterspørselen etter personer med avansert IKT-kompetanse overgår dagens tilbud av personer med denne kompetansen.

Kommunene har i dag bare unntaksvis en tydelig sikkerhetsorganisasjon, og etterspør derfor i liten grad relevant kompetanse innen IKT-sikkerhet. Kommunene har stort sett små IKT-miljøer, der IKT-sikkerhetsarbeidet bare er én av mange oppgaver for IKT-personalet. Også fylkesmennene har små organisasjoner uten dedikert personell med kompetanse innen IKT-sikkerhet. Ansvaret for IKT-sikkerhet er ofte tillagt personale med andre hovedoppgaver, og som mangler nødvendig spisskompetanse på sikkerhet. Mange ledere har også for lav bevissthet om at de er ansvarlige for IKT-sikkerheten, og har verken vilje eller evne til å ivareta denne rollen.

Det er bred enighet blant infrastruktureiere og bransjeorganisasjoner om at det er en generell mangel på personer med IKT-sikkerhetskompetanse i samfunnet, og at det er utfordrende å rekruttere til denne typen stillinger. Det er likevel få virksomheter som rapporterer om negative konsekvenser som direkte følge av mangel på kompetanse. Også konsulentbransjen oppgir underskudd på personell. De peker spesielt på et stort underskudd på folk med to–fem års erfaring innen sikkerhetsarbeid. Nyutdannede er det noe bedre tilgang på. Etterspørselen etter IKT-sikkerhetskompetanse i markedet er økende, også fra selskaper. Det synes å være enighet om at det er et gap mellom kompetansetilbudet og etterspørselen i markedet.

Utenom de nasjonale kontaktpunktene for informasjonssikkerhet og Difi ser det ikke ut som om direktorater og tilsyn ser det som sin rolle å ha tung og bred spisskompetanse på IKT-sikkerhetsområdet. Vi viser her til omtale av kompetanse under samfunnsfunksjonene i del III «Sårbarheter i kritiske samfunnsfunksjoner».

19.4 Utdanning

I det følgende omtales IKT-utdanning på ulike nivåer, med særlig vekt på ferdigheter som omhandler IKT-sikkerhet og personvern.

19.4.1 Offentlig grunnskole

I offentlig grunnskole undervises det etter læreplanverket Kunnskapsløftet (LK-06), som ble innført høsten 2006, og som også dekker utdanning i videregående skole. LK-06 setter opp fem grunnleggende ferdigheter alle elever skal tilegne seg: å kunne skrive, å kunne regne, å kunne lese, muntlige ferdigheter og digitale ferdigheter. I Utdanningsdirektoratets *Rammeverk for grunnleggende ferdigheter*[13] er digitale ferdigheter definert slik:

> «Digitale ferdigheter vil si å kunne bruke digitale verktøy, medier og ressurser hensiktsmessig og forsvarlig for å løse praktiske oppgaver, innhente og behandle informasjon, skape digitale produkter og kommunisere. Digitale ferdigheter innebærer også å utvikle digital dømmekraft gjennom å tilegne seg kunnskap og gode strategier for nettbruk.»

Digitale ferdigheter er ikke definert som et fag i seg selv, men inngår i læreplaner for andre emner og er primært et virkemiddel for å oppnå målene for disse. Det tilbys en frivillig nasjonal prøve på 4. årstrinn for å måle læringsutbyttet.

Digital dømmekraft innebærer å kunne bruke digitale verktøy, medier og ressurser på en forsvarlig måte og å ha et bevisst forhold til personvern og etisk bruk av Internett. Kildekritikk og informasjonssikkerhet er også en viktig del av den digitale dømmekraften. Senter for IKT i utdanningen har på nettstedet dubestemmer.no utarbeidet et undervisningsopplegg om personvern og digital dømmekraft for barn og unge i alderen 9–18 år.

Mens digitale ferdigheter retter seg mot bruk av digitale verktøy, er valgfaget Teknologi i praksis et mer teknisk kurs der eleven får mulighet til

[11] Forskningsrådet (2015): *Årsrapport 2014.*

[12] DAMVAD og Samfunnsøkonomisk analyse (2014): *Dimensjonering av avansert IKT-kompetanse.*

[13] Utdanningsdirektoratet (2012): *Rammeverk for grunnleggende ferdigheter - Til bruk for læreplangrupper oppnevnt av Utdanningsdirektoratet.*

å utvikle og eksperimentere med teknologi. I dette inngår også muligheter til å arbeide med IKT med for eksempel Lego-roboter. Det har frem til nå ikke vært noe tilbud om opplæring i programmering i barne- eller ungdomskolen. Denne typen opplæring har i all hovedsak blitt gitt gjennom frivillige organisasjoner som Lær Kidsa Koding og First Lego League. Disse har hatt økende pågang de siste årene.

I sammenheng med den nye realfagstrategien «Tett på realfag» kunngjorde regjeringen i august 2015 at man fra skoleåret 2016/2017 vil starte et prøveprosjekt med tilbud om programmering som valgfag i ungdomskolen. Dette prosjektet vil omfatte inntil 20 klasser det første året. Utdanningsdirektoratet har fått i oppdrag å utarbeide en midlertidig læreplan for det nye valgfaget.

Diskusjoner

Opplæring i digital kompetanse har som mål å sikre at hele befolkningen er i stand til å bruke digitale verktøy i sitt daglige virke. Men som Digitutvalget uttalte, må nye generasjoner også settes i stand til å skape, ikke bare forbruke, teknologi. Som et av tiltakene for å bøte på dette foreslo Digitutvalget å innføre programmering som valgfag i grunnskolen.

Dette er også viktig ut fra et sikkerhetsmessig standpunkt. Det krever dypere teknisk innsikt å forstå hvilke muligheter, men også farer og begrensninger, som ligger i digitale verktøy. Det er dessuten en forutsetning med teknisk innsikt dersom man vil være med og videreutvikle og forbedre teknologien.

Dette følger en trend som har gjort seg gjeldende i stort sett hele EU om å la barn og ungdom få opplæring i grunnleggende dataprogrammering. De IKT-faglige interesseorganisasjonene Informatics Europe og ACM Europe ga i 2013 ut en rapport der hovedkonklusjonen er at hele befolkningen trenger opplæring både i bruk av digitale verktøy og i informatikk.[14] Begrepet *informatikk* dekker her først og fremst kunnskap om programmering, men også en dypere forståelse av hvordan digitale verktøy er bygd opp, og hvordan de fungerer. Motivasjonen for forslaget er betydningen informatikk har for teknologisk innovasjon og dermed også økonomisk utvikling i samfunnet. Andre grunner for å lære programmering i skolen er at det fungerer som et støtteverktøy for andre fag, samtidig som det utvikler analytisk tenking og evne til problemløsing og stimulerer til kreativitet og gruppearbeid.

En rekke land i EU har allerede innført eller planlegger å innføre tilbud om opplæring i programmering i skolen. I England har programmering vært et obligatorisk fag i grunnskolen siden 2012. Tilsvarende krav vil også bli innført i Finland fra høsten 2016. Etablering av et opplæringstilbud i programmering krever imidlertid kunnskap man ikke kan forvente at dagens lærere besitter. I Finland er dette løst gjennom et samarbeid mellom privat sektor og utdanningsdepartementet for å sikre tilgang på tilstrekkelig kompetanse.

Andre land har også egne spesifikke initiativ for å ivareta utdanning innen IKT-sikkerhet. For eksempel har USA gjennom et offentlig-sivilt samarbeid opprettet The National Initiative for Cybersecurity Education (NICE) for å utvikle og vedlikeholde et utdanningsprogram som omfatter opplæring i IKT-sikkerhet, både for allmenheten og for alle utdanningsnivå.

19.4.2 Videregående opplæring

Videregående opplæring omfatter all kompetansegivende opplæring mellom grunnskolen og høyere utdanning og kvalifiserer til arbeidsliv eller videre studier. Offentlig videregående opplæring drives av fylkeskommunene, og det undervises også her etter LK-06. Det skilles mellom studieforberedende og yrkesforberedende utdanning.

Videregående opplæring bruker i stor utstrekning PC-er i skolearbeid, og fylkeskommunen kan kreve at elevene deltar i skolenes utleieordning for bærbare PC-er. Akkurat som for grunnskolen inngår bruk av digitale verktøy som grunnleggende ferdigheter i alle læreplaner.

Blant de videregående opplæringene er det IKT-servicefag som gir den grundigste opplæringen i informasjonssikkerhet. Dette er en yrkesfaglig utdanning som består av ett år med felles programfag etterfulgt av to år med læretid i bedrift. En yrkeskarriere vil typisk føre frem mot arbeid innenfor drift, støtte og vedlikehold av IKT-systemer. I studiet legges det blant annet vekt på ulike aspekter ved IKT-sikkerhet og korrekt behandling av data. I læremålene inngår blant annet

- å behandle fortrolige opplysninger på en etisk forsvarlig måte innenfor rammene av gjeldende regelverk

[14] Report of the joint Informatics Europe & ACM Europe Working Group on Informatics Education (2013): *Informatics education - Europe cannot afford to miss the boat.*

- å vurdere systeminstallasjoner mot krav til tilgjengelighet, informasjonssikkerhet og helse, miljø og sikkerhet
- å aktivisere, vurdere og dokumentere sikkerhetsmekanismer for å forebygge og varsle forsøk på sikkerhetsbrudd

Av andre yrkesfag har både data og elektronikk og el-energi fellesfag der informasjonssikkerhet inngår i læreplanen. Tilsvarende inngår sikkerhetsrutiner for virksomhetens kunnskapsorganisering og informasjonsflyt i læreplanen for kontor- og administrasjonsfaget.

I det studiespesialiserende utdanningsprogrammet er det to programfag som omhandler IKT – Informasjonsteknologi 1 og Informasjonsteknologi 2. Disse kan velges uavhengig av hverandre. Informasjonsteknologi 1 er et basiskurs i informasjonsteknologi og dekker blant annet Digital samtid, samt utvikling av nettsteder og bruk av databaser. Informasjonsteknologi 2 er mer teknisk rettet og med et større tilsnitt av programmering og multimedieutvikling. I læreplanen for Informasjonsteknologi 1 inngår IKT-sikkerhet og kjennskap til gjeldende regelverk og etiske normer for bruk av informasjonsteknologi. IKT-sikkerhet inngår ikke i læreplanen for Informasjonsteknologi 2.

Diskusjoner

Alle yrker der man kan trenge å bruke datamaskiner, krever digitale basiskunnskaper. Mye av dette oppnås gjennom opplæring i skolen og gjennom daglig bruk, men etter som samfunnet blir stadig mer digitalisert, kreves det ofte også yrkesspesifikk IKT-kunnskap. Det er derfor vesentlig at hver utdanning gir relevant opplæring i aktuelle datasystemer, samtidig som det blir lagt vekt på hvordan disse brukes på en forsvarlig måte. For eksempel vil mindre foretak ofte ikke ha egne IKT-spesialister til å drifte datamaskiner, og de ansatte må selv holde programvaren oppdatert og vite hvordan man håndterer grunnleggende IKT-sikkerhet. Det er derfor vesentlig at særlig avsluttende yrkesutdanninger har en tilstrekkelig IKT-komponent som også inneholder opplæring i IKT-sikkerhet.

Utvalget registrerer at flere yrkesutdanninger innen IKT og elektrofag allerede har en komponent av opplæring i IKT-sikkerhet og personvern. Det er spesielt positivt at IKT-sikkerhet vektlegges såpass grundig i IKT-servicefaget. Dette er i den yrkesutdanningen det er størst sannsynlighet for at man blir eksponert for denne typen problemstillinger, det er derfor vesentlig at uteksaminerte kandidater har relevant kunnskap.

19.4.3 Høyere utdanning

Det tilbys høyere utdanning i IKT ved en rekke høyskoler og universiteter i Norge. Det er særlig to områder som er sterkt representert: informasjonsteknologi og IKT innenfor ingeniørutdanning. Ved universitetene gis det både bachelor- og masterutdanninger innen IKT.

Av ulike årsaker er det vanskelig å få frem sikker statistikk over hvor mange som har fullført en bachelorgrad innenfor IKT-studier ved enkelte universiteter. Ved høgskolene har det i snitt blitt uteksaminert cirka 410 kandidater hvert år de siste tre årene. Av disse kommer cirka 28 prosent fra Høgskolen i Oslo og Akershus og 21 prosent fra Høgskolen i Sør-Trøndelag. Samlet er det cirka 400 mastergradskandidater per år. Av disse kommer over 90 prosent fra universitetene, flest fra NTNU (42 prosent) og Universitetet i Oslo (27 prosent).

Innenfor IKT-sikkerhet tilbys det utdanning på bachelor-, master- og PhD-nivå ved norske høgskoler og universitet. Høgskolen i Gjøvik og Universitetet i Bergen er de eneste institusjonene som tilbyr en bachelorgrad spesifikt rettet mot informasjons- og IKT-sikkerhet. Noroff høyskole har dessuten et bachelorprogram i digital etterforskning. Universitetet i Bergen, NTNU og Høgskolen i Gjøvik har egne masterprogrammer for IKT-sikkerhet. Fra 2017 vil spesialisering innen IKT-sikkerhet på masternivå bli tilbudt også ved Universitetet i Oslo. Det er dessuten flere universiteter som tilbyr masteroppgaver innen IKT-sikkerhet uten å ha et eget program for dette.

De fleste høgskoler og universiteter tilbyr enkeltkurs i IKT-sikkerhet som del av sin undervisningsportefølje. Dette er for eksempel kurs i sikker programvareutvikling, nettverkssikkerhet og informasjonssikkerhet. Det varierer mellom studieprogrammene om slike kurs er obligatoriske eller ikke, men hovedtendensen er at de ikke er det.

Høgskolen i Gjøvik har de siste fem årene uteksaminert i overkant av 10 kandidater per år fra sine sikkerhetsrelaterte bachelorstudier. Bachelorprogrammet ved Universitetet i Bergen ble startet i 2015 og har ennå ikke uteksaminert noen kandidater. Det uteksamineres i overkant av 70 masterkandidater per år innenfor temaer relatert til IKT-sikkerhet. De fleste av dem kommer fra NTNU (cirka 46 prosent) og fra Høgskolen i Gjøvik (cirka 26 prosent). Kandidatene fra NTNU

kommer i all hovedsak fra telematikk, men også fra matematikk (kryptografi).

Fra 1. januar 2016 vil NTNU, Høgskolen i Gjøvik, Høgskolen i Sør-Trøndelag og Høgskolen i Ålesund bli slått sammen under NTNU-paraplyen. Gitt dagens kandidatproduksjon vil det nye universitetet stå for nesten 50 prosent av masterproduksjonen innenfor IKT og cirka 70 prosent av masterproduksjonen innenfor IKT-sikkerhet.

PhD-utdanning innenfor IKT-sikkerhet foregår ved de fleste universitetene og ved Høgskolen i Gjøvik. PhD-utdanningen er organisert gjennom Norges nasjonale forskerskole i informasjonssikkerhet, COINS (Research School of Computer and Information Security). COINS er ledet av Høgskolen i Gjøvik, og trekker sammen norske forskningsmiljøer i informasjonssikkerhet til en større enhet ved å integrere den relevante kursportfolioen til de deltagende institusjonene, bygge sterkere relasjoner imellom PhD-studentene og tilby dem et større nettverk. Partnere i forskerskolen inkluderer Høgskolen i Gjøvik, NTNU, Universitetet i Oslo, Universitetet i Bergen, Universitetet i Agder, Universitetet i Stavanger og Universitetet i Tromsø. I overkant av ti doktorgradskandidater disputerer hvert år innen IKT-sikkerhet. Disse kommer i all hovedsak fra de store universitetene og fra Høgskolen i Gjøvik.

Diskusjoner

I følge EU-kommisjonens estimater vil så mange som 90 prosent av alle fremtidige jobber i EU kreve digital kompetanse. EU-kommisjonen har også advart at det ved utløpet av inneværende år vil mangle inntil en halv million arbeidere med spesialkompetanse innen IKT.

Etterspørselen etter ferdige kandidater med IKT-kompetanse vil variere med de økonomiske konjunkturene i samfunnet. De siste årene har imidlertid etterspørselen vært langt større enn tilgangen på kandidater. KMD estimerer at det i det offentlige og i næringslivet med dagens utdanningstakt vil mangle mer enn 10 000 personer med avansert IKT-kompetanse i 2030.[15] IKT-sikkerhet er et av områdene der det forventes et særlig behov for kompetanse. Utvalget har sett den samme tendensen i sin kontakt med ulike samfunnsaktører.

Både universiteter og forskningsinstitusjoner oppgir at det er generelt vanskelig å rekruttere tilstrekkelig personell nasjonalt, og at flere er avhengige av internasjonal rekruttering. Enkelte oppgir i den sammenheng at det kan være utfordrende å bruke utenlandsk personell, enten fordi det er vanskelig å få dem sikkerhetsklarert, eller fordi de ikke kjenner norske forhold. Det synes å være spesielt vanskelig å rekruttere til doktorgradsstillinger, der det er gjennomgående få norske søkere.

Utvalget registrerer at det er en underdekning både av kandidater med generell IKT-kompetanse og av kandidater med mer spesifikk IKT-sikkerhetskompetanse. Det er like fullt ønskelig at de som faktisk gjennomfører en generell IKT-utdanning, har grunnleggende kunnskaper om IKT-sikkerhet. Utvalget har sett at det er flere utdanningsløp der dette ikke er tilfellet. Det er imidlertid nå en internasjonal trend å inkludere IKT-sikkerhet i samtlige bachelorprogrammer innenfor IKT. De internasjonale IKT-interesseorganisasjonene ACM og IEEE ga i 2013 ut sin siste rapport med retningslinjer for hvilke temaer som bør dekkes av en bachelorutdanning innenfor Computer Science.[16] [17] Selv om rapporten først og fremst retter seg mot amerikanske forhold, er det ingen grunn til å tro at den ikke også er dekkende for hva som bør inngå i en norsk IKT-bachelor.

Sammenlignet med foregående rapport fra 2008 anbefaler den nye rapporten to nye områder som enhver bachelorutdanning i Computer Science bør dekke. Ett av disse er Information Assurance and Security (IAS). Dette området dekker både tekniske løsninger og policy-beslutninger som har til hensikt å beskytte og forsvare informasjon og informasjonssystemer blant annet gjennom å sikre konfidensialitet, integritet og tilgjengelighet.[18] Rapporten anbefaler at av den totale undervisningstiden bør cirka 3 prosent brukes på dedikert IAS-stoff og cirka 20 prosent på IAS-stoff som kan dekkes gjennom andre kurs.

Som en oppfølging ble det også gitt ut en egen rapport[19] i Storbritannia i 2015 med retningslinjer for hvordan dette materialet skal dekkes av alle bachelorprogrammer innenfor IKT. Overført til

---

[15] DAMVAD og Samfunnsøkonomisk analyse (2014): *Dimensjonering av avansert IKT-kompetanse*.

[16] Mehran Sahami og Steve Roach (2014): *Computer science curricula 2013 released.* Communications of the ACM, Vol. 57 No. 6, Side 5.

[17] ACM/IEEE-CS Joint Task Force on Computing Curricula (Desember 2013): *Computer Science Curricula 2013 - Curriculum Guidelines for Undergraduate Degree Programs in Computer Science.*

[18] NISTIR 7298 Revision 2. *Glossary of Key Information Security Terms.* National Institute of Standards and Technology, U.S. Department of Commerce.

[19] ISC2 (2015): *Cybersecurity principles and learning outcomes for computer science and IT-related degrees. A resource for course designers and accreditors.* Versjon 1.1.

norske forhold vil en norsk bachelorgrad bestå av 180 studiepoeng, hvorav et IKT-studie inneholder cirka 100 studiepoeng IKT-relatert materiale. Det eksakte tallet varierer mellom institusjonene og også mellom ulike studier. Det skulle tilsi at dersom man følger rapportens anbefalinger, vil IAS-relatert materiale utgjøre cirka 23 studiepoeng, fordelt på 3 dedikerte studiepoeng, og 20 studiepoeng som kan dekkes av andre kurs.

19.4.4 Etterutdanning

NSM er en sentral aktør innen etterutdanning innen forebyggende sikkerhet. NSMs kurssenter gjennomfører en rekke kurs av kortere og lengre varighet over hele landet. Grunnkurs i forebyggende sikkerhet og sikkerhetsledelse har som mål å gjøre deltakerne i stand til å redusere sårbarheter knyttet til spionasje, sabotasje eller terrorhandlinger. Tempest-kurset gir opplæring i å håndtere informasjonslekkasje via utilsiktet elektromagnetisk utstråling fra elektronikk. Kurs i fysisk sikring er rettet mot eiere eller leverandører av skjermingsverdige objekter og annen kritisk nasjonal infrastruktur. NSM har et lederrettet kurs om sikkerhetskultur og kurs om sårbarheter ved bruk av sosiale medier, i tillegg til en rekke kurs innen personellsikkerhet. NSM tilbyr også kurs i verdivurdering og informasjonssystemsikkerhet. NSM er vert for den årlige sikkerhetskonferansen.

Det finnes ulike tilbud om erfaringsbaserte utdanninger i universitets- og høyskolesektoren. Høyskolen i Gjøvik har etablert en erfaringsbasert mastergrad innen informasjonssikkerhet og dataetterforskning. Universitetet i Oslo har etablert en erfaringsbasert mastergrad i IT og ledelse som blant annet inneholder kurs i ledelse av informasjonssikkerhet. Dette emnet kan brukes til ulike sikkerhetssertifiseringer som CISM og CISSP. Sammen med CISA utgjør disse de mest kjente sertifiseringene innen IKT-sikkerhet og -revisjon. Forberedende kurs for disse sertifiseringene tilbys av en rekke private norske og internasjonale aktører.

19.5 Forskning og utvikling (FoU)

19.5.1 Norsk FoU-aktivitet innen IKT-sikkerhet

Det foregår forskning innenfor emner relatert til IKT-sikkerhet ved flere universiteter og høyskoler. De største miljøene finnes ved Universitetet i Oslo, Universitetet i Bergen, NTNU og Høgskolen i Gjøvik. Utenom disse foregår det forskning ved Universitetet i Agder, ved Universitetet i Stavanger og ved Universitetet i Tromsø. I instituttsektoren foregår det relevant forskning ved Simula Research Laboratory, SINTEF og Forsvarets forskningsinstitutt (FFI). I det følgende beskrives de største gruppene kort.

Ved Universitetet i Oslo har det meste av undervisningen i og forskningen på informasjonssikkerhet vært knyttet til UNIK. Det matematisk-naturvitenskapelige fakultet opprettet i 2014 «Endringsmiljø» (strategisk forskningsinitiativ) ved Institutt for informatikk for å bygge en kraftfull satsing på IKT-sikkerhet. Dette endringsmiljøet – ConSeRNS – består av 11 vitenskapelig ansatte og 6 PhD-stillinger, med IKT- sikkerhet eller tilstøtende temaer som hovedfelt.

Ved Universitetet i Bergen er forskning relatert til IKT-sikkerhet organisert i Selmersenteret og gjennom Simula@UiB ved Institutt for informatikk. Forskningen dekker et bredt spekter av fundamentale forskningsfelt som informasjonsteori, kodeteori, kryptografi og datasikkerhet. Totalt består gruppen av fem professorer og fire forskere samt flere PhD-studenter. Simula@UiB er et samarbeidsprosjekt med Simula Research Laboratory om forskning på kryptografi, IKT-sikkerhet og informasjonsteori. Senteret består av to professorer fra Selmersenteret og to forskere finansiert av Simula. Forskerne er i første omgang ansatt for en periode på fire år. For å styrke dette arbeidet vil Samferdselsdepartementet fra og med 2016 bidra til finansieringen av Simula@UiB med 5 millioner kroner årlig.

Simula Research Laboratory har siden 2006 utført all forskningsaktivitet innenfor IKT-sikkerhet i Robuste nett-senteret (Center for resilient Networks and Applications – CRNA). Senteret får sin grunnbevilgning fra Samferdselsdepartementet og har et teknologisk fokus. Blant annet foretas det langsiktige målinger av mobile bredbåndsnett i Norge. Dette danner grunnlag for en årlig rapport om stabiliteten og ytelsen til disse nettene. Hovedtyngden av forskningen omhandler effekten av utilsiktede hendelser, men CRNA har også et pågående samarbeid med UiB (Simula@UiB) om forskning for å håndtere tilsiktede hendelser som dataangrep. Forskerkapasiteten ved Simula har cirka 20 årsverk knyttet til Robuste nett og ytterligere 7 årsverk delt med Universitetet i Bergen. Av disse 27 er omtrent halvparten midlertidige PhD- og postdoktorstillinger. Simula samarbeider med UiO gjennom ConSeRNS.

Ved NTNU foregår i all hovedsak forskning relatert til IKT-sikkerhet ved Institutt for telematikk, og er fokusert på kryptologi, kommunikasjonssikkerhet, tilgangskontroll og digital etterforskning. Totalt er det åtte fast ansatte som arbeider med IKT-sikkerhet ved instituttet. Det foregår også sikkerhetsrelatert forskning ved andre institutter, om enn i mindre omfang.

Ved Høgskolen i Gjøvik ble forskning relatert til IKT-sikkerhet etablert i 2002 gjennom Norwegian Information Security Laboratory (NISlab), og har siden 2014 blitt videreutviklet gjennom Center for Cyber and Information Security (CCIS). CCIS er et forsknings- og utdanningssenter innen sikkerhet basert på et partnerskap mellom 25 offentlige, private og akademiske virksomheter. Det overordnede målet for CCIS er å styrke samfunnets kompetanse og ferdigheter i å beskytte mot, oppdage, respondere på og etterforske uønskede og kriminelle handlinger som benytter datamaskiner. Ved senteret er det forskningsgrupper innen informasjonssikkerhet, beskyttelse av kritisk infrastruktur, cyberforsvar, biometri, personvern og digital etterforskning og bevissikring. Forskerkapasiteten ved CCIS utgjør til sammen 32 årsverk hvorav 16 i fast stilling. Miljøet er det største innenfor fagfeltet i Skandinavia. Fra 2016 vil Høgskolen i Gjøvik være en del av NTNU. Sammen med Cyberforsvaret etablerer CCIS Cyber Range som et nasjonalt virtuelt øvingsfelt for forsking og utdanning på både beskyttelse og angrep på systemer og nettverk.

FFI utfører forskning på IKT-sikkerhet i militære informasjons- og kommunikasjonsinfrastrukturer og systemer. Forskergruppen som har IKT-sikkerhet som sitt hovedarbeidsområde, består av cirka 15 fast ansatte og er i hovedsak finansiert gjennom prosjekter for Forsvaret eller basisbevilgninger til FFI. Flere av forskerne har en bistilling ved universiteter og høyskoler. IKT-sikkerhet dekkes også av forskere som understøtter Forsvarets anskaffelser eller modernisering, og kompetansegruppen for IKT-sikkerhet teller totalt 45 personer. Utenom oppdrag for Forsvaret har FFI sporadiske oppdrag for sivile myndigheter og et nært samarbeid med andre forskningsmiljøer – primært gjennom NATOs forskningsaktiviteter og -grupper og samarbeid med sivile forskningsinstitusjoner. FFI støtter økonomisk et halvt professorat ved CCIS.

SINTEF er Skandinavias største uavhengige forskningsorganisasjon. De forsker blant annet på programvaresikkerhet, nettverkssikkerhet, cybersikkerhet, informasjonskontroll, risikoanalyse (også kombinert med testing) og innebygd personvern. SINTEF arbeider også med ikke-tekniske problemstillinger relatert til sårbarhet, nettmobbing og personvern. Totalt har SINTEF cirka 22 fast ansatte som arbeider med ulike sikkerhetsrelaterte problemstillinger.

19.5.2 Kvaliteten på norsk IKT-sikkerhetsforskning

I 2012 gjennomførte Forskningsrådet en evaluering av forskning og utvikling innen IKT ved et utvalg norske universiteter og høyskoler. Rapporten konkluderte med at Norge mangler en nasjonal strategi for IKT og underinvesterer i IKT-forskning relativt til feltets viktighet og potensial sammenlignet med andre vesteuropeiske og nordamerikanske land. Samtidig som rapporten påpeker at Norge ligger langt fremme på en rekke enkeltområder, konkluderer den med at utilstrekkelig vektlegging på forskning innenfor cybersikkerhet kan utgjøre en potensiell sikkerhetsrisiko for Norge. Rapporten anbefaler at Norge utvikler en nasjonal IKT-forskningsstrategi som tar hensyn til de særegne behovene til norsk industri og samfunn, og konstaterer at det er av nasjonal betydning med en strategisk innsats for å øke nasjonal kompetanse på cybersikkerhet.[20]

I Forskningsrådets evaluering av IKT-forskning i 2012 fikk hver forskningsgruppe en karakter på en skala fra 1 til 5, der 1 er lavest og tilkjennegir at gruppen har substansielle strukturelle problemer og begrenset påvirkningskraft og produktivitet. Karakteren 5 er høyest og gis til grupper med internasjonalt lederskap, synlighet og visjon. Av gruppene som driver forskning innenfor IKT-sikkerhet, var det bare gruppen i Bergen som fikk karakteren 5, mens Simula fikk 4 og Høgskolen i Gjøvik 3 til 4. De resterende gruppene fikk karakteren 3 eller lavere. Denne evalueringen ble gjort før UiO startet ConSeRNS og før Høgskolen i Gjøvik startet CCIS. Simula@UiB-samarbeidet ble også startet etter evalueringen.

Norge har i en årrekke hatt faglig sterke forskningsgrupper innen kryptografi. I tillegg til rådgivning og vurderinger har disse miljøene utdannet kandidater som er med på å høyne det generelle nasjonale kompetansenivået innen kryptografi. Gruppene er imidlertid relativt små og dermed også personavhengige. Innen matematikk og datavitenskap er kryptografi bare ett av mange forskningsområder. Det er derfor ikke gitt

[20] Research Council of Norway (2012): *Research in Information and Communication Technology in Norway. An evaluation.*

at universiteter og andre forskningsinstitusjoner vil prioritere å bygge opp og vedlikeholde levedyktige og kompetente miljøer.

19.5.3 Forskningsrådets rolle

Forskningsrådet er den viktigste finansieringskilden for prosjektstøtte i universitetets- og høyskolesektoren. I tidsrommet 2010–2014 bevilget Forskningsrådet cirka 75 millioner kroner til prosjekter som ser på forskjellige aspekter ved IKT og sikkerhet, personvern og sårbarhet. Fra 2015 er IKTPLUSS Forskningsrådets hovedprogram innen IKT og skal løpe frem til 2024, med et årlig budsjett på cirka 165 millioner kroner. Årets bevilgning kommer fra KMD, SD, NFD og KD. Figur 19.1 viser tildeling av de ulike departementenes bevilgning til forsking de tre siste årene. JD bevilger generelt lite midler til forskning og utvikling.

De faglige tematiske prioriteringene i IKTPLUSS tar utgangspunkt i de tre overordnede satsingsområdene Kompleksitet og robusthet, Data og tjenester overalt og Et trygt informasjonssamfunn.[21] Forskningsområder som er nevnt i forbindelse med Et trygt informasjonssamfunn, inkluderer blant annet sikkerhet i komplekse infrastrukturer, personvernfremmende teknologier, digital etterforskning og datakriminalitet, samt kryptografi og sikkerhetsmekanismer. Disse forskningstemaene er gjensidig knyttet til forskningstemaene om kompleksitet og robusthet, herunder samspill mellom teknologi, individer og samfunn. Å håndtere kompleksitet og skape robuste systemer er sentralt for å ivareta samfunnssikkerheten.

Programmet har gjennomført sin første utlysning og har i 2015 innvilget prosjekter relatert til IKT-sikkerhet med en samlet ramme på 150 millioner kroner.

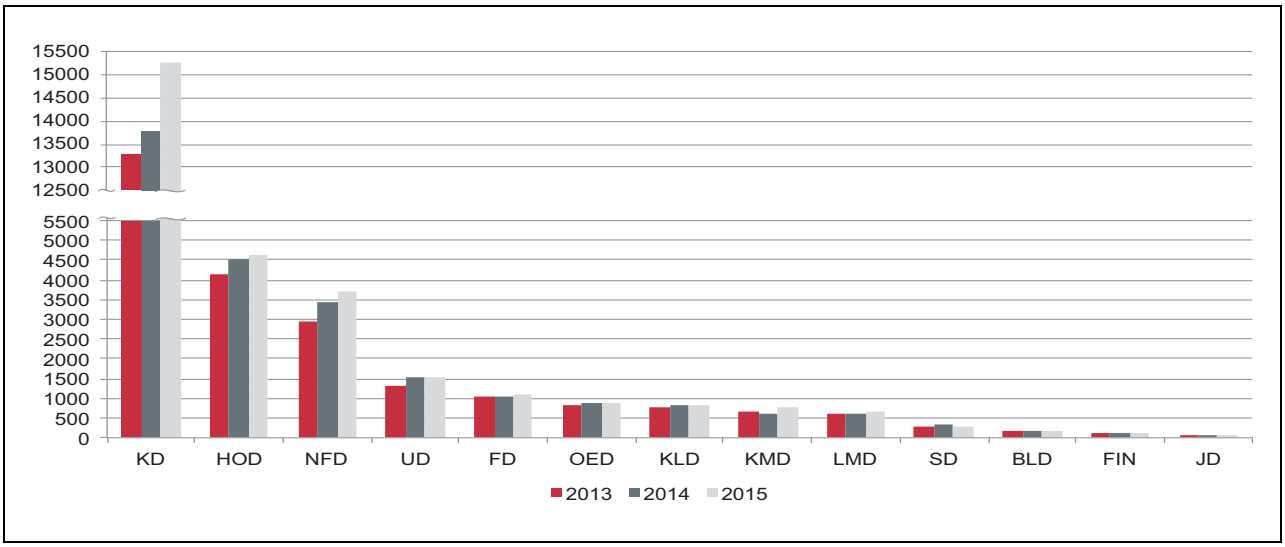
[21] Forskningsrådet (2015): *IKTPLUSS – Plan for satsingen*.

19.5.4 Internasjonal finansiering

Horisont 2020 er EUs gjeldende forskningsprogram for tidsrommet 2014–2020, og er verdens største program for innovasjon og forskning. I 2015 gjennomførte Horisont 2020 en utlysning av midler som dekker problemstillinger relatert til IKT-sikkerhet og personvern, «Digital security: cybersecurity, privacy and trust H2020-DS-2015-1». Det totale budsjettet for utlysningen var på 50 M€. Det er forventet at resultatet fra utlysningen foreligger ved årsskiftet 2015/2016.

19.5.5 Diskusjoner

Blant universitetene mener enkelte at det har blitt vanskeligere å få forskningsmidler til IKT-sikkerhet fra Norges forskningsråd de siste årene. Det pekes på at den manglende satsingen på IKT-sikkerhet har ført til at det utdannes svært få kandidater i Norge med den nødvendige kompetansen til å drive forskning på et høyt internasjonalt nivå.



Figur 19.1 Tildeling av FoU-midler fordelt på departement for 2013–2015. Beløpene er i millioner kroner. Tall for FAD er lagt inn i KMD for 2013. Statistikken er fra NIFU.[1]

[1] Statistikk fra Nordisk institutt for studier av innovasjon, forskning og utdanning (NIFU).

Det er usikkert om Norge per i dag har nødvendig og tilstrekkelig kompetanse til å dekke behovet for forskning innen IKT-sikkerhet, og for enkelte forskningsinstitusjoner er mangel på kompetanse en begrensende faktor for hvilke oppdrag de kan påta seg. Basert på svarene utvalget har mottatt, er det grunn til å anta at konklusjonene vedrørende manglende satsing på forskning og utvikling innen IKT-sikkerhet som ble avdekket av Forskningsrådet i deres evaluering fra 2012, fremdeles gjelder.

Å ha tilgang på gode forskningsmiljøer innenfor IKT-sikkerhet er vesentlig av flere grunner. Det er forskning som produserer ny kunnskap, og som kan adressere problemstillinger som er viktige for nasjonale aktører. Kapasiteten og kvaliteten på utdanning innen IKT-sikkerhet er dessuten nært knyttet til kvaliteten og størrelsen på tilhørende forskningsgrupper. Forskningsrådets evaluering fra 2012 viser at Norge har forskningsmiljøer innenfor IKT-sikkerhet som til dels er svært gode. Det skulle tilsi at vi har potensial for å bygge videre på eksisterende miljøer og dermed sikre høy kvalitet og også tilstrekkelig volum innen både forskning og utdanning.

Selv om enkeltforskere kan oppnå meget gode resultater, er det en gjennomgående trend at den beste forskningen krever forskningsgrupper av en viss størrelse. Å ha tilgang på bred nok kunnskap er også en forutsetning for at uteksaminerte kandidater skal ha best mulig kunnskapsgrunnlag i sitt videre arbeid. Det er derfor svært positivt at det i kjølvannet av 2012 har foregått en konsolidering av de viktigste norske forskningsmiljøene innen IKT-sikkerhet. Samarbeidet gjennom Simula@UiB sikrer at man får bygd opp et sterkt forskningsmiljø innen mer teoretisk datasikkerhet og kryptografi, som også kan dra veksler på kompetansen ved Simula om «resilience». Ved Høgskolen i Gjøvik har man bygd opp en, i nasjonal målestokk, stor satsing på mer anvendt datasikkerhet sammen med mange av de viktigste samfunnsaktørene på området. Sammenslåingen av NTNU og Høgskolen i Gjøvik fra 2016 vil også legge grunnen for videre synergieffekter mellom telematikk- og kryptografimiljøet ved NTNU og sikkerhetsmiljøet i Gjøvik. Ved siden av denne satsingen har Universitetet i Oslo begynt å bygge opp en egen forskningsgruppe gjennom ConSeRNS.

Frem til starten av IKTPLUSS-programmet har tilgangen på prosjektmidler vært en begrensende faktor for forskningsaktiviteten, både når det gjelder forskningsvolum og antall utdannede PhD-kandidater. Dette har ført til en gradvis utarming av miljøene, noe som igjen går ut over fremtidig rekruttering. Imidlertid ser det nå ut til at ressurstilgangen har bedret seg gjennom Forskningsrådets satsing på IKT-sikkerhet, og sammen med EUs program for cybersikkerhet i Horisont 2020 burde det nå være mulig både å vedlikeholde og bygge videre på den kompetansen som allerede finnes. Dette forutsetter imidlertid at Forskningsrådet vedlikeholder sin nåværende satsing.

Antall uteksaminerte PhD-kandidater avhenger både av finansiering og veiledningskapasitet. Selv om Forskningsrådets økte satsing er prisverdig, gir den ikke flere faste stillinger. Universitetene og høgskolene har mulighet til å foreta interne omprioriteringer for å bygge opp prioriterte forskningsmiljøer, men slike tiltak vil være av begrenset omfang og tar dessuten lang tid. Muligheten til å bygge opp langsiktig satsing basert på midler fra eksterne aktører vil også være begrenset over tid. Det er derfor ønskelig at bevilgende myndigheter ser på dimensjoneringen av hele området og setter i verk nødvendige tiltak.

En slik vurdering må ta hensyn til hvilke områder som er nasjonalt viktige, både med tanke på produksjon av kandidater og på hvilke forskningstemaer man ønsker å prioritere.

19.6 Kunnskap og støtte til befolkningen

NorSIS vektlegger å gi råd og veiledning til befolkningen, siden kunnskap i befolkningen i stor grad overføres til de små og mellomstore virksomhetene. NorSIS driver i dag nettsidene norsis.no, sikkert.no, slettmeg.no og idtyveri.info.[22] NorSIS utgir årlig rapporten *Trusler og trender*.[23]

NorSIS er tilrettelegger for Nasjonal sikkerhetsmåned, som holdes hver oktober. Hensikten med initiativet er å understøtte digitaliseringen av samfunnet. Lignende arrangementer gjennomføres i USA, cirka 30 land i EU og også i andre land i verden. Nasjonal sikkerhetsmåned tilbyr informasjon og råd, arrangementer og e-læring og annen type opplæring til offentlige og private virksomheter. I 2014 nådde NorSIS ut til 270 000 ansatte i norske virksomheter med e-læringspakken.

[22] NorSIS vil trolig overta redaktøransvaret for nettvett.no i løpet av 2016, støttet av en redaksjonskomite fra NSM, Nkom og andre bidragsytere. Se for øvrig omtale i kapittel 21 «Avdekke og håndtere digitale angrep».

[23] NorSIS (2015): *Trusler og trender*.

NorSIS jobber aktivt i media og med å skape møteplasser. NorSIS arrangerer årlig flere konferanser, mange av dem i samarbeid med andre aktører. Konferansen Identitet fokuserer på identitetsutfordringer og løsninger, Security Divas på å stimulere kvinner til å jobbe med informasjonssikkerhet, Kritisk IS på informasjonssikkerhet i kritisk infrastruktur og Kraft IS på informasjonssikkerhet i kraftbransjen. I tillegg kommer avslutningskonferansen til Nasjonal sikkerhetsmåned, Sikkert NOK.

NorSIS har på oppdrag fra Justis- og beredskapsdepartementet satt i gang et prosjekt for å måle befolkningens kunnskap og bevissthet om informasjonssikkerhet. Prosjektet vil kunne gi viktig informasjon om sikkerhetstilstanden, avvik og effekten av ulike tiltak. Måling av status på innbyggerne er beskrevet som et krav i Nasjonal strategi for informasjonssikkerhet.

Forbrukerrådet er en statlig finansiert, men uavhengig interesseorganisasjon som bistår forbrukerne ved å tilby kostnadsfri juridisk veiledning og megling i konflikter med næringsdrivende. Årlig ber nesten 100 000 nordmenn om hjelp. Rådet jobber aktivt med å påvirke myndigheter og næringsliv i en forbrukervennlig retning gjennom dialog, påvirkningsarbeid og utredninger. Forbrukerrådets markedsportaler gir forbrukere informasjon om produkter og tjenester. I 2014 hadde rådet en gjennomgang av avtalevilkår i skytjenester for lagring,[24] og de jobber nå med en kartlegging av mobilapplikasjoner. Innen IKT jobber rådet spesielt for forbrukerrettigheter innen

- flyttbarhet av egne data mellom tjenester, slik at vi som forbrukere kan bytte mellom tjenester; i forlengelse av dette kommer retten til å bli glemt, som handler om å få sine data fjernet fra tjenesten
- akseptable vilkår med gradert personvern, slik at brukeravtaler blir enklere å lese, og at vi slipper såkalte «take it or leave it»-tjenester der forbrukeren ikke har et reelt valg
- åpenhet om hva virksomheter gjør med våre persondata, og hvem de deler dem med[25]

Forbrukerombudet er en offentlig tilsynsmyndighet. Ombudet jobber med å forebygge og stoppe ulovlig markedsføring samt urimelige kontrakter. Dette oppnås gjennom dialog, forhandlinger og bruk av sanksjonsapparatet. Forbrukerombudet får rundt 10 000 skriftlige klager og henvendelser i året. Rådet fører tilsyn med digitale tjenester og jobber for globale standarder, siden flesteparten av tjenestene er utenfor EU/EØS og dermed ikke følger de samme rammevilkårene.

Datatilsynets veiledningstjeneste besvarer henvendelser fra offentlige og private virksomheter, så vel som fra enkeltpersoner. Spørsmålene som kommer inn, er av både juridisk, teknisk og sikkerhetsmessig art. Denne tjenesten er et viktig lavterskeltilbud for publikum som har spørsmål knyttet til behandling av personopplysninger, og et viktig mål med tjenesten er å gjøre borgere og virksomheter i stand til å ivareta eget ansvar for personvern. I løpet av 2014 hadde veiledningstjenesten besvart 9 033 henvendelser.

19.7 Tjenesteutsetting

Utsetting av IKT-tjenester kan på sikt medføre tap av kompetanse i virksomhetens systemer og teknologi og svekket eierskap til oppgavene. Dette ser likevel ikke ut til å være en stor bekymring for virksomhetene. I noen grad er dette en kjent konsekvens og et resultat av bevisste valg fra virksomhetens side, og samarbeid med private er ikke til hinder for at virksomheten bygger opp sin egen kompetanse på området. Ved å sette ut driftsoppgaver kan man få stabil tilgang på et kompetansemiljø som er mer robust enn det er realistisk for virksomheten selv å opprettholde over tid. På den andre siden velger enkelte virksomheter å bygge opp sin egen kompetanse på grunn av manglende kompetanse hos underleverandører eller stort gjennomtrekk av konsulenter.

Bildet er dermed tosidig. Det er en fordel for virksomhetene å benytte en større leverandør som er i stand til å tiltrekke seg kompetanse og bygge opp fagmiljøer som bidrar til at de kan etablere løsninger som mindre virksomheter normalt ikke har mulighet til selv. Virksomheten er samtidig avhengig av å opprettholde et minimum av bransje- og løsningskunnskap. En positiv sikkerhetsmessig effekt av tjenesteutsetting forutsetter at virksomheten selv skaffer seg en ny type sikkerhetskompetanse på hvordan de skal sikre og følge opp oppdragene som settes ut. Dette gir andre utfordringer enn det å ha tjenesten internt. Virksomheten må ha tilstrekkelig bestillerkompetanse i forhold til dialogen med leverandøren for å kunne stille krav og følge opp med kontroller og testing.

---

[24] Forbrukerrådet (2014): *Tåkete vilkår i skyen*. Publisert på www.forbrukerradet.no 31.01.2014.

[25] For eksempel bruk av web-baserte gratismoduler på offentlige webportaler, som kan bidra til at personlig informasjon tilkommer kommersielle aktører.

Det er mangel på personell som forstår den tekniske risikoen på tvers av infrastrukturer og verdikjeder, og er løsningsarkitekter som kan bistå virksomheter med etablering av grunnleggende sikkerhetsarkitektur på tvers av en portefølje for å sikre god utnyttelse av investeringer og tilrettelegging for fremtidige digitaliseringsbehov. Sikkerhetsarkitekter forstår både landskapet fra sikkerhetskrav i standarder og lover til det tekniske bildet. Denne kompetanse er også viktig ved tjenesteutsetting for å sikre grensesnitt mellom leverandører og for eksempel miljøer som er driftet internt i en virksomhet. Vi viser for øvrig til omtale av skytjenester i punkt 23.7.3 «Juridiske forhold ved skytjenester» og de øvrige samfunnsfunksjonene i del III «Sårbarheter i kritiske samfunnsfunksjoner» for ytterligere diskusjoner rundt tjenesteutsetting.

19.8 Vurderinger og tiltak

19.8.1 Etablere en overordnet nasjonal kompetansestrategi innen IKT-sikkerhet

Justis- og beredskapsdepartementet bør sammen med Kunnskapsdepartementet utarbeide en overordnet nasjonal strategi for å sikre en langsiktig oppbygging av kompetanse innen IKT-sikkerhet i det norske samfunnet. En slik strategi må dekke tiltak for å bygge opp kapasitet innen både forskning og utdanning.

Hensikten er å sikre langsiktig finansiering, slik at ikke kompetansemiljøer forvitrer mellom finansierte prosjekter. Tiltaket er begrunnet i at Forskningsrådet i dag bare gir prosjektstøtte, og ikke midler for å opprettholde fagmiljøer. Utvalget mener det er lite trolig at universitets- og høyskoleinstitusjonene klarer å løse dette ved egne omprioriteringer. I tillegg bevilger Justis- og beredskapsdepartementet svært lite midler til forskning. Justis- og beredskapsdepartementet er primæradressat for tiltaket fordi de har fått samordningsansvaret for forebyggende IKT-sikkerhet i sivil sektor.[26]

19.8.2 Prioriteringer i en overordnet strategi

Punktene under utdyper hva utvalget mener bør inngå som prioriteringer i en overordnet strategi. Utvalget merker seg at flere av de foreslåtte tiltakene samsvarer godt med Justis- og beredskapsdepartementets egen FoU-strategi.[27] Det er også viktig å presisere at flere av tiltakene bør iverksettes av henholdsvis Justis- og beredskapsdepartementet og Kunnskapsdepartementet i påvente av at den overordnede strategien blir utarbeidet.

1. *Etablere en langsiktig plan for å bygge opp og vedlikeholde forskningskapasitet*

Det er prisverdig at Norges Forskningsråd (NFR) har lansert IKTPLUSS-programmet med en sterk satsing innenfor informasjons- og IKT-sikkerhet. Programmet løper over ti år og vil kunne tilby tiltrengte forskningsmidler til dette området. Man må imidlertid merke seg at som for alle NFR-programmer tilbys det tidsbegrenset prosjektstøtte. Det vil derfor ikke kunne finansiere faste stillinger og heller ikke gi lengre tidshorisont enn lengden av hvert enkelt prosjekt, som regel fire til fem år. De norske FoU-miljøene innenfor IKT-sikkerhet er i stor grad små og har et relativt beskjedent antall faste stillinger. Det varierer også i hvilken grad disse miljøene er samlokalisert med stedene der volumproduksjonen av IKT-kandidater foregår. For eksempel har informatikkmiljøene ved UiO og NTNU relativt sett liten aktivitet innenfor IKT-sikkerhet.

Selv om Forskningsrådet gir verdifull støtte til forskningsprosjekter innenfor IKT-sikkerhet, vil midlene bare være prosjektbaserte og derfor ikke gi en varig oppbygging av forskningskapasiteten ved norske universiteter og høyskoler. Samferdselsdepartementets støtte til Robuste nett-senteret ved Simula, som helt nylig er blitt ytterligere styrket gjennom Simula@UiB, er derfor et svært positivt eksempel. Det samme gjelder støtten Justis- og beredskapsdepartementet har gitt til CCIS ved Høgskolen i Gjøvik. Oppbyggingen av forsknings- og undervisningsmiljøer gjennom de siste årene har i stor grad vært basert på støtte fra eksterne kilder. I denne sammenheng viser særlig etableringen av CCIS at det er mulig å få til et langsiktig samarbeid med både private og offentlige aktører.

Siden Justis- og beredskapsdepartementet har samordningsansvar for forebyggende IKT-sikker-

[26] Statsministerens kontor (2013): *Overføring av samordningsansvaret for forebyggende IKT-sikkerhet fra Fornyings-, administrasjons- og kirkedepartementet til Justis- og beredskapsdepartementet*. Kgl. res. 22.03.2013.

[27] Justis- og beredskapsdepartementet (2015): *FoU-strategi for samfunnssikkerhet 2015–2019*.

het, har departementet et særlig ansvar for å sikre tilstrekkelig nasjonal forskningskapasitet innenfor IKT-sikkerhet og bekjempelse av IKT-kriminalitet. Selv om Justis- og beredskapsdepartementet har vært med på å støtte CCIS, er JDs FoU-bevilgninger fremdeles lave. Utvalget ser det derfor som svært positivt at JD ønsker å etablere strategiske partnerskap med enkelte utdannings- og forskningsinstitusjoner innen blant annet IKT-sikkerhet, og at JD har som målsetting at det settes av midler til å utføre forskning, utredning og evalueringer i forbindelse med større tiltak innen samfunnssikkerhet. *En naturlig konsekvens av dette er at JD nå øker sine FoU-bevilgninger rettet mot IKT-sikkerhet. Planen bør også omfatte andre relevante aktører, blant annet forsvarssektoren, Nærings- og fiskeridepartementet og andre relevante departementer og myndigheter.* Utvalget vil samtidig understreke viktigheten av at en slik satsing er innrettet mot et begrenset antall forskningsmiljøer for å sikre høy kvalitet.

2. *Opprettholde forskningsinnsatsen på IKT-sikkerhet*

Utvalget ser svært positivt på Forskningsrådets nye forskningsprogram IKTPLUSS. Programmet kommer etter at det over tid har vært bevilget relativt lite midler til forskning på IKT-sikkerhet. Gjennom å fokusere på «Et trygt informasjonssamfunn» vil programmet ha mulighet til å styrke kvaliteten og øke dristigheten og relevansen i norsk IKT-forskning innenfor samfunnssikkerhet generelt og IKT-sikkerhet spesielt. Både programmets langsiktige tidshorisont og det årlige omfanget tilsier at det kan ha påvirkningskraft utover de enkeltprosjektene som støttes.

Sikkerhet er imidlertid bare ett av flere temaer som IKTPLUSS dekker. *Utvalget vil derfor understreke viktigheten av at Forskningsrådet opprettholder satsningen på IKT-sikkerhet på linje med den man hadde i 2015. Det er også vesentlig at Forskningsrådet bevilger forskningsmidler til IKT-sikkerhet etter at programmet er avsluttet.*

Utvalget observerer en generell mangel på kunnskap om de økonomiske tapene som følge av digital sårbarhet og hva forebyggende IKT-sikkerhet koster. Dersom slike sikkerhetshensyn skal få nok oppmerksomhet og tyngde inn i beslutningsprosesser, bør de økonomiske sidene også synliggjøres. Se punkt 7.2.1 «IKT-kriminalitet» om kostnaden ved IKT-kriminalitet.

Utvalget anbefaler at sikkerhetsøkonomi blir et forskningstema inn i Forskningsrådets programmer for IKT-sikkerhet.

3. *Innføre krav til IKT-sikkerhetsfag for alle IKT-bachelorgrader*

Utvalget støtter de anbefalingene som er gjort av ACM[28] om hvilke kurs som bør inngå i en generell IKT-utdanning. Kunnskapen som formidles gjennom disse utdanningene, danner grunnmuren for å oppnå god IKT-sikkerhet i samfunnet. Nylig har også NSM kommet med en anbefaling om at alle IKT-utdanninger bør inneholde minst ett obligatorisk kurs innen IKT-sikkerhet.

Utvalget mener at alle bachelorutdanninger i Norge innenfor IKT må inneholde minst 15–20 studiepoeng med fag som omhandler IKT-sikkerhet. Det er viktig at tilbydere av IKT-relaterte bachelorprogrammer går igjennom studiene sine og sørger for at disse dekker vesentlige deler av informasjons- og IKT-sikkerhet. Et slikt tiltak vil i utgangspunktet ikke nødvendigvis medføre store ekstra kostnader for den enkelte institusjon, men først og fremst være et spørsmål om interne prioriteringer. Dette tiltaket samsvarer med anbefalingene i Sikkerhetsfaglig råd fra NSM.

Omfanget av IKT-relaterte kurs er vanligvis 10 studiepoeng. Det skulle tilsi at den totale mengden lærestoff relatert til IKT-sikkerhet bør utgjøre minst to kurs i løpet av et bachelorstudium. Nå dekkes mye av dette stoffet gjennom andre kurs, men utvalget vil likevel anbefale at enhver IKT-bachelor inneholder minimum ett obligatorisk kurs i IKT-sikkerhet.

4. *Øke kapasiteten på masterutdanning innen IKT-sikkerhet*

Utvalget mener det må etableres tilstrekkelig kapasitet på masterutdanning med spesialisering innen IKT-sikkerhet. Dette gjelder særlig ved de store universitetene og høyskolene som har slik aktivitet allerede i dag. Et slikt løft vil kreve tilførsel av midlertidige utvidelsesmidler.

Dette begrunnes i den forholdsvis lave kapasiteten ved UiO og i manglende tilbud innenfor IKT-sikkerhet ved NTNUs studieprogram for datateknikk. Det bør samtidig legges til rette for at studenter fra høyskoler og universiteter som ikke har masterprogram i IKT-sikkerhet, har mulighet til å fortsette på masterstudier ved læresteder som har slike studier.

Økt utdanningskapasitet innen avansert IKT-sikkerhet vil først og fremst møte det innenlandske behovet for slik kompetanse i alle sektorer. Imidlertid vil det også kunne styrke vår konkur-

[28] Se punkt 19.4.3 «Høyere utdanning».

ranseevne og åpne nye muligheter for norsk næringsliv til å møte en økende internasjonal etterspørsel etter både kvalifisert personell og tekniske løsninger innen IKT-sikkerhet.[29]

5. *Styrke nasjonal forskningskompetanse i kryptografi*

Bruk av kryptografi er en forutsetning for sikker informasjonsutveksling på Internett. Selv om trygg ende-til-ende-kommunikasjon forutsetter mer enn bare kryptografi, er kryptografi i en særstilling når det gjelder kunnskap som må være på plass for å understøtte sikker kommunikasjon. Bruk av foreldede, eller av andre årsaker utrygge, kryptosystemer kan føre til at kommunikasjon blir avlyttet, eller at man ikke kan stole på identiteten til andre aktører.

Kryptografi baserer seg i stor utstrekning på avanserte matematiske metoder. Det er derfor en langsiktig prosess å bygge opp kompetanse- og forskningsmiljøer. Slik kunnskap må også vedlikeholdes dersom den skal være relevant.

Det er ikke gitt at kryptosystemene som blir brukt i dag, er trygge. Systemene kan være foreldet, eller de kan til og med ha blitt utviklet for at de skal kunne knekkes. Uten avanserte nasjonale miljøer vil norske myndigheter og bedrifter måtte forholde seg til utenlandske aktører for å innhente kvalifiserte vurderinger og råd om kryptografiske systemer. Dette vil være en svært uheldig situasjon sett i et sikkerhetsperspektiv.

Utvalget mener det er vesentlig at Norge bygger opp og vedlikeholder kompetente forskningsmiljøer innen kryptografi som kan bidra med veiledning og verifikasjon ved implementering av systemer med kryptografiske sikkerhetsmekanismer. Som ansvarlig departement for sikkerhet og beredskap tilfaller det derfor JD i samarbeid med FD å gå inn med tilstrekkelige langsiktige midler for å sikre nødvendig oppbygging og vedlikehold av nasjonal kompetanse innen kryptografi. Dette bør primært gjøres gjennom å støtte eksisterende miljøer og ikke gjennom å bygge opp nye. Det må også vurderes om dette kan gjennomføres slik at nøkkelpersonell i slike grupper kan sikkerhetsklareres.

En slik satsing samsvarer med NSMs ønske om å videreutvikle en nasjonal kryptopolitikk for å sikre nødvendig nasjonal kryptokompetanse og utvikling av kryptoutstyr for høygradert informasjon.

6. *Opprette øremerkede stipendiatstillinger som kan sikkerhetsklareres*

For å sikre tilgang på høyt kvalifiserte personer mener utvalget at det bør opprettes øremerkede stipendiatstillinger innenfor IKT-sikkerhet for personer som kan sikkerhetsklareres.

Dette begrunnes i at FFI har utfordringer med å få tak i godt kvalifisert personell som kan klareres. Utvalget vurderer dette som en voksende utfordring, der også andre aktører, som NSM, CCIS og politiet, vil ha sikkerhetsklarering som en forutsetning. Kravet om sikkerhetsklarering er en spesiell utfordring innen IKT-sikkerhetsarbeid. Det er eksisterende ordninger som sikrer Forsvaret tilgang på klarert IKT-sikkerhetspersonell.[30]

7. *Øke oppmerksomheten rundt IKT-sikkerhet og personvernrelaterte problemstillinger*

Utvalget mener at IKT-sikkerhets- og personvernrelaterte problemstillinger må få en større plass i relevant høyere utdanning.

For IKT-sikkerhet vurderer utvalget særskilt lederutdanninger, for å sikre tilstrekkelig kompetanse og forståelse for problematikken. Dette er begrunnet i at det endelige ansvaret for IKT-sikkerhet i en virksomhet alltid vil ligge hos den øverste ledelsen. Det gjelder selv om ledelsen verken har formal- eller realkunnskap om IKT-sikkerhet. For eksempel har lederutdanninger som siviløkonomstudiet ved Norges Handelshøyskole per dags dato svært lite opplæring i IKT-sikkerhet. Tilsvarende finnes det heller ingen formelle krav, slik det gjør for HMS-arbeid, om at en virksomhets øverste leder må ha gjennomført opplæring i IKT-sikkerhet. *Et tiltak kan være å innføre krav til rapportering om IKT-sikkerhet i årsmeldinger* slik beskrevet i punkt 23.5 «Redegjørelse for IKT-sikkerhet bør inngå i årsmeldinger».

Personvernrelaterte problemstillinger gjelder i særlig grad for juridiske og helserelaterte utdanninger.

Bevissthet og kompetanse om IKT-sikkerhet henger naturlig sammen med den enkeltes generelle kunnskap om de IKT-systemene man bruker. Uten grunnleggende forståelse av disse er det vanskelig å opprettholde tilstrekkelig sikkerhet. Det er derfor vesentlig at alle høyere utdanninger inkluderer tilstrekkelig opplæring i fagspesifikk IKT-kunnskap.

---

[29] *The 2015 (ISC)^2 Global Information Security Workforce Study.*

[30] Cyberforsvaret har Forsvarets Ingeniørhøgskole, som utdanner ingeniører med lederutdanning for Forsvarets behov.

8. *Gjennomføre tiltak rettet mot grunnskole og videregående opplæring*

Skal vi sikre trygg bruk av IKT, og Norges fremtidige deltagelse i utviklingen av fremtidens IKT-teknologi, er vi avhengige av kontinuerlig å heve det generelle kompetansenivået. Dette arbeidet må starte allerede i grunnskolen, slik det nå skjer i en rekke sammenlignbare land. Utvalget har derfor valgt å samle noen eksempler på tiltak:

Etterprøve læringsutbytte i trygg bruk av IKT. Utvalget mener at dagens program for opplæring i digital kompetanse i grunnskolen i stor utstrekning dekker de grunnleggende behovene det enkelte individet har. Opplæring i digital dømmekraft er spesielt viktig for å sikre forsvarlig bruk av sosiale medier og andre kommunikasjonsprogrammer. Det er viktig å evaluere hvordan denne undervisningen fungerer i praksis, og hvilket læringsutbytte elevene faktisk sitter igjen med. Utvalget er kjent med at Senter for IKT i utdanningen utfører undersøkelser om både digitale verktøy i skolen og læreres og elevers digitale kompetanse.[31] Undersøkelsen fra 2011 har vært kritisert[32] for at den kun kartlegger «operativ bruk» av datamaskiner, uten å se på lærernes forutsetninger for å undervise i hvordan datamaskinene faktisk fungerer. *Her er det vesentlig at man ser på hvilken kompetanse lærerne har for å gjennomføre slik opplæring. Etterutdanning av lærere kan være en nødvendig følge av tiltaket.* NSM har også anbefalt at IKT-sikkerhet innarbeides i lærerutdanningen.

Øke oppmerksomhet rundt teknisk bruk av IKT. Skoleverket retter primært oppmerksomheten mot nettvett og regler for personvern på Internett og i sosiale medier. Dette er nødvendig kunnskap som alle trenger. Bruk av IKT forutsetter imidlertid også økt kjennskap til de tekniske aspektene ved maskin- og programvare. Dette gjelder for alle typer personlige maskinplattformer som mobiltelefoner, nettbrett og PC-er. Elevene må forstå behovet for oppdatering av programvare, jevnlige sikkerhetskopier og farene ved ukritisk bruk av nedlastet programvare og nettbaserte tjenester. *Utvalget anbefaler derfor at opplæring i digitale ferdigheter i grunnskole og videregående skole utvides til også å gi kompetanse i relevante tekniske aspekter ved IKT.* Et viktig steg på veien vil være å sørge for at undervisning i programmering blir tilgjengelig i alle skoler, og at innføring i informasjonssikkerhet gis tilsvarende oppmerksomhet.

Bygge ut tilbud om undervisning i programmering. Fravær av avansert IKT-opplæring i skolen risikerer å sette Norge i en situasjon hvor vi primært blir et samfunn som bare forbruker informasjonsteknologi. Det er derfor positivt at regjeringen vil starte forsøk med programmering i grunnskolen fra 2016. Det er vesentlig at denne satsingen raskt blir bygd ut til alle skoler, og at den får et innhold som gjør den relevant for bruk i andre emner og for videre studier. *Kunnskapsdepartementet bør derfor utarbeide en plan for hvordan dette skal gjennomføres.* Det kan gjøres i samarbeid med allerede eksisterende frivillige organisasjoner, samt med IKT-industrien, etter mal fra Finland.

Skal satsingen lykkes på lang sikt, forutsetter det også opplæring av både nåværende og fremtidige lærere. Det er også verdt å merke seg at selv om dette nå ser ut til å starte opp, ligger vi et godt stykke etter land det er naturlig å sammenligne seg med. *Det kan derfor allerede nå være på sin plass å vurdere hva som blir neste steg når tilbudet er etablert. Det bør vurderes hvordan opplæring i algoritmisk tenking og bruk av programmerbare digitale verktøy kan integreres tidligere i den ordinære undervisningen.*

Behov for IKT-sikkerhet i elektrofag. Det er ikke klart ut fra læringsmålene om IKT-sikkerhet er dekket i tilstrekkelig grad i rene elektrofag. Dette gjelder spesielt automatiseringsfaget, der emnet ikke inngår i læreplanen. Kontrollsystemer for temperatur, lys og luft i bygninger styres ofte via nettet, og det er vesentlig at uvedkommende ikke har tilgang til disse. *Utvalget mener det bør foretas en gjennomgang av læreplanene i alle elektrofag for å vurdere om disse er tilfredsstillende med tanke på hvordan de dekker IKT-sikkerhet.*

Revidere læringsmålene i fagene Informasjonsteknologi 1 og 2. Informasjonsteknologi 1 og 2 er allmennfag og gir grunnleggende kunnskap om IKT. Som del av den studiespesialiserende videregående utdanningen skal de også forberede elevene på videre studier innen området. Siden fagene ikke bygger på hverandre, er imidlertid det samlede kunnskapsnivået man kan forvente at ferdige kandidater oppnår, begrenset. En konsekvens av dette er at studenter som kun tar Informasjonsteknologi 2, ikke får opplæring i IKT-sikkerhet. Det er dessuten en lav grad av integrering mellom kursene og høyere utdanninger innenfor IKT i universitets- og høyskolesektoren. Ingen av kursene inngår som forkrav for videre studier i IKT, da disse stort sett bare forutsetter generell studiekompetanse og for enkelte studieretninger også fordypning i matematikk. *Utvalget mener derfor at*

[31] Sjette utgave het «Monitor Skole 2013».
[32] NOU 2013: 2 *Hindre for digital verdiskaping.*

læringsmålene i Informasjonsteknologi 1 og 2 er modent for revisjon, slik at elever som tar disse fagene, går ut med kunnskap om informasjonssikkerhet som er relevant for videre studier.

Kapittel 20
Styring og kriseledelse

Styring og kriseledelse bygger på de grunnleggende prinsippene om ansvar, likhet, nærhet og samvirke (se punkt 8.1 «Overordnede mål for IKT-sikkerhetsarbeidet»). Målsettingen er å opprettholde konstitusjonelle funksjoner og virksomhet i prioriterte deler av forvaltningen under ulike former for påkjenninger.

Ansvaret for en rekke viktige samfunnsoppgaver er delegert til kommunene, og den kommunale forvaltningen spiller en svært viktig rolle i mange krisesituasjoner. I norsk statsadministrasjon er videre en rekke faglige virkefelt skilt ut og lagt til direktorater, mens Fylkesmannen er statens representant i fylket, med blant annet ansvar på vegne av flere departementer og direktorater. Veiledning, oppfølging og tilsyn med kommunenes beredskapsarbeid er i tillegg til samordning en viktig oppgave for Fylkesmannen (se punkt 8.2 «Sentrale myndighetsaktører med særlig ansvar for oppfølging av IKT-sikkerhet»).

Å kunne ivareta styring og kriseledelse på sentralt, regionalt og lokalt nivå er kritisk avhengig av fungerende og pålitelige IKT-systemer. I hovedsak dreier dette seg om administrative kommersielle støttesystemer og ekomtjenester.

Innenfor visse deler av forvaltningen er det spesielle krav til egne IKT-systemer som skal kunne bidra til en ekstra sikkerhet for å opprettholde funksjonalitet. For størstedelen av forvaltningen, både på sentralt, regionalt og lokalt nivå, foreligger det imidlertid ingen bestemte krav til systemer, men det er et krav at virksomhetene på alle nivåer definerer hvilke tjenester som er absolutt nødvendige for å kunne opprettholde en minimumsdrift nærmest uansett hva som skjer, og hvilke IKT-systemer som dermed må være fungerende. I tillegg skal virksomhetene ha kontinuitetsplaner og beredskap dersom viktige systemer svikter.

20.1 IKT-systemer for beredskap og krisehåndtering

20.1.1 Hva er en krise?

En krise defineres som en hendelse som har potensial for å true viktige verdier og svekke en organisasjons evne til å utføre viktige funksjoner. En krise kan være en tilstand som kjennetegnes av at samfunnssikkerheten eller andre viktige verdier er truet, og at håndteringen utfordrer eller overskrider kapasiteten og/eller kompetansen til den organisasjonen som i utgangspunktet har ansvaret for denne.[1]

Dette kapittelet handler om det krisehåndteringssystemet som trer i kraft ved IKT-hendelser som er så omfattende at det får tverrsektorielle samfunnsmessige konsekvenser. Digitale sikkerhetsutfordringer, spionasje, sabotasje og terror, samt behovet for å avdekke, håndtere og etterforske digitale angrep omtales i kapittel 21 «Avdekke og håndtere digitale angrep».

En digital krise kan oppstå når viktige digitale systemer svikter og konsekvensen av bortfallet rammer mange. Krisen får betydelige konsekvenser for samfunn, næringsliv og individer.

Med sikkerhetspolitisk krise menes en krise som utfordrer statens territorielle integritet og politiske suverenitet, men uten at det dreier seg om et militært angrep i tradisjonell forstand. En slik krise kjennetegnes av å være i en uklar gråsone mellom krig og fred. Politisk-militært press fra en annen stat, omfattende terroraksjoner og alvorlige cyberangrep er eksempler på situasjoner som kan forårsake slike kriser.[2]

Mange IKT-kriser har et annet opphav enn ren svikt i IKT-systemer eller infrastruktur, de tekniske systemene kan svikte som følge av andre hendelser. Naturhendelser kan føre til at kommunikasjonsinfrastruktur skades og mobilnettet fal-

[1] St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet*.

[2] Forsvarsdepartementet (2015): *Et felles løft*. Ekspertgruppen for Forsvaret av Norge.

ler ut. Dette påvirker i stor grad evnen til raskt å håndtere situasjoner og opprettholde nødvendig funksjonalitet for de virksomhetene som blir rammet.

20.1.2 Sentral kriseledelse

Sentral kriseledelse er knyttet til et departements evne til å være lederdepartement, håndtere alle typer kriser i egen sektor og yte bistand til andre departementer i kriser som involverer flere sektorer.

Hvert enkelt departement har primæransvaret for egne IKT-løsninger for å kunne opprettholde egen styring og kriseledelse. I dette ansvaret ligger at departementet selv må velge å ta i bruk løsninger som er sikre nok i forhold til behovet. Dette følger av ansvarsprinsippet.

Overordnede bestemmelser og krav til departementenes styring og krisehåndtering fremgår av kgl.res. 15. juni 2012 *Instruks for departementenes arbeid med samfunnssikkerhet og beredskap, Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering*.

Departementenes oppgaver i krisesituasjoner er i hovedsak å innhente og bearbeide informasjon til bruk i faglig rådgivning og tilrettelegging overfor politisk ledelse, vurdere og samordne tiltak, koordinere informasjon til og fra underliggende etater, utstede fullmakter og ivareta og utøve en helhetlig informasjonsstrategi. Disse oppgavene krever fungerende og sikre IKT-løsninger.

Av instruksen går det frem at departementene skal ha planer for å kunne ivareta sine mest kritiske samfunnsoppgaver nærmest uavhengig av hva som skjer. I dette ligger implisitt krav om at de IKT-systemene som departementene er avhengige av for å ivareta driften, er robuste og sikre, og at departementene har planer for manuelle løsninger hvis det skulle oppstå svikt i IKT-systemer eller ved strømbrudd. Redundante løsninger kan være for eksempel doble linjer, reservestrøm, satellitt-telefoni med mer. Konkrete krav til sikkerhet og funksjonalitet i IKT-løsningene fremgår verken av instruksen eller andre bestemmelser.

Det finnes både administrative og politiske ordninger for krisehåndtering på sentralt nivå, som for eksempel Kriserådet, Krisestøtteenheten og Regjeringens kriseråd. Disse er omtalt i den kongelige resolusjonen som er nevnt ovenfor.

Håndtering av IKT-hendelser/-kriser

Samfunnssikkerhetsprinsippene gjelder også for håndtering av IKT-hendelser – både hendelser som er direkte knyttet til svikt i eller angrep på IKT-systemer, og hendelser som er en følge av svikt i sentrale systemer (se kapittel 7 «Utilsiktede og tilsiktede IKT-hendelser»). Alle virksomheter skal ha planer for håndtering, og de etablerte ordningene for situasjonshåndtering og informasjonsdeling gjelder også for IKT-hendelser.

Nasjonal sikkerhetsmyndighet har imidlertid på vegne av Justis- og beredskapsdepartementet utarbeidet en modell for forebygging og håndtering av IKT-sikkerhetshendelser, det vil si angrep mot IKT-systemer og digitale infiltrasjonsforsøk. Her understrekes det at hver enkelt virksomhet skal ha iverksatt tiltak som kan forebygge IKT-hendelser og bidra til å avdekke forsøk på angrep. Det gis videre anbefalinger til etablering av sektorvise responsmiljøer. Hovedsakelig omhandler modellen for hendelseshåndtering retningslinjer for informasjonsdeling.[3] Modellen og mekanismer for håndtering av IKT-sikkerhetshendelser blir ytterligere omtalt i kapittel 21 «Avdekke og håndtere digitale angrep».

Når en IKT-sikkerhetshendelse får alvorlige konsekvenser, for eksempel ved at den forårsaker svikt i kritisk infrastruktur eller kritiske samfunnsfunksjoner, vil det imidlertid være behov for at de etablerte krisehåndteringsmekanismene i Norge trer i kraft, blant annet for å håndtere og minimere uønskede samfunnsmessige konsekvenser og bidra til informasjonsflyt på tvers av sektorer og nivåer av myndighetsorganer.

Nasjonalt beredskapsplanverk, rammeverk

Justis- og beredskapsdepartementet, Forsvarsdepartementet og Statsministerens kontor har etablert et sektorovergripende rammeverk for nasjonalt beredskapsplanverk. Rammeverket er et oppslagsverk som både gir oversikt over sentral krisehåndtering – aktører, roller og ansvar – og en veiledning i hvordan kriser håndteres på sentralt nivå.

En del av rammeverket vil være et planverk som skal gi grunnlag for krisehåndtering på områder der det ikke eksisterer nasjonale scenariobaserte planer.[4] I denne sammenheng er det også vurdert om det skal utarbeides sektorovergri-

[3] *Modell for håndtering av IKT-sikkerhetshendelser – anbefalinger og retningslinjer*, brev til departementene fra Justis- og beredskapsdepartementet 18.11.2014.

pende beredskapsplaner for flere scenarioer enn de som foreligger per i dag.[5]

Sivilt beredskapssystem (SBS)

Nasjonalt beredskapssystem er basert på, og koordinert med, NATOs krisehåndteringssystem og består av én militær og én sivil del: Beredskapssystem for Forsvaret (BFF) og Sivilt beredskapssystem (SBS). SBS inneholder også tiltak rettet mot håndtering av IKT-relaterte hendelser. Hensikten med systemet er at man skal kunne gjennomføre koordinerte og forhåndsplanlagte tiltak på nasjonalt nivå. Virkeområdet er sektorovergripende kriser i fredstid som er forårsaket av alvorlige tilsiktede hendelser eller trusler om slike, og kriser med en sikkerhetspolitisk dimensjon inklusiv væpnet konflikt eller trusler om slike. Det fremgår av Sivilt beredskapssystem (SBS) at departementene skal utarbeide egne beredskapsplaner basert på SBS som utdyper tiltak der departementet har et direkte handlingsansvar i egen sektor. De ulike sektordepartementene skal også bidra til jevnlig revisjon av tiltak i SBS, slik at disse til enhver tid er oppdatert.

En rekke handlingsbeskrivelser i SBS eller i underliggende beredskapsplaner vil også inngå i ulike sektorplanverk, som for eksempel Politiets beredskapssystem eller Nasjonal helseberedskapsplan. SBS setter ikke annet sektorplanverk til side, men gjør det mulig med en koordinert iverksetting av tiltak besluttet på tvers av ulike departementer og sektorer i en situasjon da det er viktig med politisk styring.[6]

Politiet har etablert et eget planverk, Politiets beredskapssystem (PBS). Dette er et eksempel på sektorplanverk som bør avstemmes med det nasjonale systemet. Utvalget er kjent med at det er noen mangler i systemet som gjør at det per i dag ikke er avstemt med SBS. Ansvaret for at de ulike sektorplanene er avstemt og koordinert med det nasjonale planverket tilligger hver enkelt sektor.

Støtteverktøy for krisehåndtering

Både på lokalt, regionalt og sentralt nivå er CIM (Crises Incident Manager) valgt som system til krisehåndteringsstøtte. CIM er et nettbasert krisestøtteverktøy som blant annet brukes til deling av informasjon, situasjonsforståelse, tiltakskort og ROS-analyser. Hovedsakelig benyttes CIM av de fleste aktørene i dag til å systematisere og organisere rutinemessige oppgaver, slik at man i en beredskapssituasjon kan få bedre kontroll og mer tid til ledelse og beslutninger.

Som andre kommunikasjonssystemer er CIM avhengig av at funksjonaliteten i ekomnettet opprettholdes for at beredskapsaktører skal kunne benytte seg av krisestøtteverktøyet. Det er en opsjon å bruke CIM lokalt, men da faller muligheten til å dele informasjon vekk. På det enkelte myndighetsnivå, og særlig for kommunene, vil verktøyet CIM kunne ha en viss verdi selv uten forbindelse til andre nivåer.

CIM finnes i flere utgaver og er i dag kun på ugradert plattform.

IKT-systemer i sentralforvaltningen

Departementenes sikkerhets- og serviceorganisasjon (DSS) har et ansvar for å levere sikrede IKT-løsninger til departementsfelleskapet, og vedlikeholder også overordnede retningslinjer når det gjelder sikkerhet for tilknyttede virksomheter.

Fire departementer[7] pluss Statsministernes kontor har valgt å etablere egne IKT-løsninger utenfor DSS.

Som samordningsdepartement har JD tatt et overordnet ansvar for graderte løsninger i sentralforvaltningen. Det foregår nå en etablering og innfasing av flere sikre kommunikasjonssystemer, inklusiv en løsning for sensitiv og lavgradert mobiltelefoni.

I tillegg pågår det et arbeid med å implementere nasjonale IKT-løsninger på ulike graderingsnivåer. KSE-CIM skal implementeres på Nasjonalt BEGRENSET nett i løpet av 2015.

Justis- og beredskapsdepartementet har også en sentral rolle i arbeidet med å videreutvikle en lavgradert mobiltelefonløsning. Dette er implementert hos samtlige departementer, sentrale etater blant annet i justissektoren og flere sentrale beredskapsaktører. Den samme lavgraderte mobilløsningen blir også vurdert av andre statlige aktører, blant annet Stortinget.

Sentrale aktører har også mulighet for å gjennomføre graderte videokonferanser (VTC). Denne kommunikasjonsformen blir hyppig brukt i forbindelse med krisehåndtering på sentralt nivå.

---

4 Det eksisterer i dag nasjonale scenarioplanverk for pandemier, atomulykker og akutt forurensning.

5 Prop. 1 S (2015–2016) Justis og beredskapsdepartementet. Rammeverket er gjort gjeldende fra juli 2015.

6 Systemet ble sist revidert i april 2015.

7 Finansdepartementet (FIN), Forsvarsdepartementet (FD), Utenriksdepartementet (UD) og Justis- og beredskapsdepartementet (JD).

En arbeidsgruppe med deltagere fra JD, DSB og POD har utredet hvordan samarbeidet på direktoratsnivå kan bli bedre under større hendelser og kriser. Som en del av sitt arbeidet har arbeidsgruppen kartlagt graderte og ugraderte IKT-systemer og kommunikasjonsløsninger i forvaltningen.

Sikret offentlig nett (SON) startet som et arbeidsprosjekt i 2007 med Politiets data- og materielltjeneste (Politiets IKT-tjenester) i samarbeid med andre særorganer under politiet.

Arbeidsprosjektet ble videreført som et pilotprosjekt under navnet SON av Justis- og beredskapsdepartementet i 2012. Bakgrunnen for prosjektet var at man ville etablere en teknologisk løsning som kunne benyttes til å beskytte definert kritisk infrastruktur, dele sensitiv (ikke gradert) informasjon og potensielt inkludere flere offentlige departementer med underliggende etater.

SON er et høyhastighets datanett mellom SON-deltagerne som er koblet til Internett, men der deltagerne har kontroll over den fysiske infrastrukturen, i motsetning til det som er tilfellet med alminnelig Internett. Etter at SON er etablert, skal det etter planen være mulig å etablere fellestjenester mellom alle eller mellom enkelte av deltagerne. Eksempler på tjenester er SharePoint-løsninger, felles sikkerhetsløsninger, streaming av TV-signaler, bærere for nasjonale graderte nett, bærere for Forsvarets og politiets IKT-systemer og politiets alarm- og varslingssystem.

20.1.3 Regionalt nivå

Det regionale nivået skal ha etablert egne krisehåndteringsordninger for å ivareta kriseledelse innenfor egen sektor. Krav og føringer til planer og systemer for krisehåndtering blir ivaretatt av overordnet departement innenfor hver sektor. I tillegg har Direktoratet for samfunnssikkerhet og beredskap (DSB) et samordningsansvar på etatsnivå og ansvar for embetsstyringen til Fylkesmannens (FM) samfunnssikkerhetsansvar, jf. sivilbeskyttelsesloven[8]. De prinsippene, lovene og forskriftene som gjelder for styring og kriseledelse på det regionale nivået, er også gjeldende for håndtering av alvorlige IKT-hendelser og kriser.

Fylkesmannens beredskapsråd (FBR) er Fylkesmannens viktigste samordningsorgan for både forebygging og krisehåndtering. FBR ledes av Fylkesmannen og har medlemmer fra politiet, Forsvaret, Sivilforsvaret, frivillige organisasjoner og statlige og fylkeskommunale etater som har vesentlige beredskapsoppgaver. I tillegg deltar ofte representanter for andre sentrale beredskapsaktører, som for eksempel virksomheter med ansvar for kritisk infrastruktur og andre samfunnskritiske funksjoner i fylket. Kraftforsyningens distriktssjefer (KDS)[9] deltar også fast i FBR. KDS representerer en samlet kraftbransje på regionalt nivå, og bidrar til å opprettholde oversikt over brudd i kraftforsyningen og gjenopprettingstiltak. I en krisesituasjon kan KDS, sammen med andre relevante aktører, blant annet bidra til å vurdere prioritering og rasjonering av kraft. På ekomområdet finnes per i dag ikke noen tilsvarende ordning, men Telenor deltar i de fleste FBR. Nkom har imidlertid etablert en ordning med et sentralt strategisk element bestående av Nkom og utvalgte tilbydere som skal bistå med råd, veiledning og informasjonsdeling i krisesituasjoner. Nkom er tilgjengelig for å delta på møter i FBR når det vurderes som nødvendig.

I en krisesituasjon har DSB ansvar for å samle inn rapportering fra berørte fylkesmenn og direktorater/tilsyn og sette sammen et situasjonsbilde. Denne rollen er nå formalisert. DSB utarbeider også analyser av samfunnsmessige konsekvenser på tvers av sektorer, både i nåtid og fremtid. Disse oversendes Justis- og beredskapsdepartementet, Krisestøtteenheten og Kriserådet og bidrar til en felles situasjonsforståelse og grunnlag for tiltak. Situasjonsbildet sendes også samlet ut til alle relevante aktører. Dette gjøres via CIM, i tillegg til e-post.

Avhengighet av IKT-/ekomsystemer

Det er et krav at Fylkesmannen skal kunne ivareta sine viktigste funksjoner nærmest uansett hva som skjer. Avhengighet av IKT og kraftforsyning skal inngå i ROS-analyser, og det skal iverksettes tiltak som ivaretar kontinuiteten i de viktigste funksjonene som Fylkesmannen forvalter. Fylkesmannen er ansvarlig for at det utarbeides en helhetlig ROS-analyse for fylket. I denne skal fylkets kritiske infrastruktur og samfunnsfunksjoner og avhengigheter mellom dem belyses. Både private og offentlige virksomheter er inkludert her.

Fylkesmannen er først og fremst avhengig av IKT-systemer for å drifte administrative støtte-

[8] Justis- og beredskapsdepartementet (2011): *Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret*.

[9] Kraftforsyningens distriktssjefer (KDS) er representanter for kraftforsyningen som skal sørge for godt samarbeid og samordning om sikkerhet og beredskap mellom energiselskapene. Se kapittel 13 «Energiforsyning».

systemer og kommunikasjonsløsninger, og har en viktig rolle som statens representant i kriser der regionen er avskåret fra kontakt med sentrale myndigheter. Fylkesmannen har derfor også tilgang til Forsvarets nett, satellitt-telefoni og Nødnett som backup-løsning til offentlige ekom-tjenester.

Fylkesmannen benytter også CIM i sin krisehåndtering og i kommunikasjon med kommunene og offentlige etater.

20.1.4 Lokalt nivå

Uønskede hendelser og kriser oppstår alltid i en kommune. Til å begynne med er det kanskje bare virksomheten selv som er involvert, men etter hvert kan flere aktører komme til. Selv en lokal brann krever bidrag fra og samvirke med flere aktører – både private virksomheter, frivillige organisasjoner, DSB, Sivilforsvaret og nødetatene. Dette er aktører som en kommunal kriseledelse må forholde seg til og kunne kommunisere med. Alle relevante aktører er avhengige av ekomnett og -tjenester for å kommunisere med hverandre, og er prisgitt sikkerhetsnivået i disse.

Større hendelser som berører flere kommuner, løftes til fylkesnivå og gjerne også til høyere nivå i forvaltningen. Dette krever samvirke på tvers av sektorer og virksomheter.

Kommunene har ansvar for mange viktige samfunnsfunksjoner, som spenner vidt i fagområder og gjør at en kommunal kriseledelse må være forberedt på å håndtere hendelser av svært ulik karakter og med svært mange og ulike aktører. Sivilbeskyttelsesloven og forskrift om kommunal beredskapsplikt setter rammene for lokal krisehåndtering.

Forskrift om kommunal beredskapsplikt

Kommunene skal være forberedt på å håndtere alle uønskede hendelser og med utgangspunkt i en helhetlig risiko- og sårbarhetsanalyse utarbeide en overordnet beredskapsplan, inkludert IKT-hendelser – alt fra uønskede hendelser i kommunenes IKT-systemer til større nasjonale IKT-kriser som får konsekvenser for kommunene.

I lov og forskrift stilles det ingen konkrete krav til IKT-sikkerhet, men på samme måte som for det regionale og sentrale nivået ligger dette implisitt ved at nødvendig funksjonalitet er avhengig av fungerende IKT-systemer. Det går imidlertid frem av forskrift om kommunal beredskapsplikt at kommunens ROS-analyse som minimum skal omfatte «særlige utfordringer knyttet til kritiske samfunnsfunksjoner og tap av kritisk infrastruktur».

20.1.5 Sivilt–militært samarbeid i kriser

Politiet har ofte en sentral lederrolle i krisesituasjoner og kan via bistandsinstruksen be Forsvaret om assistanse. Eventuell bistand på IKT-sikkerhetsområdet reguleres på samme måte.

Forsvarsdepartementet har satt i gang et arbeid med å revidere operativt strategisk planverk for kriser og væpnet konflikt / krig. Forsvarets arbeid på dette feltet vil på flere områder basere seg på bidrag fra det sivile samfunnet innenfor rammen av totalforsvaret (se punkt 8.2 «Sentrale myndighetsaktører med særlig ansvar for oppfølging av IKT-sikkerhet»). I denne forbindelse blir det gjort en gjennomgang av totalforsvarskonseptet og det sivile samfunnets støtte til Forsvaret i samarbeid med DSB.[10] Videre har Justis- og beredskapsdepartementet, i samarbeid med Forsvarsdepartementet, bedt DSB om å utrede avhengigheter mellom Forsvarets digitale infrastruktur og den sivile ekominfrastrukturen. Offentlig mobiltelefoni er så langt det eneste felles kommunikasjonsmiddelet for totalforsvarsaktørene innen nasjonal kriseledelse, det vil si sentral kriseledelse, Fylkesmannen, kommunenes kriseledelse, nødetatene, Sivilforsvaret, helseforetakene og Forsvaret.[11]

På vegne av Justis- og beredskapsdepartementet har DSB ansvar for å koordinere de årlige NATO-øvelsene Crisis Management Exercise (CMX) på sivil side. På norsk side er øvelse CMX åpen for deltagelse fra departementer, enkelte sentrale etater og fylkesmenn. Hensikten er å øve både eksisterende konsultasjons- og krisehåndteringsprosedyrer og prosedyrer under utvikling mellom NATO og medlemslandene. Ett av hovedmålene i CMX 2015 var å øve et stort cyberangrep.

20.1.6 Risiko- og krisekommunikasjon

Prinsipper for krisekommunikasjon

I enhver krisesituasjon er behovet for og nødvendigheten av å nå ut med riktig og veiledende informasjon til befolkningen essensielt. Kommunika-

[10] *Støtte til Forsvarssjefens operative planverk*, oppdragsbrev fra Justis- og beredskapsdepartementet til Direktoratet for samfunnssikkerhet og beredskap, 10.02.2015.

[11] FFI-Fakta (2014): *Krisehåndtering i et sårbart cybersamfunn*.

sjon med befolkningen spenner fra varsling og risikokommunikasjon før, under og etter en krise til ren krisekommunikasjon som veileder og informerer under en hendelse. Kommunikasjonen skal begrense usikkerhet om ansvarsforhold, klargjøre hva virksomheten gjør for å løse problemet, redusere omfanget av krisen og formidle hvordan de som er rammet, kan få hjelp og støtte. Krisekommunikasjon inkluderer kommunikasjon med medier, samarbeidspartnere, egne ansatte og befolkningen i alvorlige situasjoner og kriser. En effektiv risiko- og krisekommunikasjon krever fungerende IKT-systemer.

Statens kommunikasjonspolitikk[12] er ment å være utgangspunkt og rammeverk for utarbeidelse av lokale planer og strategier for informasjon og kommunikasjon. Statens kommunikasjonspolitikk omtaler ulike typer kommunikasjon, inklusiv krisekommunikasjon.

Kommunikasjonskanaler og varsling

Myndigheter på ulike nivåer benytter flere ulike virkemidler for å ivareta sitt informasjons- og kommunikasjonsansvar. Det finnes i dag mange ulike kanaler og virkemidler som kan tas i bruk for å informere befolkningen i krisesituasjoner. Eksempler er kringkasting, mediehus, sosiale medier, flygeblader med mer. Valg av kanaler avhenger av hvilke krisesituasjoner en står overfor, hvem som er målgruppene, og hvilke kanaler som er tilgjengelige.

NRK har en spesiell rolle i nasjonal beredskapssammenheng ved at de har en plikt til å formidle informasjon til befolkningen i krisesituasjoner gjennom beredskapskanalen NRK P1. I tillegg foreligger det en nærradioavtale som gjør at NRK kan overføre sine sendinger til andre lokalradiostasjoner ved brudd i eget nett.[13] Denne ordningen ble benyttet under Dagmar i 2011, da NRK falt ut i Møre og Romsdal. Det er stor bevissthet i befolkningen om at myndighetene vil gi nødvendig informasjon over radio, og FM-båndet er i tillegg et svært robust.

Kulturdepartementet har vedtatt å avvikle FM-båndet og heldigitalisere norsk radio innen 2017.[14] Det er imidlertid stilt betingelser som må oppfylles før avviklingen skal kunne gjennomføres. I denne sammenheng er blant annet NRKs og P1s rolle som beredskapsfunksjon omtalt, og departementet har vurdert dekning og lydkvalitet samt forholdet til lokalradioer og bruk av mobilnettet som varslingskanal. Når det gjelder dekning, er det stilt krav om at NRKs radiotilbud må ha digital dekning tilsvarende dagens P1-dekning i FM-nettet, og at frekvensblokkene som er satt av til kommersielle kanaler, til sammen må være utbygd til å dekke minst 90 prosent av befolkningen. Nkom har på oppdrag fra SD og KUD beregnet og målt dekningen for DAB-nettene (Digital Audio Broadcasting) i Norge, og konkluderte i februar 2015 med at de dekningsmessige vilkårene for avvikling er oppfylt.[15]

DSB etablerte i januar 2012 nettstedet www.kriseinfo.no for risiko- og kriseinformasjon. Kriseinfo.no er en portal som samler myndighetsinformasjon i kriser og lenker til relevant informasjon hos andre aktører. I de tilfellene Internett er utilgjengelig, vil informasjon fortrinnsvis måtte gis gjennom andre kanaler. Alternative kommunikasjonskanaler bør være omtalt i beredskapsplanene til myndighetene. Kriseinfo.no publiserer også på Facebook og Twitter.

Hver enkelt kommune og hver enkelt virksomhet har ansvar for å varsle befolkningen ved kriser. I hovedsak benyttes SMS-varsling til dette. Men også varsling via sirener (tyfoner) blir brukt, eksempelvis i industriområdet i Grenland. DSB har gjennom Sivilforsvaret ansvaret for den nasjonale befolkningsvarslingen ved bruk av tyfoner. Disse utløses via FM-båndet. Når FM-båndet legges ned, vil utløsermekanismen mest sannsynlig kobles på Nødnett.

For IKT-hendelser er NSM NorCERT det tverrsektorielle nasjonale IKT-responsmiljøet. Flere andre sektorer er i ferd med å etablere egne responsmiljøer. Dette legger forholdene til rette for på sikt å kunne dele informasjon om trusler, sårbarheter og tiltak og dermed oppnå et mer helhetlig situasjonsbilde og en bedre håndtering av spesielt målrettede angrep og IKT-hendelser (se kapittel 21 «Avdekke og håndtere digitale angrep»).

---

[12] *Statens kommunikasjonspolitikk.* Fastsatt av Fornyings- og administrasjonsdepartementet 16. oktober 2009.

[13] *Avtale om samarbeid om lokalradiostasjonens virksomhet under kriser og katastrofer av 22.01.2007.* Inngått mellom Justis- og beredskapsdepartementet, Norsk rikskringkasting, Telenor Norge AS og Norsk lokalradioforbund.

[14] Meld. St. 8 (2010–2011) *Digitalisering av radiomediet.*

[15] Nasjonal kommunikasjonsmyndighet (2015): *Vurdering av om dekningsvilkår for avvikling av FM er oppfylt.* Dekningsvurderinger for NRKs DAB-nett, de kommersielle DAB-nettene og NRK P1s stereodekning i FM-nettet.

20.2 Sårbarheter knyttet til styring og kriseledelse

I beskrivelsen av sårbarheter vil utvalget spesielt vise til pinseflommen i 2011 og ekstremværet Dagmar samme år. Dette er eksempler på hendelser som fikk konsekvenser for styring og kriseledelse for ulike etater. I begge hendelsene var utfordringen særlig knyttet til samordning mellom aktører som skulle håndtere krisen, og kommunikasjon mellom befolkningen og myndighetene.

Utvalget bruker også funn fra DSBs *Nasjonalt risikobilde 2014*[16], som presenterer et hypotetisk cyberangrep på ekominfrastruktur som et scenario.

20.2.1 Samhandlingsutfordringer og behov for informasjonsdeling

Evalueringer fra en rekke øvelser og reelle hendelser viser at samhandling og informasjonsdeling er både svært viktig og utfordrende i en krisesituasjon. Manglende informasjonsdeling kan blant annet føre til en begrenset felles og oppdatert situasjonsforståelse, noe som er viktig for evnen til krisehåndtering.

Et effektivt samarbeid på tvers av organisasjoner krever at tekniske systemer kan kommunisere og utveksle informasjon, og at de samarbeidende organisasjonene kan samvirke ved å bruke utstyret. I mange tilfeller er disse organisasjonene teknisk heterogene og har ulik kommunikasjonskultur og organisasjonsstruktur. Dette utfordrer samvirke og samarbeid i praktiske krisesituasjoner. 22. juli viste at den eneste felles plattformen for kommunikasjon var mobilnettet, og at viktige aktører ikke fikk mulighet til å utveksle gradert informasjon på grunn av mangel på godkjente systemer og informasjonsutveksling mellom fagsystemer.[17]

Selv om samhandling og informasjonsdeling er nyttig og nødvendig, har utstrakt deling av informasjon også en skyggeside. At flere gis tilgang til informasjon, og at systemer kobles sammen, gir økt sårbarhet. Det blir derfor viktig også å gjøre en verdivurdering av informasjon og kartlegge behovet for beskyttelse av sensitiv informasjon gjennom tilgangskontroll og kryptering.

DSB har nylig stilt sammen funn fra de største øvelsene i perioden 2006–2014. I perioden er det kun under øvelse IKT (2008), øvelse Orkan (2012) og øvelse Østlandet (2013) digital infrastruktur har vært utsatt for påkjenninger som er relevante i denne sammenhengen. Påkjenningene har kommet som følge av naturhendelser. Funn fra øvelsene knyttet til digital infrastruktur kan kort oppsummeres slik: Virksomheter mangler egenberedskap for slike hendelser, herunder nødstrøm og alternative kommunikasjonsløsninger. De som har kommunikasjonsutstyr, mangler brukerkompetanse, og det er uklare ansvarsforhold knyttet til håndtering.

20.2.2 Avhengigheter på lokalt og regionalt nivå, og kompetanseutfordringer

Svært ofte er bortfall av ekomtjenester en følgehendelse av bortfall av kraft. Hvis man er forberedt på og har en beredskap for bortfall av kraft, vil man følgelig stå sterkere i tilfelle bortfall og svikt i ekomtjenester. Funn fra tilsyn med regionalt og lokalt nivå viser at det er ulike oppfatninger om hvilke krav til egenberedskap som gjelder.

I 2012 gjennomførte DSB er utredning om kommunenes beredskap mot bortfall av elektrisk kraft.[18] Utredningen viste at mange norske kommuner vil kunne få store problemer ved langvarig bortfall av elektrisk kraft. Det kom blant annet frem at det er til dels store svakheter knyttet til reservestrøm for viktige samfunnsfunksjoner og tjenester som kommunene har ansvaret for å opprettholde. Mange kommuner ville også fått problemer med å opprettholde nødvendig kommunikasjon dersom ekomtjenester falt bort som følge av strømbrudd.

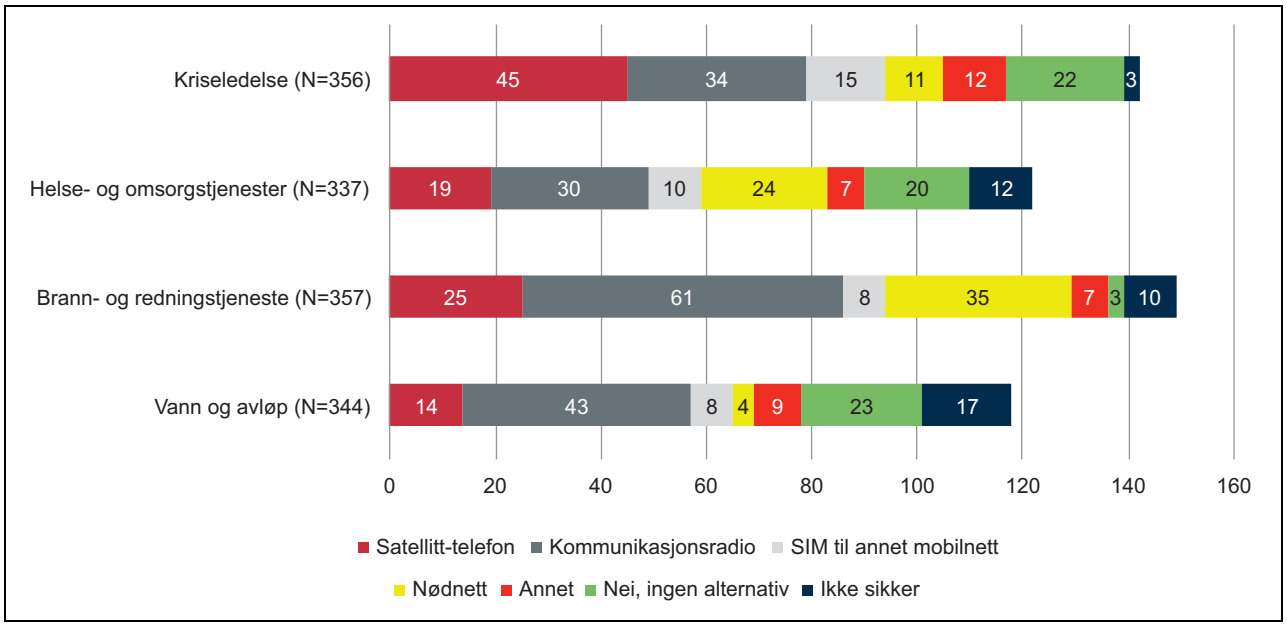
Det er en tydelig sammenheng mellom gjennomføring av risiko- og sårbarhetsanalyser (ROS-analyser) og utarbeidelse av beredskapsplaner og kommunenes sårbarhet overfor bortfall av elektrisk kraft. I kommuner der bortfall av elektrisk kraft var inkludert i ROS-analyser, hadde man bedre oversikt over de utfordringene som kan oppstå, flere forebyggende tiltak var iverksatt, og beredskapsplanverket var i større grad tilpasset og egnet som hjelpemiddel for kommunens kriseledelse enn i kommuner som ikke hadde prioritert dette arbeidet. Videre var det en betydelig andel av kommunene som ikke hadde en beredskapsplan der bortfall av elektrisk kraft var dekket, og mange hadde ikke planlagt for mer enn ett døgns strømbrudd.[19] [20]

---

[16] Direktoratet for samfunnssikkerhet og beredskap (2014): *Nasjonalt risikobilde 2014*.

[17] NOU 2012: 14 *Rapport fra 22. juli-kommisjonen*

[18] Direktoratet for samfunnssikkerhet og beredskap (2012): *Nasjonalt risikobilde (NRB) 2012*, med fordypningsdel: *Kommunenes beredskap mot bortfall av elektrisk kraft.*



Figur 20.1 Alternative kommunikasjonsløsninger i kommunene i 2014.

Kilde: DSB.

Boks 20.1 Pinseflommen 2011

Under pinseflommen i 2011 førte utfallet i Telenors mobilnett til at NVE ikke fikk inn data fra målestasjoner i vassdragene. Disse dataene blir vanligvis sendt automatisk via Telenors mobilnett. Utfallet i mobilnettet gjorde det vanskelig for NVE å følge utviklingen i vannføringen mange steder, særlig den 10. juni, da flommen utviklet seg raskt. NVE kompenserte dette med bruk av modellberegninger og rapporter fra personer ute i felt og ved bruk av fasttelefon og satellitt-telefon.

Nødnett var i 2011 ennå ikke bygd ut i Gudbrandsdalen, og nødetatene hadde analoge sambandsløsninger. En av politiets utfordringer under pinseflommen var knyttet til oversikt og utarbeidelse av et felles oppdatert situasjonsbilde. Det var særlig viktig å opprettholde kommunikasjon med Statens vegvesen for å ha oversikt over fremkommeligheten i veinettet. Politiet hadde likeså behov for å fremskaffe opplysninger om hvor det var størst sannsynlighet for nye skred, og hvor det kunne bli behov for hurtig evakuering. Oversikt over fremkommelighet var også viktig for valg av transportmiddel for innsatspersonell og evakuerte hvis det skulle oppstå ulykker. På grunn av problemer med kommunikasjonen måtte politiet innhente oversikt over fremkommelighet ved å benytte flere alternative kanaler, blant annet informasjon fra lensmenn ute i bygdene og innrapportering via politiets samband og politihelikoptre. Politiet brukte derfor store ressurser på å skaffe seg en oversikt over veinettet. Det var også utfordringer knyttet til kommunikasjon med andre aktører, som kommunal kriseledelse, og til en viss grad innkalling av mannskaper. Politiets mannskaper varsles per telefon, og det er mange som ikke lenger har en fasttelefonlinje hjemme. I noen tilfeller ble det benyttet tjenestebil for å kontakte personell.

Vegvesenet, som skal ha oversikt over fremkommelighet på veinettet, stenge veier, skilte, holde vakt og ikke minst rekvirere driftsentreprenører, baserer i stor grad sin kommunikasjon på mobiltelefoni. Dette gjelder til dels internt, og særlig overfor driftsentreprenører, som de er avhengige av å nå. Under begge hendelsene hadde Vegvesenet store problemer med å nå ut til sine driftsentreprenører. Dette medførte at veier ikke ble effektivt ryddet og reparert fortløpende. Svikt i kommunikasjonen førte også til problemer med å få tak i informasjon fra lokalt nivå om hvilke veier som var fremkommelige. Manglende informasjon fra lokalt nivå medførte problemer med å gi Fylkesmannen, nødetatene og publikum et oppdatert situasjonsbilde av fremkommeligheten i veinettet.

Status for kommunenes beredskap for bortfall av kraft og ekom ble fulgt opp gjennom *Kommuneundersøkelsen* i 2014.[21] I denne undersøkelsen svarte 16 prosent at de ikke hadde, eller var usikre på om de hadde, beredskap for bortfall av elektrisk kraft – mot 40 prosent i 2012. Spørsmålene i 2012-undersøkelsen var imidlertid mer detaljerte og mer konkretiserte. Det er likevel grunn til å tro at situasjonen har bedret seg.

Beredskap for bortfall av ekom:

I 2014 ble også spørsmål om beredskap mot bortfall av ekom berørt, ved at det ble stilt spørsmål om alternative kommunikasjonsløsninger. Figuren over viser variasjoner i type kommunikasjonsløsning innenfor de ulike områdene. Satellitttelefon er i større grad oppgitt som alternativ kommunikasjonsløsning for kriseledelsen enn for de andre områdene.

Selv om myndighetene har iverksatt nødvendige tiltak for å styrke sin robusthet ved å anskaffe alternative kommunikasjonsløsninger og nødstrøm, er man i all hovedsak avhengig av ekomnettet for å kommunisere. Et aspekt ved dette er at robustheten i ekomnettet er geografisk betinget som følge av vår topografi og demografi. Det er store forskjeller mellom spredtbygde distrikter og tettbygde strøk når det gjelder robusthet i underliggende kommunikasjonsinfrastruktur og dekning.[22]

Kompetansebehov på lokalt nivå

Både gjennom DSBs undersøkelser og andre innspill[23] kommer det frem at mangel på IKT-sikkerhetskompetanse både på ledelsesnivå og hos ansatte er en utfordring på lokalt nivå. Dette er også beskrevet i kapittel 15 «Vannforsyning» og i punkt 19.3 «Kompetansesituasjonen i samfunnet». KINS trekker blant annet frem som en sårbarhet at ledelsen har mange tradisjonelle ansvarsområder, og at IKT-sikkerhet er et relativt nytt område som ikke når opp i forhold til andre, «gamle», oppgaver. Dessuten har mange et inntrykk av at dette er teknisk vanskelig.

Mange kommuner mangler dessuten et styringssystem og har for dårlig internkontroll. Videre pekes det på at IKT-sikkerhet anses for å være et teknisk komplisert område, og at det er lite og/eller for dårlig opplæring. Det er et stort behov for kontinuerlig opplæring.

KINS (Kommunal Informasjonssikkerhet) viser til at få eller ingen kommuner har gode reserveløsninger ved bortfall av IKT-systemer over lengre perioder. Årsaken til dette er etter KINS' syn knyttet til kostnader og prioritering av IKT-beredskap, samt at dette er teknisk krevende å etablere og vedlikeholde.

Flere av utfordringene som synliggjøres ved bortfall av ekom og kraft i krisesituasjoner, har også elementer av kompetanseutfordringer ved seg. Kommunene har i liten grad gjort tilstrekkelige ROS-analyser og igangsatt tilstrekkelige tiltak for å styrke egenberedskapen ved bortfall av kritisk infrastruktur. Som et tiltak for å øke kompetansen hos kommunene har Nkom gitt ut en veileder som kan støtte deres ROS-analyser på ekomområdet.[24]

20.2.3 Risiko- og krisekommunikasjon

Både under pinseflommen i 2011 og under Dagmar samme år skapte svikten i telenettet problemer for myndighetenes arbeid med å gi informasjon til befolkningen. Fylkesmannen og kommunene hadde problemer med kommunikasjonen med hverandre og ut til andre aktører, noe som igjen førte til et mangelfullt situasjonsbilde. Under stormen Dagmar var det i tillegg ikke mulig å legge ut informasjon på Internett. Dette ble ytterligere komplisert i Møre og Romsdal da NRK P1 falt ut i lengre perioder.

Under pinseflommen var det et særskilt behov for å informere publikum om at mange veier var stengt som følge av flom og skred. Et brudd i mobilnettet førte imidlertid til at Vegtrafikksentralen tidvis ble overbelastet, noe som reduserte publikums muligheter til å motta informasjon om situasjonen. Kommunene kunne heller ikke gi oppdaterte oversikter, og de hadde ikke kapasitet til å hjelpe publikum som tok kontakt. Mange ringte til politiet, noe som medførte en ekstrabelastning også der.

---

19 Direktoratet for samfunnssikkerhet og beredskap (2012): *Nasjonalt risikobilde (NRB) 2012*, med fordypningsdel: *Kommunenes beredskap mot bortfall av elektrisk kraft.*

20 Direktoratet for samfunnssikkerhet og beredskap (2012): *Kommuneundersøkelsen 2012.*

21 Direktoratet for samfunnssikkerhet og beredskap (2014): *Kommuneundersøkelsen 2014. Status for samfunnssikkerhets- og beredskapsarbeidet i kommunene.*

22 Janne Merete Hagen og Vinh Quam Pham: *Brannvesenets behov for robust informasjonsinfrastruktur for samhandling i krisesituasjoner – en forstudie.* FFI-rapport 2014/01704.

23 Blant annet KINS' svar til Lysneutvalget og NSR (2014): *Mørketallsundersøkelsen – informasjonssikkerhet, personvern, og datakriminalitet.*

24 Nasjonal kommunikasjonsmyndighet (2014): *Robusthet i elektronisk kommunikasjon – veiledning og råd til kommuner.* November 2014.

Siden Internett ikke var rammet av bortfall under pinseflommen, søkte mange informasjon på kommunenes, Fylkesmannens og Vegvesenets nettsider. På grunn av problemene med å skaffe oppdaterte situasjonsbilder var imidlertid informasjonen på sidene ufullstendig.

Både under Dagmar og pinseflommen så man behov for å skape trygghet for bygder som var helt avskjermet, og som ikke hadde mulighet til å motta informasjon om situasjonen. Mange av kommunene uttrykte at en av de største utfordringene var kontakt med de delene av kommunen der telefoni var falt bort. Flere kommuner tok i bruk alternative løsninger for på best mulig måte å opprette en form for kommunikasjon.

Som en følge av bortfall av telefoni under Dagmar hadde befolkningen over store områder ikke mulighet til å nå nødetatene hvis det skulle oppstå kritiske situasjoner. Både kommunene og nødetatene ga uttrykk for at dette var en stor utfordring.

Avvikling av FM-båndet

Overgang til DAB gjør at nærradioer må kjøpe inn nytt utstyr. I NRK er det kommet frem at en del nærradioer kan få problemer med å finansiere dette og dermed videreføre driften. I lokalradioavtalen går det blant annet frem at det skal være teknisk mulig å videreformidle NRKs programmer samtidig og uendret på lokalradiostasjonenes frekvenser i ulike krisesituasjoner. Det er usikkert hvilken reell beredskapsmessig konsekvens overgangen til DAB-radio vil ha. I stortingsmeldingen om digitalisering av radioen[25] pekes det på at det også er andre måter å varsle befolkningen i et område på – for eksempel via SMS – men denne evnen/muligheten må i så fall implementeres hos ansvarlige varslingsaktører som for eksempel politi og andre virksomheter.

I stortingsmeldingen omtales også NRKs beredskapsansvar. Det blir påpekt at NRKs beredskap kan bli svekket hvis digitaliseringen trekker ut i tid – dette fordi FM-nettet blir stadig eldre, noe som kan gi redusert oppetid. Det legges til grunn at NRK skal sørge for de nødvendige investeringene som må til for å opprettholde forsvarlig oppetid, så lenge FM-nettet benyttes.

I meldingen påpekes det at beredskapshensyn er viktige for dekningskravet til kanalen, men at distribusjonsnettet også må være robust, redundant og ha rom for reserveløsninger. Videre fremheves det at det etter hvert har vokst frem flere alternative beredskapskanaler – blant annet kan mobilnettene benyttes til å kringkaste SMS-meldinger til mobiler i et gitt område. En svakhet ved disse systemene er at de i en krisesituasjon kan bli overbelastet. Inntil videre må derfor P1 fremdeles fylle en funksjon som beredskapskanal. Kulturdepartementet skriver videre at de vil ta initiativ til en dialog med Direktoratet for samfunnssikkerhet og beredskap og Nasjonal kommunikasjonsmyndighet for å vurdere om det på sikt vil være grunnlag for å redefinere beredskapsrollen til NRK P1.

20.2.4 Meteorologiske tjenester

I Norge er Meteorologisk institutt (MET) gitt særskilte oppgaver knyttet til meteorologiske tjenester. MET bidrar med meteorologiske og klimatologiske data og tjenester som skal tjene som beslutningsstøtte for en rekke samfunnsområder. Særskilt prioriterte oppgaver er varsling av ekstreme værforhold, som sterk vind, store nedbørmengder, høye bølger og høy vannstand. Varsling av farlige utslipp til luft og hav, for eksempel ved kjernefysiske ulykker, vulkanutbrudd og oljesøl, er viktige nasjonale beredskapsoppgaver, i tillegg til all varsling i forbindelse med redningsoppdrag på land og til havs. Videre er viktige samfunnsfunksjoner som transport, jordbruk, forsvar, luftfart og sjøtransport avhengige av tjenestene.

Sentralt i mange krisehåndteringssituasjoner står evnen til å detektere og overvåke naturfarer. For å kunne ivareta dette er man helt avhengig av meteorologiske tjenester.

Klimadatabaser ved MET vurderes som fellesverdier som det er viktig å beskytte. Slike data lagres derfor også hos Riksarkivet. Overvåking og forskning på klima og tilgjengeliggjøring av data til langsiktig planlegging er viktig, for eksempel for å sørge for at infrastruktur, installasjoner og bygg tar høyde for et nytt og endret klima i fremtiden.

Meteorologisk infrastruktur

Den meteorologiske infrastrukturen i Norge består av automatiske og enkelte manuelle målestasjoner (for alle typer værparametere eller kun for nedbør), værradarer, lidarer, radiosonder, drivende bøyer og satellitter, som alle samler inn værdata og rapporterer jevnlig. I dag kan enkelte observasjonsstasjoner rapportere på minuttbasis, og behovet for tungregnekraft er derfor økende.

For å skaffe tilgang til resultater fra numeriske prognosemodeller er MET avhengig av egne og andres tungregneressurser. Meteorologisk institutt eier per i dag en tungregnemaskin sammen

[25] Meld. St. 8 (2010–2011) *Digitalisering av radiomediet.*

med NTNU. I tillegg har MET et operasjonelt samarbeid med det svenske meteorologiske instituttet (SMHI) om numeriske værprognoser. MET deler tungregneressurser med blant annet SMHI og bruker også SMHIs supercomputer som backup-system. Langtidsvarslene krever ytterligere tungregnekraft, og utføres i dag ved det internasjonale regnesenteret i Storbritannia (ECMWF). ECMWF eies av en rekke europeiske land i fellesskap, og er per i dag ledende innen sitt felt. Kommunikasjonen mellom Oslo og tungregnemaskinene går via Internett/UNINETT (i tillegg til NORDUnet og SUNET til Sverige). Randverdiene fra ECMWF kommer via Internett og RMDCN (dupliserte linjer).

MET er også avhengig av meteorologisk infrastruktur som tilhører andre statsetater, den internasjonale infrastrukturen og infrastrukturen i verdensrommet for å kunne utføre sine tjenester. Det er WMO (World Meteorological Organization) som sørger for at det internasjonale samarbeidet er koordinert, og at landene følger opp forpliktelsene som følger et slikt samarbeid.

Sårbarhet knyttet til meteorologiske tjenester

Den meteorologiske infrastrukturen er sårbar. For eksempel kan sabotasje, IKT-angrep eller naturfenomener slå ut viktige deler av denne infrastrukturen. Dette kan få svært uheldige følger, i og med at meteorologiske tjenester benyttes av en lang rekke kritiske funksjoner, for eksempel atomberedskapen, ekstremværberedskapen, redningstjenesten og oljevernberedskapen. At beslutningsstøtte som skriver seg fra den meteorologiske infrastrukturen, faller ut, kan derfor få svært alvorlige konsekvenser. Den meteorologiske tjenesteproduksjonen er dessuten avhengig av eksterne innsatsfaktorer som elektronisk kommunikasjon og satellittbaserte tjenester. Svikt i eller bortfall av disse innsatsfaktorene vil kunne medføre redusert kvalitet, svikt i produksjonen av og tilgjengeligheten til meteorologiske tjenester.

Den meteorologiske produksjonen er som nevnt tidligere avhengig av ulike inngangsdata og av at kommunikasjonsløsningene som benyttes, er tilgjengelige, blant annet at GSM-nettet ikke faller ut i uvær, eller at måleinstrumentene blir skadet eller faller ut i områdene som rammes.

MET har over tid fokusert på høy tilgjengelighet i egen infrastruktur gjennom redundans på datarom, strøm, kommunikasjon og IKT-tjenester. Driftsovervåking hos MET er en døgnkontinuerlig tjeneste.

Logiske sårbarheter i IKT-systemer og -infrastruktur og tilgjengelighet til riktig kompetanse ved alvorlige avvik vurderes til å være noen av de største sårbarhetene ved meteorologiske tjenester. I tillegg viser MET til at man ved anskaffelser må etterspørre sikkerhetsdokumentasjon fra systemleverandørene, og at ikke alle er like bevisste på systemsikkerhet. MET har opplevd alvorlig avvik. Ved et konkret tilfelle gjennomførte en leverandør en planlagt systemendring, som kunne ha medført alvorlige konsekvenser for infrastrukturen, og dermed viktige leveranser.

UNINETT og CERT-funksjonen

UNINETTs leveranser er kritisk for både innsamling av data, intern kommunikasjon, kommunikasjon til tungregnemaskinene og distribusjon av værvarsler. UNINETT CERT er METs CERT ved cyberangrep. De videreformidler informasjon fra NSM NorCERT og er også de som vil bistå ved angrep mot MET eller annen infrastruktur tilknyttet forskningsnettet.

20.2.5 Kommunikasjonsløsninger for departementene

Fire departementer[26] pluss Statsministerens kontor har valgt å etablere egne IKT-løsninger utenfor DSS. DSS fikk i 2013 i oppdrag å utrede en sikker, ugradert løsning for alle departementene. Denne prosessen ble stoppet, blant annet på bakgrunn av rapporten fra konsulentfirmaet Metier i forbindelse med kvalitetssikring fase 2.[27]

Kartleggingen viste at brukerne av dagens fellesløsninger i hovedsak ikke er fornøyd med tjenestene som blir levert av DSS. De fem som står utenfor, har ifølge rapporten liten tiltro til DSS som tjenesteleverandør og prosjektgjennomfører. Denne manglende tiltroen til DSS og forankringen er et viktig premiss for Metiers anbefaling om ikke å godkjenne prosjektet for fremleggelse for Stortinget. Konklusjonen i denne prosessen ble derfor at man valgte en løsning med å videreutvikle DSS' nåværende ugraderte løsning i departementsfellesskapet.

---

[26] Finansdepartementet (FIN), Forsvarsdepartementet (FD), Utenriksdepartementet (UD) og Justis- og beredskapsdepartementet (JD).

[27] Metier (2014): *KS2 (kvalitetssikring fase 2) av Ny IKT-løsning for departementene.* Rapport til Finansdepartementet og Kommunal- og moderniseringsdepartementet.

20.2.6 Målrettede IKT-angrep

Ifølge ekspertgruppen for forsvaret av Norge må Norge være forberedt på å bli stilt overfor manøverkrigføring, geriljakrigføring og andre former for irregulær krig, hybrid krigføring, avskrekking med kjernevåpen og angrep i det digitale rom.

DSBs *Nasjonalt risikobilde 2014*[28] presenterer et hypotetisk cyberangrep på ekominfrastruktur som et scenario. Her omtales blant annet de samfunnsmessige konsekvensene et slikt scenario vil få for ulike samfunnsfunksjoner. Scenarioet beskriver et logisk angrep mot Telenors transportnett som gjør at ekomtjenester som telefoni og Internett faller ut over hele landet i fem døgn.

Scenarioet beskriver enorme samfunnsmessige konsekvenser, også knyttet til styring og kriseledelse. Sentrale institusjoners evne til å utføre sine tiltenkte oppgaver vil bli svekket og informasjonsgrunnlaget mangelfullt. Sentraladministrasjon, finansinstitusjoner og presse vil ikke kunne utføre sine ordinære oppgaver. Det samme gjelder beredskapsaktører med definerte krisehåndteringsoppgaver, som for eksempel Krisestøtteenheten, nødetatene, hovedredningssentralene med flere. I et slikt scenario må kommunikasjon mellom beredskapsaktørene på de ulike nivåene skje via backup-systemer med svært begrenset kapasitet. Dette gjelder både VHF-radiosamband og håndholdte satellitt-telefoner. Som tidligere nevnt i kapittel 11 «Elektronisk kommunikasjon», er Forsvaret også til dels avhengig av det nasjonale sivile transportnettet for å nå sine sivile samarbeidspartnere.

Mennesker i akutte nødsituasjoner får ikke kontakt med politi, ambulanse, legevakt og brannvesen via nødnumrene. Dette antas å gi en følelse av manglende kontroll over egen situasjon og svekket tillit til myndighetene. Bortfall av ekom vil også ha store konsekvenser for krisekommunikasjon. Viktige informasjonskanaler til publikum blir borte.

I kriser der det står målrettede aktører bak som har større kapasitet til å operere i det digitale rom og/eller utføre psykologisk krigføring og fysisk sabotasje, vil utfordringene bli annerledes og større enn det vi hittil har sett. Det er noen forhold som spesielt bidrar til dette. Det ene gjelder flere samtidige hendelser, gjerne geografisk spredt, noe som krever koordinering og samordning både på lokalt, regionalt og sentralt nivå og på tvers av ansvarsområder.

Det andre forholdet er relatert til villedning og påvirkningskampanjer i digitale medier. I Norge er det et uttalt mål at myndighetene skal være på de samme sosiale kanaler som befolkningen. I pågående sikkerhetspolitiske kriser ser en at parter på begge sider i konflikter opererer i de samme sosiale mediekanalene, og at ulike teknikker blir tatt i bruk for å påvirke motparten, for eksempel sosial manipulasjon for å få tilgang til passord på sosiale medier og bruk av falske brukerkontoer og falske «likes» for å påvirke grupper i befolkningen. I tillegg til denne dimensjonen kommer sympatisører og hackergrupperinger som angriper motpartens nettsider og IKT-systemer. Som omtalt i kapittel 7 «Utilsiktede og tilsiktede hendelser», kan digitale angrep av ulik karakter og styrke kjøpes på nett.

Sosiale medier er også benyttet som inngangsport til spionasje. Et eksempel er Taliban-opprørere som laget falske profiler og fremsto som attraktive kvinner som søkte vennskap med koalisjonssoldater. Baktanken var å skaffe informasjon om operasjonene.[29] Det digitaliserte samfunnet er spesielt sårbart for informasjonsoperasjoner, og samfunnet må ha beredskap for å håndtere denne typen sammensatte trusler. De profesjonelle mediene er viktige informasjonsformidlere i nasjonale kriser. Journalister på stedet bidrar til å skape et situasjonsbilde, men de risikerer også å bli formidlere av feil informasjon når de henter informasjon fra sosiale medier.[30]

Målrettede trusler mot informasjonssystemer, der informasjon blir manipulert og endret av ikke-autoriserte personer, er derimot et prematurt område. Trusselen i dag er primært utøvd utenfor Norges grenser, og den er aktuell i større konflikter og krig. Krisehåndtering for å håndtere slike trusler blir det øvd lite på i sivil sektor. Når informasjonsinnholdet blir upålitelig, vil det for det første kunne øke usikkerheten, noe som i sin tur kan forsinke beslutningsprosessen. Dernest vil det, dersom det er uoppdaget, føre til at beslutninger tas på feil grunnlag. Feil beslutninger vil spre seg til de mange aktørene som er involvert i krisehåndteringen. Informasjon fra pålitelige kilder, for eksempel egen etterretning eller vitneobservasjoner på stedet, vil være viktig for å sjekke gyldigheten til informasjonen.[31]

---

[28] Direktoratet for samfunnssikkerhet og beredskap (2014): *Nasjonalt risikobilde 2014.*

[29] Deceglie, Antony (2012): *Taliban Using Facebook to Lure Aussie Soldier*, The Sunday Telegraph, September 09.2012, In: Harley, J.: *Information Operations Newsletter*, Vol. 13, no. 01 (September–October 2012).

[30] Kilde: FFI Fokus, *Kampen om sannheten.* Nr. 2 2014.

[31] Ibid.

20.3 Vurderinger og tiltak

Det er ikke mulig å garantere 100 prosent oppetid på ekom- eller kraftnett. Det er med andre ord en restrisiko som en ikke kan fjerne helt, selv med forebyggende og skadebøtende tiltak.

Denne restrisikoen er også geografisk betinget. Dette skyldes ulike forhold knyttet til vær og vind, topografi, befolkningstetthet og hvor robust infrastrukturen er i området. Det er viktig å forberede både befolkningen og virksomhetene på å klare å leve med denne risikoen og håndtere konsekvensene i en avgrenset tidsperiode inntil systemene er gjenopprettet, uten at det medfører sosial uro. Da trengs det beredskapsplaner og -tiltak som er tilpasset det digitale samfunnet.

Et aspekt ved dette er at myndighetene på alle nivåer må ha tilstrekkelig kompetanse for å håndtere restrisiko og sette inn kostnadseffektive forebyggende tiltak. Dette krever også at både myndigheter, virksomheter og enkeltpersoner har et bevisst forhold til sårbarhetsbildet. Erfaringer fra både hendelser, internasjonale kriser og øvelser viser at denne bevisstheten ikke er til stede i tilstrekkelig grad. Det er et gap mellom befolkningens forventninger til IKT-systemenes sikkerhet og det faktiske sikkerhetsnivået. Utvalget vil derfor anbefale følgende tiltak:

20.3.1 Øke IKT-sikkerhetskompetansen på lokalt og regionalt nivå

Den økte digitale kompleksiteten fører til store utfordringer for lokalt og regionalt nivå. Særlig gjelder dette i kommunesektoren, med mange små enheter som har ansvar for viktige systemer og tjenester, men som også kan ha manglende kompetanse på IKT-sikkerhet. Utvalget observerer at det mangler en felles arena for IKT-sikkerhet i kommunesektoren. Mange kommuner har behov for økt veiledning for å gjennomføre blant annet gode ROS-analyser og etablering av styringssystemer som ivaretar IKT-sikkerhet. Utvalget ser at kommunale fellesarenaer kan bidra til å øke kompetansen, ved for eksempel at det utveksles informasjon om IKT-sikkerhetsløsninger.

Utvalget anbefaler derfor at Justis- og beredskapsdepartementet i samarbeid med Kommunal- og moderniseringsdepartementet tar initiativ til etablering av en felles arena for IKT-sikkerhet for lokalt og regionalt nivå. I denne sammenheng bør det ses til videreføringen av KommIT[32] som skal bidra til å høyne forståelsen av og kunnskapen om IKT som virkemiddel for effektivisering og kvalitetsheving i kommunal sektor, og om dette programmet også bør omfatte IKT-sikkerhet, samt det arbeidet som KINS gjør på området.

Utvalget mener videre at det er behov for å tydeliggjøre hvilke krav og forventninger for IKT-sikkerhet som legges til lokalt og regionalt nivå. Utvalget henviser til gjeldende lovverk med forskrifter, samt anbefalinger i denne NOUen om hendelseshåndtering, og anbefaler at JD tydeliggjør sin styring på IKT-sikkerhetsområdet og koordinerer sine krav med krav og forventninger fra KMD. Den praktiske styringen bør følges opp av aktuelle tilsynsmyndigheter. En klargjøring av krav og forventninger, sammen med økt veiledning vil også kunne bidra til økt bevissthet og kompetanse.

20.3.2 Styrke beredskapen på regionalt og lokalt nivå

Utvalget ser at det er behov for å øke evnen til å håndtere IKT-kriser på lokalt og regionalt nivå. Fylkesberedskapsrådet (FBR) har i dag representanter fra kraftbransjen (KBO), Telenor og Nkom som representant fra ekom-sektoren. *Utvalget mener det bør vurderes om dette forumet bør utvides med representanter fra andre infrastrukturer og viktige leverandører*.

Utvalget mener videre at det må etableres en mekanisme for deteksjon og håndtering av IKT-sikkerhetshendelser for kommunesektoren. I denne forbindelse bør det ses til det pågående arbeidet med å vurdere en etablering av en kommune CSIRT, se kapittel 15 «Vannforsyning», kapittel 17 «Helse og omsorg» og kapittel 21 «Avdekke og håndtere digitale angrep». Utvalget vil også vise til viktigheten av at det *gjennomføres tverrsektorielle øvelser som har IKT-sikkerhet som øvelsesmål*.

20.3.3 Etablere felles gradert IKT-infrastruktur

Det er under utvikling et felles gradert system for sentralforvaltningen, noe utvalget ser på som viktig. Utvalget er kjent med at brukervennligheten oppleves som lav for en del av de graderte systemene som finnes i dag, og at det trenes for lite på å bruke dem. Dette kan tale for variantbegrensning, men det må vurderes opp mot de ulike behovene og den robustheten som ulike systemer gir. Mange departementer og etater peker i dag på at det er flere aktører som tar initiativ på dette

[32] KommIT er et program i KS som skal høyne forståelsen av og kunnskapen om IKT som virkemiddel for effektivisering og kvalitetsheving i kommunal forvaltning og tjenesteproduksjon. Progammet avsluttes i år, og det er per i dag ikke besluttet videreføring.

området, og at det er uklart hvem som har det overordnede ansvaret.

Utvalget vil derfor anbefale at Justis- og beredskapsdepartementet tydeliggjør hvilket departement som skal ha dette ansvaret, og også klargjør hvilke roller og hvilket ansvar KMD og FD har i dette bildet.

I denne forbindelse vil utvalget også anbefale at den eventuelle videreutviklingen av SON ledes av Justis- og beredskapsdepartementet, og støtter med dette anbefalingen fra NSMs Sikkerhetsfaglige råd.

20.3.4 Vurdere virkemidler for kommunikasjon med befolkningen

I dag benyttes flere virkemidler og kanaler for kommunikasjon med befolkningen under kriser. Felles for de fleste er at de er avhengige av en tilgjengelig ekominfrastruktur. NRK P1 har en særskilt rolle ved befolkningsvarsling.

Forut for avgjørelsen om nedleggelse av FM-båndet utførte Nkom en analyse. I denne ble dekningsmessige forhold belyst. Det er utvalgets oppfatning at beredskapshensyn i liten grad er vurdert i forbindelse med avviklingen av FM-båndet. Utvalget ser dette som et eksempel på at myndighetene i for liten grad vurderer sikkerheten i tilknytning til større samfunnsmessige endringer i struktur, organisasjon og teknologi. Denne problemstillingen er også omtalt i kapittel 23 «Tverrsektorielle sårbarhetsreduserende tiltak».

Å beholde FM-sendinger vil muligens ikke bidra til bedre robusthet, fordi ingen etter hvert vil ha mottakerapparat, og teknologien vil heller ikke bli vedlikeholdt. Fremtidige IP-løsninger vil etter utvalgets vurdering ha innvirkning på hvilken utbredelse DAB vil få. Dette avhenger spesielt av den teknologiske utviklingen og markedet. Utvalgets vurdering er at hvis trenden med IP-løsninger slår inn, vil «alle egg bli lagt i samme kurv». Det vises her til kapittel 11 «Elektronisk kommunikasjon».

Utvalget vil derfor anbefale at DSB vurderer bruken av virkemidler for kommunikasjon med befolkningen i kriser og i denne sammenheng også vurderer beredskapsrollen til NRK i samarbeid med Kulturdepartementet.

Kapittel 21
Avdekke og håndtere digitale angrep

Dette kapittelet omhandler de digitale sikkerhetsutfordringene ved IKT-kriminalitet, spionasje, sabotasje og terror. Utvalget vurderer i kapittelet behovet for å kunne avdekke, håndtere og etterforske digitale angrep, og omhandler både nasjonal sikkerhet, samfunnssikkerhet, individets sikkerhet og personvern.

Presumptivt lave kostnader ved og mulighet til å operere i det skjulte gjør det digitale rom til en attraktiv arena for å begå uønskede handlinger.[1] Økt bruk av teknologi og Internett åpner for kriminelle handlinger mot staten, næringslivet og enkeltindivider. De digitale angrepene øker i omfang og blir stadig mer målrettet, og de kan i ytterste konsekvens ramme nasjonal sikkerhet ved at kritiske funksjoner blir satt ut av spill. Kriminalitet og mellomstatlige kriser og konflikter har i stadig større grad elementer av digitale angrep.

Nyhetsbildet de siste årene har vært preget av tjenestenektangrep, datatyveri og IKT-sabotasje. Digitale angrep har i første rekke vært en trussel mot tilgjengelighet og konfidensialitet, men med økende fare for skade på kritisk infrastruktur, lammelse av kritiske samfunnsfunksjoner og i ytterste konsekvens fare for liv og helse. Internett ble brukt til å planlegge terrorangrepet mot redaksjonen til satiremagasinet Charlie Hebdo i Paris i januar 2015. Fransk politi brukte Internett som et ledd i etterforskningen, og det franske folket brukte Internett for å organisere massedemonstrasjoner. I november 2014 ble verden vitne til at hackere brukte Internett til å gjennomføre dataangrep mot Sony Pictures ved å stoppe kinovisningen av filmen «The Interview». Som en respons, og for å forsvare ytringsfriheten, publiserte Microsoft og Google filmen via Internett. Dette er eksempler på at Internett har fått en avgjørende rolle både før, under og etter en hendelse.

I dette kapitlet er *Ressursgruppen* benyttet som et begrep for å henvise til rapporten fra en nedsatt arbeidsgruppe. Utvalget har behandlet rapporten på lik linje med andre innspill. Se elektronisk vedlegg «Avdekke, håndtere og etterforske digitale angrep».

21.1 Sentrale begreper og føringer

21.1.1 Sentrale begreper

Med *IKT-hendelse* mener utvalget situasjoner der IKT-systemer blir utsatt for utilsiktede eller tilsiktede uønskede hendelser. *Alvorlige IKT-hendelser* er hendelser som rammer samfunnskritisk infrastruktur, samfunnskritisk informasjon eller samfunnskritiske funksjoner på en slik måte at det får betydning for samfunnets og befolkningens trygghet. *IKT-hendelser* og *cyberhendelser* blir i det følgende brukt som synonymer.

Med *digitale angrep* mener utvalget tilsiktede IKT-hendelser. Disse IKT-hendelsene er handlinger i eller gjennom det digitale rom med hensikt å skade eller påvirke personell, materiell eller konfidensialiteten, integriteten, tilgjengeligheten eller autentisiteten til et IKT-system,[2] for eksempel i form av sabotasje-, spionasje- eller terrorhandlinger. Dette står i kontrast til utilsiktede IKT-hendelser, som er forårsaket av svikt og uhell.

Begrepene *spionasje, sabotasje* og *terror* er definert i straffelovens § 147 og sikkerhetslovens § 3 nr. 3-5.

IKT-kriminalitet[3] er IKT-hendelser som er straffbare etter norsk lov. Norsk lovgivning har ingen definisjon av IKT-kriminalitet.[4] Begrepet deles ofte inn i to grupper: kriminalitet rettet mot selve IKT-systemene og kriminelle handlinger begått ved hjelp av IKT som et vesentlig redskap.[5]

---

1 Prop. 73 S (2011–2012) *Et forsvar for vår tid.*

2 Samme tilnærming som Forsvarets cyberretningslinjer 2013. Utvalget har valgt begrepet IKT-hendelser fremfor cyberhendelser.

3 IKT-kriminalitet tilsvarer det engelske cybercrime, og benyttes ofte synonymt med datakriminalitet og Internett-relatert kriminalitet.

4 Meld. St. 7 (2010–2011) *Kampen mot organisert kriminalitet – en felles innsats.*

5 Ibid, samt Kripos (2014): *Trendrapport 2015 - den organiserte kriminaliteten i Norge.*

I forbindelse med Norges ratifisering av Europarådets Budapestkonvensjon[6] ble det gjennomført en kartlegging av nødvendige lovendringer.[7] En ny straffelov[8] ble vedtatt som følge av dette, der det i kapittel 21 er samlet straffebestemmelser for vern av informasjon og informasjonsutveksling, herunder «innbrudd i datasystem», «krenkelse av retten til privat kommunikasjon», «fare for driftshindring» og «identitetskrenkelse».

IKT og Internetts betydning for kriminalitetsbekjempelsen beskrives av politiet ofte langs tre akser: objektet eller åstedet for forbrytelsen (*kriminalitetsform*), verktøyet for forbrytelsen (*modus*) og kilde til spor (*sporsted*).

Elektroniske spor er elektronisk informasjon som kan knyttes til en person, en elektronisk enhet, et sted eller en hendelse. Elektroniske spor er i dag relevant i nær sagt all etterforskning.

Politiet bruker begrepet *IKT-tekniske undersøkelser* om tekniske operasjoner for å innhente og analysere elektroniske spor. Se punkt 7.2.1 «IKT-kriminalitet» for eksempler på kriminalitetsformene.

Med *situasjonsbilde* mener utvalget et kontinuerlig oppdatert øyeblikksbilde om pågående hendelser og aktiviteter. Et *trusselbilde*[9] er en vurdering av de farene og truslene samfunnet står overfor, samt hvilke metoder og hendelser som anses sannsynlige. Trusselbilder utgis ofte periodevis.

Begrepene *overvåking* (*surveillance)* og *monitorering* (*monitoring)* vil i det følgende bli brukt om hverandre.

Etterretning og *analyse* brukes om prosesser for å innhente og sammenstille informasjon. Politiets etterretningsdoktrine definerer *etterretning* som «en styrt prosess, bestående av systematisk innsamling, analyse og vurdering av informasjon om personer, grupper og fenomener for å danne grunnlag for beslutning». Forsvarssjefens etterretningsdoktrine definerer begrepet slik: «Etterretning er systematisk innhenting og bearbeiding av informasjon som angår utenlandske forhold ervervet med åpne og fordekte metoder i en statlig legal ramme. Produktene skal redusere usikkerhet, skape forståelse og har ofte en prediktiv karakter. Begrepet brukes både om produktet, aktiviteten og organisasjonen som utøver aktiviteten».

21.1.2 Nasjonale føringer, rapporter og viktige hendelser

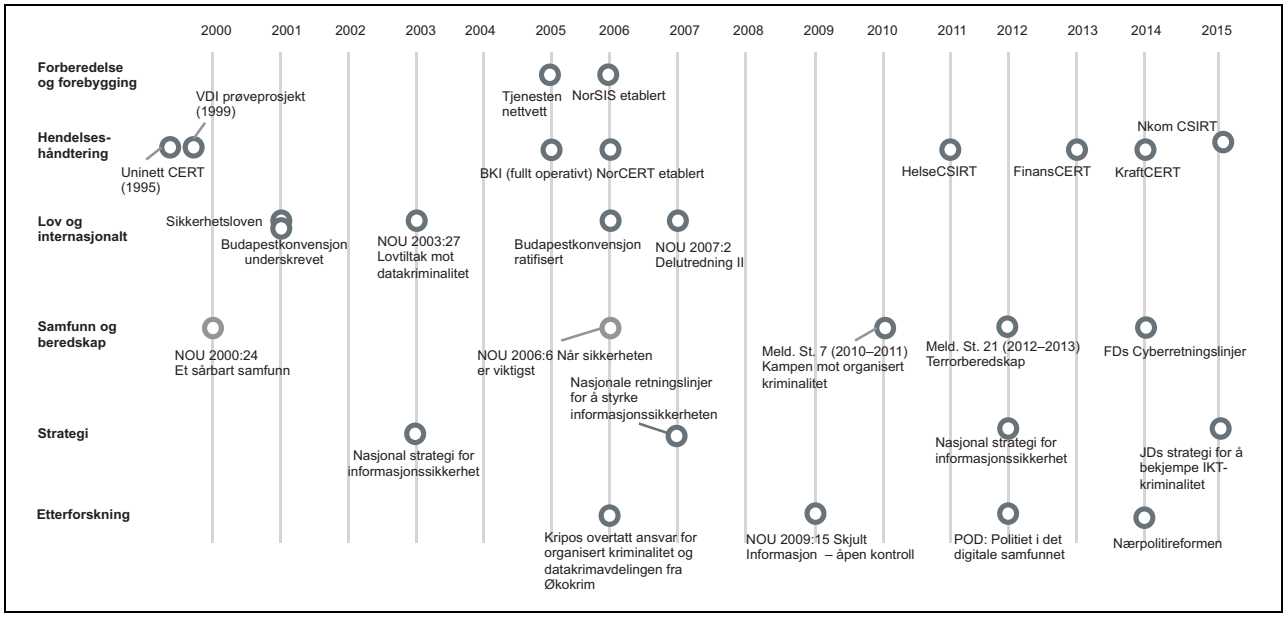
Det finnes en rekke nasjonale føringer, rapporter og milepæler som omhandler IKT-sikkerhetsutfordringer med relevans for dagens kapasiteter.

6 Council of Europe (2001): *Treaty No.185 Convention on Cybercrime.* Ble underskrevet av Norge i 2001 og ratifisert i 2006.

7 NOU 2003: 27 *Lovtiltak mot datakriminalitet*, fulgt opp av NOU 2007: 2 *Lovtiltak mot datakriminalitet – Delutredning II*, som kom med forslag til straffebestemmelser om datakriminalitet som kan tas inn i den spesielle delen i den nye straffeloven.

8 Justis- og beredskapsdepartementet (2005): *Lov om straff (straffeloven)*. Ikraftsettelse avventer implementasjon i politiets IKT-systemer.

9 Noen sikkerhetsaktører benytter begrepet *risikobilde* om det samme produktet.



Figur 21.1 Oppsummering av utvalgte nasjonale føringer, rapporter og milepæler.

Øvrige initiativer og rapporter er beskrevet i kapittel 8 «Organisering av roller og ansvar». Figur 21.1 oppsummerer et utvalg av disse.

Regjeringens ambisjoner og mål for håndtering av IKT-hendelser fremgår blant annet av Meld. St. 29 (2011–2012) *Samfunnssikkerhet* og *Nasjonal strategi for informasjonssikkerhet*. I tillegg har Justis- og beredskapsdepartementet nylig utgitt en nasjonal strategi for å bekjempe IKT-kriminalitet.[10]

21.2 Roller og ansvar

Det overordnede ansvaret for håndtering av digitale angrep og IKT-kriminalitet ligger hos Justis- og beredskapsdepartementet og Forsvarsdepartementet, som beskrevet i kapittel 8 «Organisering av roller og ansvar». I det følgende gjennomgås de mest sentrale aktørene som har utøvende ansvar for håndtering og etterforskning av IKT-kriminalitet, terror, spionasje og sabotasje. Prinsipper for krisehåndtering og kriseorganisering på sentralt nivå er omtalt under kapittel 20 «Styring og kriseledelse».

21.2.1 Nasjonal sikkerhetsmyndighet

NSM NorCERT er den funksjonen i Nasjonal sikkerhetsmyndighet som er «ansvarlig for å koordinere håndteringen av alvorlige IKT-angrep på samfunnskritisk infrastruktur eller andre viktige samfunnsfunksjoner og for å organisere og drifte et nasjonalt varslingssystem for digital infrastruktur.»[11] NSM koordinerer også håndteringen av sikkerhetstruende hendelser knyttet til sikkerhetsgradert informasjon, herunder kryptosystemer, IKT-systemer med mer, og skjermingsverdige objekter etter sikkerhetsloven. I denne sammenheng rapporterer NSM til NATO/EU og bilaterale samarbeidspartnere når hendelsen berører informasjon utstedt av disse.

NSM NorCERT er døgnbemannet og kan bistå med koordinering av hendelser og teknisk analyse av maskiner, skadelig kode og logger. Informasjonsinnsamling foregår blant annet gjennom VDI-sensornettverket. *Varslingssystem for digital infrastruktur (VDI)* ble etablert av EOS-tjenestene i 1999 som et prøveprosjekt. VDI ble i 2003 lagt til NSM og i 2006 utvidet til også å omfatte en nasjonal responsfunksjon ved slike angrep: NorCERT (Norwegian Computer Emergency Response Team), nå benevnt NSM NorCERT. Slik innsamling og deling av informasjon foregår også gjennom andre nasjonale og internasjonale responsmiljøer og samarbeidende tjenester. NSMs VDI-sensornettverk detekterer, varsler og verifiserer uønskede hendelser. Koordinering av håndteringen skjer i nært samarbeid med Politiets sikkerhetstjeneste og Etterretningstjenesten, sektorvise responsmiljøer og berørte virksomheter. EOS-tjenestenes arbeid koordineres i Cyberkoordineringsgruppen (CKG), som ledes av NSM. Tjenestene kan i fellesskap beslutte at også andre etater kan tiltre forumet. Kripos og Cyberforsvaret møter derfor regelmessig i det som betegnes som en utvidet CKG.

NSM NorCERT ivaretar flere møtearenaer. *NSM NorCERT Sikkerhetsforum* er et forum for NorCERT-medlemmer og partnere, der NSM NorCERT blant annet presenterer hva de har arbeidet med siste halvår. Den andre møtearenaen er *Nasjonalt Cybersikkerhetssenter (NCSS)*[12], der representanter for departementer, direktorater, politi og andre møtes månedlig for å bli oppdatert om hendelser, reise spørsmål eller legge frem egne opplysninger. Informasjonen kan være gradert. I *NCSS Operativt forum* deltar sentrale tjenestetilbydere/eiere av kritisk IKT-infrastruktur og sektorvise responsmiljøer. I *NCSS myndighetsforum* deltar sektormyndigheter, politiet, EOS-tjenestene og sentrale departementer. NSM samarbeider med tilsvarende tjenester i en rekke land og internasjonale organisasjoner. Se også kapittel 10 «Folkerett og internasjonalt samarbeid».

21.2.2 Sektorvise responsmiljøer

I *Nasjonal strategi for informasjonssikkerhet* og tilhørende handlingsplan var etablering av sektorvise responsmiljøer et prioritert tiltak for å sikre at sektorene og den enkelte virksomhet sto bedre rustet mot uønskede IKT-hendelser. Høsten 2014 ga Justis- og beredskapsdepartementet ut anbefalinger og retningslinjer[13] for etableringen av sektorvise responsmiljøer. De sektorvise responsmiljøene vil ha en nøkkelrolle i å sikre at alle relevante aktører mottar rask og korrekt varslingsin-

[10] Justis- og beredskapsdepartementet (2015): *Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet.*

[11] Forsvarsdepartementet (2011): *Instruks for sjef Nasjonal sikkerhetsmyndighet.*

[12] Dette er et begrep som både benyttes om en møteplass og et tiltak i Sikkerhetsfaglig råd. I denne konteksten snakker utvalget om *møteplassen*.

[13] Justis- og beredskapsdepartementet (2014): *Modell for håndtering av IKT-sikkerhetshendelser – anbefalinger og retningslinjer*, brev til departementene.

formasjon og settes i stand til å gjøre nødvendige tiltak. De sektorvise responsmiljøene er NSM NorCERTs kontaktpunkt ved IKT-sikkerhetshendelser. Videre er det de enkelte departementenes ansvar å vurdere innretningen på responsmiljøene, basert på egne risikovurderinger. I dag er det etablert fem sektorvise responsmiljøer: UNINETT CERT, Avdeling for beskyttelse av kritisk infrastruktur (BKI, for Forsvaret), HelseCSIRT, FinansCERT og KraftCERT. Det planlegges å etablere en Nkom CSIRT. Disse er nærmere beskrevet i del III «Sårbarheter i kritiske samfunnsfunksjoner». Høsten 2016 er det planlagt gjennomført en nasjonal IKT-øvelse der disse responsmiljøene inngår, og der de vil få grunnopplæring og mulighet til å teste i praksis egen og andres håndteringskapasitet.

Behovet for en kommune-CSIRT er utredet av NorSIS i samarbeid med Lillehammer og Gjøvik kommune. Arbeidsgruppen har anbefalt at det opprettes en kommune-CSIRT. Sluttrapporten ble i oktober 2015 overlevert til Lillehammer og Gjøvik kommuner for videre behandling.

Justis- og beredskapsdepartementet besluttet i 2011 å opprette en CSIRT i justissektoren. Justis-CSIRT er lagt til IKT-avdelingen i Politidirektoratet. Politidirektoratet mener at arbeidet med CSIRT i Justissektoren må evalueres, da den gir veldig begrenset effekt i dag.

Det er ikke etablert et felles responsmiljø for departementsfellesskapet. Departementenes sikkerhets- og serviceorganisasjon (DSS) drifter IKT-systemer for 11 departementer, og har derfor et primæransvar for teknisk og operativ hendelseshåndtering på vegne av disse departementene. De øvrige departementene har egne håndteringskapasiteter. Utvalget er kjent med at det pågår et arbeid mellom departementene der eventuelle endringer i organisering vurderes.

Som det fremgår av navnene, benyttes både CERT og CSIRT blant håndteringsmiljøene. CERT står for «Computer Emergency Response Team» og CSIRT for «Computer Security Incident Response Team». ISAC er et relatert begrep, som står for «Information Sharing and Analysis Center».

21.2.3 Politiet, PST og påtalemyndigheten

Politiets oppgaver er beskrevet i politilovens § 2: Politiet skal «*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*». Politiet skal forebygge, avdekke og stanse kriminell virksomhet, samt forfølge straffbare forhold i samsvar med regler gitt i eller i medhold av lov. Av dette følger politiets ansvar for forebygging og bekjempelse av IKT-kriminalitet.

Politidirektoratet er underlagt Justis- og beredskapsdepartementet, og er etatsleder for politiet. Politidirektoratet leder den forebyggende og avvergende virksomheten regulert i politiloven. Politidirektoratet har ansvar for faglig ledelse, styring, fordeling av ressurser, resultatoppfølging og utvikling av norsk politi dvs. alle politidistriktene og politiets særorganer foruten politiets sikkerhetstjeneste (PST). Politiets primære innsats mot IKT-kriminalitet ivaretas av de 27 *politidistriktene*.

KRIPOS er et særorgan med nasjonalt ansvar for bekjempelse av organisert og annen alvorlig kriminalitet, og politiets internasjonale kontaktpunkt. Arbeidsområdene omfatter forebygging, taktisk og teknisk etterforskning, metodeutvikling, påtale og kriminaletterretning. Avgjørelsen om hvorvidt enheten skal etterforske alvorlig IKT-kriminalitet, er regulert i påtaleinstruksen § 37-3 og besluttes av sjef Kripos eller assisterende sjef.

ØKOKRIM er et særorgan i politiet med nasjonalt ansvar for etterforskning og påtale av økonomisk kriminalitet og miljøkriminalitet. Særorganet er også et statsadvokatembete underlagt Riksadvokaten.

Politihøgskolen (PHS) er den sentrale utdanningsinstitusjonen for politi- og lensmannsetaten.

Politiets sikkerhetstjeneste (PST) har ansvaret for å forebygge og etterforske straffbare handlinger mot rikets sikkerhet, herunder avdekke ulovlig etterretningsvirksomhet (spionasje) og forebygge terror og sabotasje. PSTs ansvar omfatter også det å gi trusselvurderinger og sikkerhetsråd. PST er direkte underlagt Justis- og beredskapsdepartementet og står i en særstilling i politiet med både en sentral enhet og lokale enheter i politidistriktene. PST samarbeider med NSM og Etterretningstjenesten i Cyberkoordineringsgruppen (CKG), se tidligere omtale av NSM.

Den høyere påtalemyndigheten har det overordnede faglige ansvaret for straffesaksbehandlingen i politiet og påtalemyndigheten, og omfatter Riksadvokaten, alle statsadvokatembetene, Det nasjonale statsadvokatembetet (NAST) og Økokrim. NAST har det overordnede påtalemessige ansvaret for saker som blir etterforsket av Kripos og PST.

21.2.4 Forsvaret

Etterretningstjenestens (E-tjenesten) oppgaver og ansvar er regulert ved lov:

> «Etterretningstjenestens hovedoppgave er å innhente, bearbeide og analysere informasjon om andre lands politiske og samfunnsmessige utvikling, intensjoner og militære styrker, som kan utgjøre en reell eller potensiell risiko.»

E-tjenesten skal bidra til norske myndigheters evne til å forebygge, avverge og håndtere episoder, kriser og væpnet konflikt og har ansvar for en tidligst mulig varsling av forstyrrelser, kompromittering og manipulering av IKT-systemer som kan ramme rikets selvstendighet, sikkerhet og andre nasjonale interesser. E-tjenesten følger primært fremmedstatlige aktører som utfører etterretningsoperasjoner eller kan tenkes å bruke offensive cyberkapabiliteter i en sikkerhetspolitisk konflikt.

Cyberforsvaret har til oppgave å sikre, drifte og beskytte Forsvarets egne datasystemer og kommunikasjonsnettverk. I tillegg leverer Cyberforsvaret infrastruktur og tjenester til deler av statsforvaltningen og andre aktører med sikkerhets- og beredskapsbehov. Støtte til det sivile samfunnet kan også innebære bruk av Forsvarets materiell og utstyr, personell og kompetanse i særskilte situasjoner der sivile myndigheters ressurser ikke strekker til og Forsvarets kapabiliteter er relevante. Cyberforsvaret har en egen CERT-funksjon, kalt Forsvarets senter for beskyttelse av kritisk infrastruktur (BKI).[14]

Felles kontraterrorsenter (FKTS) ble opprettet av Justis- og beredskapsdepartementet og Forsvarsdepartementet i 2013, etter anbefalinger fra 22. juli-kommisjonen.[15] Senteret arbeider hovedsakelig med problemstillinger av både nasjonale og internasjonale dimensjoner, der informasjon fra begge tjenestene er nødvendig for å danne et helhetlig bilde. Senteret har tre hovedoppgaver: å ivareta rettidig relevant informasjonsutveksling mellom tjenestene, å koordinere og tilrettelegge for et effektivt operativt samarbeid og å utarbeide analyser av terrortrusler i og mot Norge. I Utenriksdepartementets stortingsmelding om globale sikkerhetsutfordringer i utenrikspolitikken blir det uttrykt at regjeringen vil videreutvikle Felles kontraterrorsenter.[16]

21.2.5 Andre aktørers ansvar

Direktoratet for samfunnssikkerhet og beredskap (DSB) skal under kriser støtte Justis- og beredskapsdepartementet (JD) i deres samordningsrolle. DSBs rolle i håndtering av IKT-kriser er knyttet til rollen som samordner, ved at DSB ved større hendelser samordner informasjon fra lokalt og regionalt nivå, samt direktoratsnivå. DSB bidrar gjennom dette til en felles situasjonsforståelse for Kriserådet og JD. De prinsippene, lovene og forskriftene som gjelder for styring og kriseledelse for det regionale nivået, er også gjeldende for håndtering av IKT-hendelser. En nærmere beskrivelse er gitt i kapittel 20 «Styring og kriseledelse».

Næringslivets Sikkerhetsråd (NSR) er en medlemsorganisasjon og nettverksarena opprettet av de sentrale arbeidsgiverorganisasjonene med formål å bekjempe kriminalitet i og mot næringslivet. NSR står bak Mørketallsundersøkelsen, som kartlegger omfanget av IKT-kriminalitet og IKT-sikkerhetshendelser. Det er inngått en samarbeidsavtale mellom NSR og Kripos for å styrke samarbeidet om å bekjempe organisert og annen alvorlig kriminalitet i og mot næringslivet.

Norsk senter for informasjonssikring (NorSIS) gir råd til virksomheter ved hendelser, ofte etter henvisning fra NSM eller NSR. NorSIS er også en sentral aktør for bistand til enkeltmennesker gjennom tjenestene slettmeg.no og idtyveri.info. Slettmeg.no er en rådgivnings- og veiledningstjeneste for de som føler seg krenket på nettet. Idtyveri.info er en nettside som gir informasjon om hvordan man beskytter seg mot identitetstyveri, og hva man skal gjøre dersom man blir utsatt for det.

Det finnes også en rekke andre aktører, samt internasjonale samarbeidsarenaer. En sammenstilling av de mest sentrale er gitt i kapittel 10 «Folkerett og internasjonalt samarbeid».

21.3 Håndteringskjeden ved tilsiktede hendelser

Utvalget har valgt å benytte begrepet *håndteringskjeden* som en betegnelse for de aktivitetene som

[14] I Fagmilitært råd fra 2015 er det foreslått navneendring til MilCERT.

[15] Beslutning om opprettelsen ble gitt i Meld. St. 21 (2012–2013) *Terrorberedskap*, som var Stortingets oppfølging av NOU 2012: 14 *Rapport fra 22. juli-kommisjonen*.

[16] Meld. St. 37 (2014–2015) *Globale sikkerhetsutfordringer i utenrikspolitikken – Terrorisme, organisert kriminalitet, piratvirksomhet og sikkerhetsutfordringer i det digitale rom.*

er nødvendige i forkant, under og i etterkant av en uønsket hendelse. Vår beskrivelse er strukturert etter temaene forebygge og forberede, avdekke, håndtere og etterforske.

21.3.1 Forebygge og forberede

Med *forebygging og forberede* menes samfunnets aktiviteter i forkant av at hendelser inntreffer, for å redusere risiko for alvorlige IKT-hendelser, herunder IKT-kriminalitet, samt planverk og andre planleggingsaktiviteter for å begrense skadevirkningene dersom hendelsen likevel inntreffer.

De ulike aktørenes forebyggende tiltak og egenberedskap er avgjørende i arbeidet med å avverge digitale angrep. IKT-sikkerhet er først og fremst et *virksomhetsansvar*. Eieren av virksomheten, som har ansvar for IKT-sikkerheten under normale forhold, har også ansvaret i en krisesituasjon.[17] Virksomheter løser ofte disse oppgavene ulikt, avhengig av virksomhetens størrelse. Enkelte virksomheter har egne responsteam som aktivt håndterer sikkerhetshendelser. De fleste virksomheter, særlig små, kjøper ofte tjenester, som overvåkingstjenester og analysekapasitet, fra eksterne drifts- og sikkerhetsleverandører. Se også punkt 23.7 «Utkontraktering og skytjenester».

Beredskapsplanverk. Både for virksomhetene og for nasjonal sikkerhet er et godt beredskapsplanverk avgjørende. En beskrivelse av det nasjonale beredskapssystemet er gitt i kapittel 20 «Styring og kriseledelse».

Felles IKT-trusselbilde. Beslutningstakere på alle nivåer i både det private og det offentlige må ha tilstrekkelig informasjon om IKT-trusselbildet, slik at de kan ta gode og begrunnede beslutninger. I dag formidler ulike aktører deler av IKT-trusselbildet. PST og Etterretningstjenesten formidler informasjon om trusselbildet gjennom årlige trussel- og risikovurderinger. NSM utgir årlig rapportene *Risiko* og *Helhetlig IKT-risikobilde*, i tillegg til kvartalsrapporter. DSB utgir årlig *Nasjonalt risikobilde (NRB)*. I tillegg utgir Kripos en årlig trendrapport om organisert kriminalitet som omhandler IKT-kriminalitet. Næringslivets Sikkerhetsråd gir gjennom Mørketallsundersøkelsen en overordnet oversikt over registrert anmeldt IKT-kriminalitet til politiet, rapporteringer til NSM og registrerte angrep håndtert av sikkerhetsleverandører. Det utgis også sektorvise rapporter om risikobildet, blant annet fra de enkelte sektorvise CERT-miljøene, sikkerhetsleverandører og enkelte IKT-leverandører. Konsulentselskaper og nasjonal og internasjonal presse har også en sentral rolle i å formidle informasjon om situasjonsbildet.

Sårbarhetskartlegging og *inntrengingstesting* er sentrale forebyggende verktøy i alle virksomheter. Inntrengingstesting vil kunne bidra til mer robuste tekniske løsninger for operativ bruk. NSM har gjennom inntrengingstesting avdekket alvorlige sårbarheter innen en lang rekke samfunnssektorer. Sårbarhetskartlegging er en tjeneste som blant annet består i regelmessig kartlegging av utvalgte IP-adresser som er tilgjengelige på Internett, og det er mange nasjonale og internasjonale leverandører som tilbyr slike tjenester. NSM lanserte i 2014 en tjeneste for sårbarhetskartlegging kalt *Allvis NOR*. Dette er en tjeneste NSM tilbyr for å bedre sikkerheten i norske virksomheter som er underlagt sikkerhetsloven.

Rapporterings- og informasjonsdelingsrutiner. Enkelte sektorer stiller krav om rapportering av hendelser. Det finnes i dag ingen entydig kategorisering eller samlet oversikt over typer rapportering. For virksomheter som er underlagt sikkerhetsloven, er det krav om å rapportere sikkerhetstruende hendelser til NSM. Ved en eventuell implementering av det kommende NIS-direktivet i Norge er det ventet tydeligere krav til rapportering. For mer informasjon om NIS-direktivet se punkt 10.6.1.

Nasjonale myndigheter er helt avhengige av at private virksomheter deler informasjon om angrep de blir utsatt for, sårbarheter som avdekkes, og så videre, for å ha et riktig risikobilde og prioritere sine ressurser riktig. Tilsvarende trenger private aktører risikoinformasjon fra myndighetene for å prioritere sine tiltak og bygge opp sine kapasiteter hensiktsmessig.

God forebygging forutsetter et tett og tillitsfullt offentlig–privat samarbeid. Flere tiltak er iverksatt for å styrke det forebyggende kriminalitetsarbeidet i næringslivet. Blant annet er det besluttet opprettet næringslivskontakter i NSM, Kripos, og i flere politidistrikt. NSR har vært en pådriver for dette arbeidet.

NSMs forebyggende arbeid. NSM utøver en rekke forebyggende myndighetsoppgaver etter sikkerhetsloven, som godkjenning av sikkerhetsgraderte informasjonssystemer, sertifisering av informasjonssystemer, inntrengingstesting av informasjonssystemer og utvikling og godkjenning av kryptosystemer. Emisjonssikkerhetsun-

[17] Fornyings- og administrasjonsdepartementet, Samferdselsdepartementet, Justis- og beredskapsdepartementet og Forsvarsdepartementet (2012): *Nasjonal strategi for informasjonssikkerhet*.

dersøkelser søker blant annet å avdekke uønsket elektromagnetisk stråling, som blant annet kan medføre uønsket informasjonslekkasje fra IKT-utstyr.

Politiet og PSTs kriminalitetsforebygging. Forebygging av kriminalitet er en av politiets mest sentrale samfunnsoppgaver. Kjent fra media er Snapchatsaken der bilder ble stjålet og distribuert på diverse fildelingsnettverk i 2014. Politiet brukte i denne saken flere virkemidler, blant annet tilstedeværelse på Internett, for å informere om alvorligheten og på den måten begrense skadeomfanget. Politiet har også i samarbeid med banker jobbet med å stoppe nye forsøk på bankran ved å gripe tidlig inn i prosessen der kriminelle forbereder skadevare rettet mot nettbankportalene.

For effektiv forebygging av IKT-kriminalitet har politiet og PST behov for gode kilder til informasjon og egen analysekapasitet. PST prioriterer forebygging og avverging høyt av hensyn til alvorlighetsgraden av hendelser innenfor sitt ansvarsområde, og har derfor utstrakt deling av sikkerhetsgradert etterretning med andre EOS-tjenester internasjonalt. Etterretning skal kunne understøtte alle politiets oppgaver. Politiets etterretningsdoktrine ble utgitt i 2014, og er rammeverket for denne virksomheten.

Både politiet og PST har sett behov for egen tilstedeværelse og innhenting av informasjon via Internett. Politiarbeid på Internett omfatter etterforskning, forebyggende arbeid og etterretning basert på informasjon fra Internett.[18] Kripos arbeider med et konsept for åpen og skjult tilstedeværelse på Internett.

21.3.2 Avdekke

Med *avdekking* mener utvalget aktiviteter som har til hensikt å oppdage IKT-hendelser. Avdekkingen kan være manuell eller automatisk, underveis eller i etterkant av hendelsen. Avdekkingen skjer på flere nivåer i samfunnet, og bygger på effektiv varsling og rapportering. Avdekking kan innebære evne til å avdekke alvorlig kriminell virksomhet, herunder virksomhet som kan true Norges eller andre lands sikkerhet, samt evne til å avdekke og varsle alvorlige angrep på kritisk infrastruktur og informasjon.

Digitale angrep kan deles i ulike faser, fra tidlig rekognosering til målet for angrepet er oppnådd. Det er dermed mange steg i prosessen angrep kan oppdages på. Angriperen må, basert på kjennskap til målet, skaffe seg tilgang, for eksempel ved å sende infiserte e-postvedlegg eller utnytte programmeringssårbarheter i nettverkstilkoblede tjenester. Angrepet kan videre oppdages som unormal aktivitet i og mellom IKT-utstyr, idet angriperen manøvrerer seg inn i det lokale nettverket, utfører endringer eller kopierer informasjon ut av nettverket.

Den nasjonale evnen til å avdekke tilsiktede IKT-hendelser avhenger av både virksomhetenes og myndighetenes evne til å avdekke. Resultatet av deres kapasiteter vil danne grunnlag for et situasjonsbilde, til hjelp for de ulike aktørene. En forutsetning for effektiv avdekking er god og effektiv informasjonsdeling.

Virksomhetenes avdekking. Mange virksomheter benytter automatiske deteksjonsmekanismer som i stor grad er basert på signaturer. Det forutsetter at angrepsmetoden er kjent, og krever mye manuelt arbeid fra teknisk kompetente ressurser. Deteksjonsmekanismene er avhengige av kontinuerlig oppdatering for at de skal fungere hensiktsmessig. Det finnes også deteksjonsmekanismer som baserer seg på analyse og varsling av unormal oppførsel i systemene. *Logging* er et viktig hjelpemiddel, både for å finne kilden til innbrudd og andre uønskede hendelser i IKT-systemer etter at hendelser har inntruffet. Mørketallsundersøkelsen har gjennom flere år vist at flere virksomheter ikke logger eller gjennomgår loggene sine.

En del virksomheter monitorerer interne nett og systemer selv eller gjennom leverandører av denne typen tjenester. Virksomhetens størrelse har ofte betydning for evnen til å avdekke digitale angrep. Mange leverandører av denne typen tjenester driver døgnkontinuerlig monitorering.

DNS-tjenesten[19] NSM NorCERT tilbyr, lar virksomheter rute sine DNS-oppslag gjennom NSMs systemer. NSM oppdaterer disse med blokkeringsregler, basert på hendelser, og kan på den måten stoppe og begrense uønsket trafikk, for eksempel skadelige nettsider som sprer ondsinnet kode (vannhullsangrep) og infiserte e-postvedlegg som forsøker å opprette kontakt med et kommando-kontrollnettverk.

Enkelte sektorvise responsmiljøer har etablert egne deteksjonsmekanismer. Justis- og beredskapsdepartementet har anbefalt at responsmiljø-

[18] Justis- og beredskapsdepartementet (2015): *Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet.*

[19] DNS (Domain Name System) er navnetjenerstandarden som brukes for å oversette mellom menneskelig lesbare domenenavn og de tekniske IP-adressene som brukes i datakommunikasjon.

ene selv vurderer hvorvidt det er hensiktsmessig å besitte denne kompetanse internt, innhente den eksternt, for eksempel ved avtale med en kommersiell sikkerhetsleverandør, og/eller etablere en felles kapasitet for flere sektorvise responsmiljøer.[20]

Forskningsmiljøers, sikkerhetsmiljøers og frivillige organisasjoners avdekking. Kommersielle sikkerhetsmiljøer og forskningsmiljøer står bak store deler av de mekanismene verdenssamfunnet har for å oppdage nye uønskede IKT-hendelser. Dette skjer blant annet ved at nye sårbarheter oppdages og analyseres, slik at automatiske deteksjonsmekanismer kan fange opp forsøk på utnyttelse. Det finnes også en rekke frivillige organisasjoner som har vist seg å ha en viktig rolle. *Underworld* bisto norsk og utenlandsk politi med å avdekke bakmennene bak banktrojaneren SpyEye, og driver automatisert oppdagelse av skjult skadevare på internettsider.[21] *Shadowserver* bidro til stengingen av skadevareinfrastrukturen bak Gameover Zeus ved å innhente, analysere og videreformidle informasjon i sitt globale nettverk av tjenestetilbydere og håndteringsteam.

Samarbeidet i CKG er sentralt i arbeidet med å avdekke digitale angrep blant annet knyttet til rikets sikkerhet. For å kunne oppdage, varsle og håndtere utenlandske trusler som terror, spionasje og digitale angrep trengs det ifølge Etterretningstjenesten å kunne følge med på relevant Internett-trafikk som går via kabler.

Varslingssystem for digital infrastruktur (VDI) i NSM har til hensikt å gi myndighetene varsel om koordinerte og alvorlige dataangrep mot samfunnskritisk infrastruktur eller andre viktige samfunnsfunksjoner. Norge var tidlig ute med dette konseptet. Mange land ser til Norge som et foregangsland i måten private virksomheter er blitt inkludert i arbeidet på.

VDI-sensornettet har et signatursett som er utviklet basert på tidligere hendelser og annen kjent aktørinformasjon. Det er ingen krav om at virksomheter må delta i VDI-samarbeidet. VDI er delfinansiert av deltagerne – hver deltager dekker kostnaden for egen sensor, mens NSM finansierer sentral infrastruktur samt utvikling og forvaltning. Samarbeidet er regulert gjennom egne avtaler mellom NSM NorCERT og den enkelte virksomheten. Virksomhetene eier selv informasjon fra egne sensorer, og har kontroll over hvordan den brukes.

Flere andre lands nasjonale responsmiljøer har etablert to parallelle spor når det er avdekket et angrep – ett etterretnings-/EOS-spor og ett samfunnssikkerhetsspor. Grunnen til at det er slik er det naturlige spenningsfeltet mellom rikets sikkerhet med stor grad av gradert informasjon og delingsbegrensninger, og samfunnets øvrige behov for åpenhet og informasjonsdeling.

21.3.3 Håndtere

Med *håndtering* mener utvalget aktiviteter som analyserer årsaker, begrenser skade og gjenoppretter drift av tjenestene. På et overordnet nivå består håndteringen i å se hendelser i sammenheng, dele informasjon og kunnskap om hendelser, samt prioritere og koordinere samfunnets innsats. Håndteringen skjer på flere nivåer i samfunnet, for eksempel i den enkelte virksomhet, i politiet eller ved NSM NorCERT.

Støtte til håndtering av hendelser. Større selskaper velger å bygge opp egne miljøer, enten internt i virksomheten, gjennom sektorvise responsmiljøer eller begge deler. De sektorvise responsmiljøene har en viktig rolle i å binde disse miljøene sammen og koordinere aktiviteten innad i sektoren. Mindre selskaper har ofte avtaler om støtte til hendelser som del av kontrakten med driftsleverandøren. NSM legger til grunn at de ulike sektorvise responsmiljøene vil løse oppdraget sitt slik det er beskrevet i *Nasjonal strategi for informasjonssikkerhet*. NSM fokuserer på de mest alvorlige målrettede angrepene, samt angrep som har potensial til å ramme tverrsektorielt. NSM mener derfor det vil være behov for en styrking av kapasiteten i NSM NorCERT for å holde tritt med økningen og utviklingen av digitale angrep.

Hendelseshåndtering og varsling. Ifølge NSM avdekket NSM NorCERT i 2014 88 alvorlige angrep mot norske bedrifter og myndigheter, se punkt 7.2 «Tilsiktede IKT-hendelser». Når saker meldes inn til NSM NorCERT, gjøres det en vurdering og prioritering i operasjonssenteret. Enkelte saker diskuteres også i Cyberkoordineringsgruppen (CKG). CKG legger ikke føringer på NSM NorCERTs prioriteringer, men diskusjonene kan gi et bredere bilde av trusselen. Man fordeler også ansvar for saker som berører alle tre tjenesters ansvarsområde. De viktigste kriteriene for prioritering er potensielle konsekvenser og omfanget av hendelsen.

---

[20] Justis- og beredskapsdepartementet (2014): *Modell for håndtering av IKT-sikkerhetshendelser – anbefalinger og retningslinjer.*

[21] Slik skadevare er ofte henvist til som «drive by malware» eller «vannhullsangrep», der skadelig programvare blir plassert på populære Internett-sider og installert i bakgrunnen uten at brukeren oppdager det.

Teknisk analyse av skadevare. Analyseevnen i Norge er delt mellom offentlige enheter (særlig NSM, Forsvaret og politiet) og private (enkelte virksomheter, driftsleverandører og kommersielle sikkerhetsleverandører). Enkelte driftsleverandører leverer tjenester innenfor analyse som del av sitt tjenestetilbud, i hovedsak logganalyse. Hovedvekten av analysekapasitet på leverandørsiden i Norge ligger hos mer dedikerte sikkerhetsleverandører. Teknisk analyse kan for eksempel innebære analyse av skadelig kode (reverse engineering), mistenkte infiserte maskiner (digital forensics) og logganalyse for avdekking og etterforskning. NSM NorCERT bistår innen sitt ansvarsområde med både koordinering av hendelser og teknisk analyse av maskiner, skadelig kode og logger. Evnen til analyse avhenger av en rekke forhold, som blant annet kapasiteten hos de ulike aktørene, kompetansen og tilgjengelige verktøy. Resultatet av slike analyser kan være svært viktig for effektiviteten i håndteringen av et digitalt angrep.

Politiets rolle ved håndtering av IKT-hendelser. Politiloven § 2 beskriver politiets primæroppgaver. I politiloven §§ 7 og 27 er politiet gitt omfattende fullmakter for å kunne ivareta disse oppgavene. Politiloven § 27 pålegger politiet å iverksette nødvendige tiltak for å avverge fare og begrense skade i forbindelse med alle ulykkes- og katastrofesituasjoner, og fastsetter at politiet har et akutt, sektorovergripende ansvar for å håndtere ulykker og katastrofer i fred på alle samfunnsområder. Ved en hendelse er politiet ved politimesteren i en akuttfase gitt myndighet til å fatte beslutninger på andre myndigheters ansvarsområde frem til ansvaret overtas av ansvarlig myndighet i henhold til ansvarsprinsippet.

21.3.4 Etterforske

Straffesakskjeden omfatter politiet og påtalemyndighetens arbeid med å forebygge, oppdage, etterforske og påtale kriminalitet, samt domstolenes iretteføring og kriminalomsorgens straffegjennomføring og tilbakeføring til samfunnet etter endt soning. Utvalget begrenser sin omtale til å gjelde kun den delen av straffesakskjeden som er knyttet til politi og påtalemyndighetenes arbeid.

Med å *etterforske* legger utvalget til grunn de aktiviteter politiet og PST utfører for å avklare om et straffbart forhold finner eller har funnet sted. Det er bare politiet og påtalemyndigheten som kan etterforske og påtale. Øvrige aktører kan ved behov bistå på etterforskningsstadiet. Arbeidet fordrer et tett samarbeid mellom private og offentlige aktører, både nasjonalt og internasjonalt.

Kompleksiteten ved IKT-kriminalitet. Etterforskning av IKT-kriminalitetssaker er svært ressurskrevende og krever ofte spesialisering og et utstrakt internasjonalt samarbeid.[22] Et gjennomgående trekk er at etterforskning har spor til utlandet, både til antatte bakmenn og medvirkere, men også flere fornærmede. I situasjoner der politiet ønsker å få utlevert informasjon fra utlandet, er tidsaspektet kritisk og sporing ofte vanskelig. Én av årsakene er ifølge Kripos at norske Internett-tilbyderes logger over hvem som kommuniserte med en IP-adresse, blir slettet tidlig i etterforskningsprosessen. IKT-kriminaliteten som avdekkes i Norge, er i mange tilfeller bare et lite ledd i et større organisert nettverk. Kriminelles bruk av blant annet kryptering og fiktiv identitet gjør etterforskningen særlig krevende.

Kapasitet i politiet. I 2012 gjennomførte politiet en kartlegging av politidistriktenes og særorganenes arbeid med IKT-kriminalitet, elektroniske spor og politiet på nett.[23] Samtlige politidistrikter opplyste i kartleggingen at IKT-kriminalitet i liten grad ble anmeldt, at mørketallene var store, og at sakene i stor grad ble henlagt. Av mindre alvorlige saker ble flere henvist til NorSIS' slettmeg-tjeneste. IKT-kriminalitet ble etterforsket av politidistriktene ved tradisjonelle etterforskningsmetoder, herunder avhør og bruk av IKT-tekniske undersøkelser. Tilstedeværelsen på Internett var ikke god nok. Enkelte politidistrikter etterforsket datainnbrudd mot private virksomheter, men kom i liten grad i mål med sakene. Årsaken var ofte manglende ressurser og begrenset tilgang på bistand fra Kripos.[24] Ressursene til IKT-tekniske undersøkelser varierte fra ingen til tre IKT-etterforskere per distrikt.[25] [26] Denne begrensede kapasiteten førte til at elektroniske spor kun ble brukt i de mest alvorlige straffesakene.

Kripos har flere seksjoner relatert til IKT-kriminalitet med i underkant av 70 ansatte. De fleste jobber med elektroniske spor og tilstedeværelse på Internett. Kripos' kapasitet til å etterforske

---

22 Meld. St. 7 (2010–2011) *Kampen mot organisert kriminalitet – en felles innsats.*

23 Politidirektoratet (2012): *Politiet i det digitale samfunnet - En arbeidsgrupperapport om: elektroniske spor, IKT-kriminalitet og politiarbeid på Internett.*

24 Ibid.

25 En *IKT-etterforsker* er en politifaglig eller sivil etterforsker som jobber med IKT-tekniske undersøkelser.

26 Politidirektoratet (2012): *Politiet i det digitale samfunnet - En arbeidsgrupperapport om: elektroniske spor, IKT-kriminalitet og politiarbeid på Internett.*

IKT-kriminalitet var i 2012 på mellom tre og fem sakskomplekser i året.

Av politidistriktene er det bare Oslo politidistrikt som har tilstrekkelig sakstilfang og kompetanse til å møte dagens utfordringer knyttet til IKT-kriminalitet. Distriktet har på grunn av sakstilfanget en sentral rolle når det gjelder å håndtere straffesaker i Norge, også innen IKT-kriminalitet. Distriktet har en egen enhet for datakriminalitet med i overkant av 20 ansatte. Enheten jobber primært med å tilrettelegge for sikring av elektroniske spor i alle typer straffesaker i politidistriktet.

Utvalget observerer at hovedressursen i politiet innenfor etterforskning primært brukes til sikring av elektroniske spor og ikke til etterforskning av IKT-kriminalitetssaker.

Nærpolitireformen tar for seg politi- og lensmannsetatens struktur, oppgaveportefølje og ansvarsdeling fremover. Dagens 27 distrikter skal reduseres til 12. Nå som politidistriktinndelingen er fastsatt, skal organiseringen av særorganene utredes.

21.4 Hindre for effektivt samarbeid

Det ser ut til å være flere forhold som er til hinder for effektivt samarbeid og informasjonsdeling mellom myndighetsaktører og private aktører. Dette innebærer uklarheter knyttet til roller og ansvar, en utilstrekkelig samarbeids- og delingskultur, manglende verktøy for utveksling av sensitiv og gradert informasjon. Mangelfull gjennomføring og evaluering av øvelser vil være et hinder for effektiv samhandling. Dette er drøftet i kapittel 20 «Styring og kriseledelse».

Utvalget merker seg at retningslinjene for åpenhet rundt IKT-hendelser kun omtaler informasjonsflyten fra virksomheter til myndighetene og ikke behovet for åpenhet fra myndighetenes side.

21.4.1 Utfordringer knyttet til roller og ansvar

Tradisjonell ansvarsdeling mellom etatene bygger på den forutsetningen at man allerede vet hvem som står bak en hendelse. Denne forutsetningen er svært ofte ikke til stede tidsnok ved digitale angrep. En ytterligere utfordring er at organisering gjerne er knyttet til geografisk nærhet til hendelsen ved tradisjonelle kriser og hendelser i samfunnet. Ved digitale angrep er geografisk nærhet ofte irrelevant. Utvalget har observert en rekke utfordringer sett fra aktørenes forskjellige ståsteder. Én av disse er knyttet til politiets manglende tilstedeværelse under håndtering av hendelser. Politidirektoratet peker på at det i initialfasen av et angrep er grunnleggende utfordringer med å identifisere hvem som står bak angrepet, og hva formålet er – om det er IKT-kriminalitet, spionasje, sabotasje eller terror. POD mener dette utfordrer arbeidsfordelingen mellom ulike myndighetsorganer på området. Kripos viser til at saker ofte blir liggende til vurdering hos CKG (og/eller PST) i såpass lang tid at de ikke er egnet til etterforskning når politiet får kjennskap til dem.

For virksomheter og leverandører er det ofte uklart hvem de skal forholde seg til på myndighetssiden. Utvalget er kjent med flere hendelser der det har vært usikkerhet knyttet til hvor man skal anmelde forholdet. En annen bekymring fra Politidirektoratet er at politiet ikke i tilstrekkelig grad får delta i det arbeidet som i dag skjer i NSM NorCERT og CKG-samarbeidet. En av begrunnelsene fra NSM har vært at NSM NorCERTs samarbeidspartnere ikke ønsker at deres informasjon skal tilflyte politiet, som kan åpne etterforskning av saken.

Straffeprosessloven § 224 regulerer når politiet åpner etterforskning ved anmeldelse eller der andre omstendigheter tilsier at det er rimelig grunn til å undersøke om det foreligger et straffbart forhold. Avgjørelsen beror på en skjønnsmessig vurdering av blant annet alvorligheten, omfanget av etterforskningen og bruken av ressurser. For IKT-kriminalitet kan ofte muligheten for å oppklare være liten, noe som kan gi grunnlag for å unnlate å åpne etterforskning. Det vises også til det alminnelige opportunitetsprinsippet i straffeprosessloven § 69 for påtalemyndigheten, som gir påtalemyndigheten en viss adgang til å unnlate å påtale handlinger av særlige grunner. Det er således viktig å tydeliggjøre alternativene regelverket gir til å åpne etterforskning.

Dagens avtaler mellom NSM og VDI-partnere og medlemmer legger formålsbegrensninger på bruk av VDI-informasjon. Denne informasjonen kan bare benyttes til håndtering av alvorlige IKT-hendelser. Det følger videre av avtalene at informasjonen ikke kan deles med tredjeparter uten at virksomheten har samtykket. Unntaket fra dette er deling med de øvrige EOS-tjenestene innenfor rammen av NSM NorCERTs formål. NSM uttrykker bekymring for at informasjonsdeling med politiet vil kunne sette en stopper for VDI-samarbeidet hvis prinsippet om VDI-partnerens eierskap til informasjonen undergraves. NSM anbefaler imidlertid virksomhetene systematisk å anmelde even-

tuelle straffbare forhold som avdekkes gjennom VDI-samarbeidet.

Det er uklart for utvalget om bekymringen rundt mulig informasjonsflyt til politiet kan bekreftes av NSM NorCERTs samarbeidspartnere. Uklarheter av en slik karakter kan medføre at aktørene selv håndterer hendelser som burde blitt overført til en annen etat eller et sektorvis responsmiljø.

Ressursgruppen opplever at det ikke er entydig hvem som har beslutningsmyndighet til å iverksette tiltak, dersom det oppstår interessekonflikter mellom aktører under håndtering av hendelser. Det kan eksempelvis være motsetningsforhold mellom en virksomhet/sektors interesser og NSM NorCERTs interesser, eller mellom en virksomhet/sektors interesser og øvrige myndigheter med særlig ansvar for sikkerhet. NSM viser til at det på dette området eksisterer et sivilt beredskapsplanverk som gir ulike aktører ulike fullmakter i det øvre spekteret av krisehåndtering. Videre viser NSM til at det i det lavere spekteret av krisehåndtering ligger et lovforslag til behandling i Justis- og beredskapsdepartementet som blant annet inneholder forslag til myndighet og fullmakter til logging av data ved håndtering av hendelser.

Flertallet av hendelser håndteres i praksis av de ulike virksomhetene som rammes. NSM NorCERT viser til at de bistår med håndtering av alvorlige dataangrep uten myndighet til å pålegge virksomheter å utføre utbedringer, utlevere data eller la systemer være i drift til støtte for kartleggingsformål. Politiet, derimot, har i noen grad slik myndighet i dag, hjemlet i politiloven med flere, men er i mindre grad involvert i den operative håndteringen av digitale angrep. NSM samarbeider innen rammen av sitt mandat løpende med PST, som kan benytte tvangsmidler.

21.4.2 Mangel på et felles operativt situasjonsbilde

Et omforent situasjonsbilde er en forutsetning for å kunne ha et enhetlig beslutningsunderlag for å styrke evnen til å iverksette nødvendige tiltak mellom de involverte i en hendelse. Det er avgjørende at enhetene som besitter denne informasjonen, er gode på kommunikasjon og informasjonsutveksling på taktisk nivå både internt og overfor berørte virksomheter og beslutningstagere. Det er ifølge Ressursgruppen krevende for mange virksomheter å ha nok kompetanse og kapasitet til å ha denne forståelsen, da situasjonsbildet endres stadig hurtigere. Utfordringer knyttet til manglende felles situasjonsbilde er uttrykt gjennom flere utredninger. NSM har nylig uttrykt at situasjonsbildet knyttet til sårbarheter i viktig norsk IKT-infrastruktur er avhengig av et godt samarbeid mellom myndigheter og aktuelle selskaper, og peker på utfordringene knyttet til dagens VDI i denne sammenheng.

21.4.3 Utfordringer knyttet til utveksling av gradert og sensitiv ikke-gradert informasjon på tvers av sektorer

NSM, Etterretningstjenesten og PST mottar mye gradert informasjon fra andre lands samarbeidende tjenester med distribusjonsrestriksjoner. I tillegg opplever flere aktører utfordringer innenfor utveksling av informasjon gradert etter sikkerhetsloven grunnet manglende infrastruktur og/eller at personell ikke er klarert for å motta sikkerhetsgradert informasjon. Dette gjelder spesielt politiet, direktorater og private aktører. NSM mener det er en stor utfordring at få private virksomheter er underlagt sikkerhetsloven. En av de siste erfaringene med dette var fra håndteringen av terrortrusselen sommeren 2014.

Utvalget er kjent med at Forsvarsdepartementet og Justis- og beredskapsdepartementet jobber med å implementere en løsning for lavgradert infrastruktur mellom departementene.

21.5 Utfordringer knyttet til avdekking av sårbarheter og deteksjon av IKT-hendelser

21.5.1 Utilstrekkelig evne til å oppdage IKT-hendelser

Det er som tidligere beskrevet store forskjeller når det gjelder grad av monitorering i ulike virksomheter og bransjer. Disse forskjellene kan ha ulike årsaker. Virksomheter som har vært utsatt for målrettede spionasjeangrep, synes i større grad å ha etablert deteksjonsmekanismer som avdekker ukjente angrep, i tillegg til mer tradisjonelle, signaturbaserte systemer. Evne til å oppdage handler imidlertid om mer enn bare teknologi. Det er krevende for virksomhetene å ha kompetanse til å følge opp og ha forståelse for det som blir oppdaget.

For den nasjonale evnen til å avdekke hendelser er NSM NorCERT avhengig av informasjon fra samarbeidspartnerne og fra etterretningstjenestene. VDI-sensorene gir NSM NorCERT viktig informasjon. VDI-sensorenes evne til å avdekke er begrenset av datainnsamlingen som sensorene utfører. Sensorene forholder seg i dag hovedsake-

lig til metadata. Unntaket er at ved en VDI alarm vil sensoren lagre innholdsdata fra 2–3 IP-pakker for å understøtte det videre analysearbeidet. Dette er hensiktsmessig i forhold til oppdraget NSM NorCERT har, da man vil evne å avdekke digitale angrep mot virksomheter, bare ved hjelp av metadata. VDI-sensorene er i dag ikke satt opp til å trigge alarmer basert på innholdsdata.

VDI-sensorene har i dag ingen mulighet til å se innholdet i trafikk som går kryptert. I fremtiden vil VDI-sensorene i noen grad kunne dekryptere trafikk, da man vil benytte brannmurens dekrypteringsfunksjonalitet. Dette vil være en viktig føring i den fremtidige VDI-strategien når det gjelder plassering av sensorer. Som beskrevet i kapittel 6 «Trender som påvirker sårbarhetsbildet», krypterer trusselaktørene trafikken sin i økende grad, noe som er en stor utfordring for nettverksbaserte signaturbaserte deteksjonsmekanismer. En annen utfordring med signaturbaserte deteksjonsmekanismer er at angrepsmetoden må være kjent før den kan oppdages.

NSM har erkjent at det er behov for flere sensorer, og det er i dag en lang kø av virksomheter som ønsker sensor. Andelen virksomheter som inngår i nettverket, samt begrensninger i teknologien, gjør at VDI-sensornettverket ikke dekker behovet for å avdekke digitale angrep mot kritisk infrastruktur og informasjon i Norge i dag.

I et lovforslag NSM har oversendt Justis- og beredskapsdepartementet, ligger det inne et forslag om å pålegge ulike typer sensorer, i tillegg til at det skal pålegges en plikt til rapportering også utover sikkerhetsloven.

Som tidligere beskrevet er samarbeidet i CKG sentralt i arbeidet med å avdekke digitale angrep blant annet knyttet til rikets sikkerhet. Etterretningstjenesten har uttrykt at

> «kommunikasjonsetterretning frembringer i særklasse mest av den type informasjon som bidrar til både å forhindre terrorhandlinger og å oppdage den mest alvorlige skadevaren som treffer våre vitale datanettverk».[27]

For å kunne oppdage, varsle og håndtere utenlandske trusler som terror, spionasje og digitale angrep trengs det ifølge Etterretningstjenesten å kunne følge med på relevant Internett-trafikk som går via kabler (såkalt grenseforsvar). Denne muligheten finnes ikke i Norge i dag.

21.5.2 Varierende og tidvis motstridende krav til logging og sletting av samme informasjon

Ressursgruppen peker på områder der krav til logging og sletting av samme form for informasjon underlegges ulike krav i ulike sektorlovverk. Virksomheter i enkelte sektorer har sektorregelverk som gir rom for mange års lagringstid, mens andre sektorer har hjemler som begrenser lagring til noen få dager. Kort lagringstid kan få konsekvenser for de operative miljøenes håndteringsevne og for effektiv straffeforfølgning. Det kan oppleves som en utfordring at dette ikke er standardisert på tvers av sektorer. For å gi lengre lagringstid kreves omfattende lovendringer. Graver og Harborg har levert en utredning om datalagring.[28]

Utvalget er kjent med at det foreligger forslag om å anbefale minimumslogging i ugraderte, men sensitive IKT-systemer i statlig sektor. Forslaget er utarbeidet av NSM på oppdrag fra Justis- og beredskapsdepartementet.

21.5.3 Mangelfullt grunnlag for et helhetlig IKT-trusselbilde

Det finnes ingen helhetlig statistikk over omfanget av digitale angrep i Norge, og heller ingen helhetlig fremstilling av IKT-trusselbildet. Aktører involvert i å avdekke, håndtere og etterforske digitale angrep har ofte egen statistikk over saker de er involvert i, men dette samles ikke noe sted. Politiet viser til at de har dårlig statistisk grunnlag for IKT-kriminalitetsbildet. Enkelte sektorer stiller krav om rapportering av hendelser, men det er ingen entydig kategorisering eller samling av denne typen rapporter. Manglende rapportering av IKT-hendelser begrenser vår evne til å få et felles og korrekt IKT-trusselbilde, og dermed evnen til å forebygge og håndtere digitale hendelser.

21.6 Kapasitets- og kompetanseutfordringer knyttet til håndtering av digitale angrep

21.6.1 Kompetanse- og kapasitetsutfordringer ved håndtering av hendelser

En rekke kapasitets- og kompetanseutfordringer vil ha innvirkning på evnen til effektivt å håndtere

[27] Generalløytnant Kjell Grandhagen, Sjef Etterretningstjenesten (16. mars 2015): Foredrag i Oslo Militære Samfund *«Trusler og risiki for Norge i et endret sikkerhetsbilde»*.

[28] Graver, H. P., Harborg H. (2015): *Datalagring og menneskerettighetene – Utredning til Justis- og beredskapsdepartementet og Samferdselsdepartementet.*

hendelser. Som det går frem av innledende beskrivelser i punkt 21.3 «Håndteringskjeden ved tilsiktede hendelser» har i dag mange virksomheter, særlig små og mellomstore, mindre IKT-miljøer internt, eller IKT-løsninger som leveres av en ekstern leverandør. Mange mindre IKT-miljøer har i liten grad kompetanse til å forstå situasjonsbildet, sårbarheter, indikatorer på et angrep, og så videre. Utvalget er kjent med at enkelte virksomheter opplever at det er en ubalanse mellom tilbud og etterspørsel av tjenester hos NSM NorCERT.

NSM har uttrykt at det er vanskelig å rekruttere og holde på kompetanse, idet denne er etterspurt av flere aktører. Med styrkingen av responsmiljøer i sektorer og virksomheter, og med økt vekt på sikkerhet i næringslivet, antar NSM at etterspørselen etter kompetanse vil øke i tiden fremover.

21.6.2 Fragmentert analysekapasitet mellom offentlige og private aktører

Resultatet av analyser er svært viktig for å kunne håndtere et digitalt angrep effektivt. Analysekapasiteten i Norge er delt mellom offentlige enheter, private virksomheter, driftsleverandører, kommersielle sikkerhetsleverandører og frivillige organisasjoner. Kapasiteten til Etterretningstjenesten og PST er av sikkerhetsmessige årsaker ikke offentlig kjent. I større og/eller flere parallelle digitale angrep opplever flere av virksomhetenes operative miljøer at analysekapasiteten er begrenset. Manglende og forsinkede analyser kan føre til at håndteringen av en sak blir forsinket. I tillegg fører det gjerne til at beslutninger må tas på mangelfullt eller feil grunnlag, noe som igjen kan føre til økte eller ukjente konsekvenser av hendelsen.

Effektiv analyse forutsetter inngående kjennskap til hvordan et system fungerer i en normalsituasjon, og det kreves ulik kompetanse det ofte er knapphet på. Få virksomheter i Norge har selv tilgang på effektive verktøy for å gjennomføre analysen. Dette påvirker kvaliteten og tiden det tar å utføre analysen. Økokrim driver analyse blant annet innenfor kriminaletterretning basert på mistenkelige transaksjoner i samarbeid med finansinstitusjoner i Norge.

21.6.3 Utfordringer knyttet til sektorvise responsmiljøer og skaleringsbehov ved større hendelser

Virksomhetene bygger opp egne responsmiljøer, enten internt i virksomheten, gjennom sektorvise responsmiljøer eller begge deler. Det fører til mindre miljøer med parallelle aktiviteter som kjemper om den samme kompetansen. Dette kan i neste omgang medføre at den totale utnyttelsen av ressursene i Norge med kompetanse innenfor digitale angrep blir mindre effektiv.

NSM NorCERT har vist til at dagens modell ikke er skalerbar for fremtidens utfordringer, og har uttrykt at utviklingen av sektorvise responsmiljøer er helt nødvendig. NSM har i dag ikke kapasitet til å bistå eiere av kritisk IKT-infrastruktur i tilstrekkelig grad. Innenfor eksempelvis teknisk analyse vil imidlertid NSM NorCERT med utgangspunkt i ansvar for å håndtere nasjonale utfordringer også kunne bistå med spisskompetanse der det av kapasitetshensyn ikke bør bygges opp kompetanse i hver enkelt sektor. NSM mener det er viktig å ha fungerende tilpasset håndteringskompetanse i alle større sektorer, men at vi er i ferd med å nå et krysningspunkt der det blir mangel på kompetanse. Det er viktig med en sterk nasjonal evne, men det er også viktig å ha respekt for de faglige vurderingene og lokalkunnskapen innenfor hver enkelt virksomhet. Politidirektoratet er også bekymret for opprettelsen av de mange sektorvise responsmiljøene, på grunn av at det er et begrenset antall personer i Norge som kan fylle stillingene. Politidirektoratet mener en alternativ strategi vil være å samle ressursene i én felles CERT-funksjon.

Utover at NSM NorCERT arrangerer forum for sektor-CSIRT, er det ikke noe formalisert samarbeid mellom sektor-CSIRT-ene. Det betyr at informasjonen en sektor-CSIRT sitter på som er av interesse for andre miljøer, i dag ikke deles gjennom standardprosesser og grensesnitt med andre sektor-CSIRT-er. Informasjonsdelingen blir i for stor grad personavhengig og tilfeldig.

Forsvaret kan, som tidligere nevnt, gi bistand til sivile myndigheter ved alvorlige cyberhendelser i henhold til gjeldende prinsipper og regelverk. Å utnytte denne kapasiteten krever imidlertid en bistandsanmodning, som erfaring fra øvelser viser at det tar tid å effektuere. Det er også viktig å være klar over at Forsvarets operative ressurser primært er skalert for å adressere Forsvarets eget behov.

21.7 Kapasitet-, kompetanse- og prioriteringsutfordringer i politiet

Virksomheter og enkeltindivider anmelder i liten grad IKT-kriminalitet til politiet, og det er store mørketall. Årsaker virksomhetene oppgir, er blant annet forventningen om at forholdet vil bli hen-

lagt, og at det ikke er mulig å finne gjerningspersonen. Enkeltindividet blir ofte henvist av politiet til andre aktører, som råd- og forsikringstjenester. Manglende anmeldelser gir politiet begrenset kunnskap og oversikt over den totale IKT-kriminaliteten.

21.7.1 Utfordringer knyttet til rammefaktorer

Politiet er en sterkt regulert virksomhet. Internasjonalt oppgir flere land at eget nasjonalt lovverk i liten grad reflekterer den teknologiske utviklingen.[29] Prosesser for utlevering av informasjon i straffesaker er for eksempel ikke tilstrekkelig tilpasset sikring av elektroniske spor. Innenfor EU utgjør ulikheter i nasjonale regelverk og manglende harmonisering et betydelig hinder for å oppdage og utveksle informasjon om grenseoverskridende IKT-kriminalitet.

IKT-kriminalitet har ofte internasjonale forgreninger. Anmodninger til andre lands myndigheter og samarbeid med internasjonale tjenesteleverandører er både utfordrende og tidkrevende. Dagens system for internasjonal informasjonsutveksling[30] mellom politi på tvers av landegrenser går for tregt. Avtalene er i stor grad basert på tradisjonell praksis for utlevering av fysiske bevis mellom land, og tar ikke innover seg den teknologiske utviklingen. Utvalget er kjent med at det i EU jobbes med effektivisering av prosessen i lys av den teknologiske utviklingen. Norge deltar i liten grad i internasjonale «innsatsstyrker» rettet mot bekjempelse av IKT-kriminalitet.

I dag finner en digitale spor i nærmest enhver straffesak. Økt bruk av kryptering er en stor utfordring for politiet. Det fører ofte til at saker henlegges i situasjoner der beslagene ikke lar seg lese. Dataavlesing[31] er derfor en etterspurt metode, både fra politiet og fra PST, for å imøtekomme denne utviklingen. Dataavlesing er utredet i kapittel 23 i NOU 2009: 15 Skjult informasjon – åpen kontroll.

[29] UNODC (2013): *Comprehensive Studyon Cybercrime (Draft)*.

[30] Mutual Legal Assistance Treaty (MLAT).

[31] Dataavlesing er en samling teknikker for å skaffe seg tilgang til kommunikasjonen på et stadium før den blir gjort uleselig ved kryptering. Én måte er å koble til en passiv avlyttingsenhet mellom tastatur og maskin, eller installere spionprogramvare på den mistenktes datautstyr gjennom et datainnbrudd.

21.7.2 Mangelfull kapasitet i politiet

Politiet etterforsker i dag i relativt liten grad IKT-kriminalitet.[32] Utvalget er gjort kjent med at det kan forekomme store restanser av ubehandlede saker knyttet til elektroniske spor innenfor alle kriminalitetsformer. Kapasiteten og ressursene når det gjelder elektroniske spor, brukes til å støtte all etterforskning ved politidistriktet.

Bekjempelse av IKT-kriminalitet krever i økende grad internasjonalt samarbeid og er teknologikrevende. Det økende behovet for bistand i politidistriktene og i interne enheter i Kripos går på bekostning av særorganets metodeutvikling og etterforskning av egne IKT-kriminalitetssaker. Justis- og beredskapsdepartementet har gitt POD i oppdrag å utrede alternativer knyttet til å opprette et nasjonalt «Cyber Crime Center» for å styrke politiets kapasitet og innsats på området.

Politidirektoratet viser til at det er mangel på kompetanse i politiet til å håndtere utfordringer som følge av teknologiutviklingen. PODs kartlegging *Politiet i det digitale samfunn* pekte på behovet for både etterforsknings- og teknisk kompetanse. Distriktene lykkes bare delvis med å oppnå ønsket tverrfaglighet.

Når det gjelder påtale, viser kartleggingen at bare politiadvokatene ved Kripos' seksjon for datakriminalitet har spesialisert kompetanse på IKT-kriminalitet. Når det gjelder håndtering av elektroniske spor i ulike typer straffesaker, har både statsadvokatene og erfarne politiadvokater nå betydelig erfaring.

Oslo politidistrikt er som nevnt tidligere det eneste distriktet med både kompetanse og mengdetrening i å håndtere IKT-kriminalitet som ellers naturlig faller inn under Kripos' ansvarsområde.

Politiadvokatene tilknyttet Kripos' seksjon for IKT-kriminalitet har særskilt kompetanse innen etterforskning av IKT-kriminalitet. Den høyere påtalemyndigheten kan ikke vise til tilsvarende erfaring og kompetanse på området.

Politidirektoratet peker på behovet for tverrfaglighet, herunder ingeniørstillinger. Utfordringen ligger blant annet i at tildelte polititjenestemannsstillinger ofte ikke kan gjøres om til sivile stillinger av hensyn til politiske føringer. Politidistriktene må derfor opprette sivile ingeniørstillinger for egne driftsmidler.

[32] Næringslivets sikkerhetsråd (2014): *Mørketallsundersøkelsen 2014 – Informasjonssikkerhet, personvern og datakriminalitet*. Se også tall fra Strafferegistret (2014) over antall registrerte anmeldelser.

Oslo politidistrikt mener det er utfordrende å bygge opp kompetanse i samtlige politidistrikter. Distriktet opplever at det er lett å rekruttere sivile teknologer, men sliter med å rekruttere politiutdannede til datakrimenheten.

Ved Politihøgskolen (PHS) er undervisning i digitalt politiarbeid nylig blitt en del av den obligatoriske grunnutdanningen. Hensikten er å gi politistudentene grunnleggende forståelse for sikring av digitale spor fra datautstyr, over Internett og fra mobiltelefoner.

PHS tilbyr etterutdanning i IKT-tekniske undersøkelser rettet mot håndtering av ulike former for digitale spor og et tilbud til sivile dataingeniører i politiet med tanke på begrenset politimyndighet.

Ved Center for Cyber and Information Security (CCIS) er det etablert en forskningsgruppe i samarbeid med Politihøgskolen. Den består av fire professorer innen fagfeltet. I tillegg etablerte PHS og CCIS en erfaringsbasert mastergrad innen informasjonssikkerhet og dataetterforskning i 2014. Politidirektoratet støtter forskningsgruppen ved CCIS økonomisk, og ønsker å styrke dette samarbeidet ytterligere.

Justis- og beredskapsdepartementet har i sin strategi for å bekjempe IKT-kriminalitet (2015) bedt Politidirektoratet sette i gang en rekke tiltak. Blant annet for å heve digital og politifaglig kompetanse, utarbeide en forskningsstrategi for å forebygge og bekjempe IKT-kriminalitet, styrke etterforskningskapasiteten og styrke det nasjonale og internasjonale samarbeidet.[33]

21.7.3 Uklarheter knyttet til hvilken aktør som skal etterforske

Anmeldelse av digitale angrep skal skje til det lokale politidistriktet – det til tross for at lokale politidistrikter ofte verken har ressurser eller kompetanse til å etterforske IKT-kriminalitet. Hvor saken skal videre i politiet, er avhengig av trusselaktøren og intensjonen med angrepet. Anmeldelser av IKT-kriminalitet kan dermed etterforskes ved det enkelte politidistrikt, Kripos, Økokrim eller PST. I initialfasen av saksgangen er det ofte vanskelig å avgjøre hvor saken hører hjemme, særlig der det er usikkerhet knyttet til trusselaktøren, for eksempel om dataspionasje er utført av en statlig eller ikke-statlig aktør. Saken må i slike tilfeller ofte overføres mellom ulike instanser i politiet. Det kan skape merarbeid for virksomheten som anmeldte forholdet, og etterforskningen sett under ett tar lengre tid. Virksomhetene opplever også at det kan ha betydning for utfallet av saken hvilken instans i politiet som etterforsker.

21.7.4 Prioriteringsutfordringer

I Riksadvokatens årlige rundskriv[34] er alvorlig IKT-kriminalitet vist til som en av de prioriterte sakstypene i samtlige politidistrikters straffesaksbehandling. Politidistriktene og Kripos må daglig prioritere IKT-kriminalitet opp mot andre typer alvorlig kriminalitet, som for eksempel vold og narkotikasaker, som ofte har høyere strafferammer. Kompetansen i digitalt politiarbeid er som tidligere nevnt så mangelfull i politidistriktene at de i stor grad må be om bistand fra Kripos. Kripos bruker av den grunn mye kapasitet på mindre alvorlige IKT-kriminalitetssaker, selv om de kunne håndtert mer alvorlige saker.

Funn i *Politianalysen* viser at svært få ressurser var dedikert til operativ analyse og forebyggende politiarbeid. Mesteparten av ressursene i politidistriktene gikk til straffeforfølgning og synlig tilstedeværelse.[35] Straffeforfølging av IKT-kriminalitet er ofte grenseoverskridende og svært ressurskrevende. Teknologien gjør det dessuten lett for kriminelle å skjule sin identitet. Disse faktorene bidrar til at en straffeforfølgning ofte kan ende med henleggelse. Politidirektoratet mener politiets innsats mot IKT-kriminalitet bør legge mer vekt på det forebyggende arbeidet enn det som er situasjonen dag.

Det er begrenset analysekapasitet i de fleste politidistrikter. De fremste fagmiljøene finnes hos Kripos og i Oslo politidistrikt. Erfaring med operativ analyse i IKT-straffesaker er begrenset, blant annet fordi få slike saker etterforskes.

Den generelle etterretningskapasiteten i politidistriktene er lav med unntak av Oslo politidistrikt, som sammen med Kripos har bygd opp en operativ etterretningskapasitet på området.

---

[33] Justis- og beredskapsdepartementet (2015): *Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet.*

[34] Riksadvokaten (2015): Rundskriv nr. 1/2015 *Mål og prioriteringer for straffesaksbehandlingen i 2015 – Politiet og statsadvokatene.*

[35] NOU 2013: 9 *Ett politi – rustet til å møte fremtidens utfordringer – Politianalysen.*

21.8 Manglende evne til videreutvikling av og investering i politiets IKT-systemer

Det er stort behov for økt overføringskapasitet og redundans i politiets IKT-infrastruktur. I tillegg er det utfordringer knyttet til å opprettholde kompetanse for videreutvikling av politiets systemer, support utover normal arbeidstid, samt standardisering av lokale IKT-løsninger. Drift av datalagre og nødvendige verktøy for IKT-tekniske undersøkelser håndteres i dag av hvert enkelt politidistrikt. Ikrafttredelsen av ny straffelov av 2005 har grunnet IKT-situasjonen i politiet blitt utsatt. Implementeringen av lovendringene skjer nå i gamle systemer. Politiets manglende oversikt over dagens IKT-kriminalitetsbilde skyldes blant annet utdaterte IKT-verktøy for registrering av kriminaliteten (STRASAK).

Justis- og beredskapsdepartementet uttrykker en sterk bekymring for IKT-situasjonen i politiet, særlig knyttet til sårbarheter i IKT-infrastrukturen. Informasjon er en kritisk innsatsfaktor for politiet, og konsekvensene av at politiets datasentre blir utilgjengelige, er store. Nedetid i politiets datasenter kan innebære langvarig begrenset operativ kapasitet.

Politidirektoratet fremhever også at IKT-sikkerhetsarbeidet i politiet har vært mangelfullt over lang tid, og at det er behov for en tung satsing på IKT-infrastruktur. Et grunnleggende styringsprinsipp i staten er mål- og resultatstyring, som også ligger til grunn for styringen av politiet. De operative enhetene i politiet mottar en ettårsramme som alle IKT-investeringene må dekkes innenfor. POD viser til behovet for mer langsiktige investeringsbudsjetter med mulighet for å planlegge utover ett år.

Merverdiprogrammet ble opprettet i 2012, blant annet med sikte på en mer langsiktig investering og modernisering av norsk politi, herunder nye IKT-verktøy og arbeidsformer for å øke tilgjengelighet, effektivitet og fleksibilitet.[36] Programmet ble i 2015 delt opp i mindre prosjekter for å redusere risikoen i IKT-fornyingen av politiet.

[36] Politidirektoratet (2013–2014): *Merverdiprogrammet – Politiets program for merverdi av kunnskap, ressurser og teknologi.*

21.9 Sårbarheter som påvirker private virksomheter og enkeltindividets evne til å håndtere hendelser

21.9.1 Utilstrekkelig støtte for innbyggerne og SMB

Vår nasjonale sikkerhet er avhengig av enkeltindividets og virksomhetenes IKT-sikkerhet. Det er krevende for den enkelte borger både å forstå og å gjøre de riktige valgene ut fra kompleksiteten i teknologien, og det hviler mye ansvar på brukeren av teknologien. Forbrukerrådet understreker viktigheten av sikkerhet og personvern. Særlige utsatte grupper er for eksempel eldre med begrenset digital kompetanse og unge på grunn av at handlinger kan få konsekvenser gjennom et langt liv. NorSIS har en rådgivende rolle overfor forbrukeren. Tall fra NorSIS' tjeneste slettmeg.no viser at alvorlighetsgraden i flere av de sakene NorSIS blir kontaktet om, øker. NorSIS ser en økning i antall henvendelser fra personer eldre enn 26 år og i bruken av selvhjelpstjenestene. 7 500 kontaktet tjenesten i 2014, og utviklingen så langt indikerer en vekst på 20 prosent i løpet av 2015. NorSIS oppgir at de har begrenset kapasitet til å håndtere slike henvendelser.

NorSIS utfører årlige spørreundersøkelser om misbruk av identitet, og tallene mellom 2010 og 2013 viste en økning fra 3,1 prosent til 5,9 prosent. For 2014 oppgis det en nedgang til 3,2 prosent. På grunn av manglende ressurser har NorSIS måttet begrense prosjektet, men de har opprettholdt den årlige konferansen om idtyveri, samt at de svarer på telefonhenvendelser fra forbrukere. NorSIS har registrert en nedgang i antall henvendelser de siste årene, og mener det kan ha sammenheng med at forsikringsselskaper har tatt tak i denne problemstillingen.

På bakgrunn av dette kan det synes som om innbyggerne og SMB ikke har et godt nok tilbud om hjelp, råd og veiledning når de blir utsatt for hendelser. Se også punkt 19.6 «Kunnskap og støtte til befolkningen».

21.9.2 Manglende operative krav i anskaffelser og styring av drifts- og tjenesteleverandører

De fleste virksomheter benytter seg av drifts- og tjenesteleverandører i større eller mindre grad. Ressursgruppen peker på at det kan være vanskelig for virksomheter å følge opp leverandører, som ofte er de som kan bistå under og etter et digitalt angrep. Dette kan for eksempel skyldes man-

glende bestillerkompetanse, som ofte er vanskelig å løse gjennom hver enkelt virksomhets avtale med leverandøren. Ressursgruppen har påpekt utfordringer i anskaffelsesprosessen, der det ofte ikke stilles krav på området, som eksempelvis krav til operativ evne, analysekapasitet, styring og samhandling.

Dersom tjenestene leveres fra andre land og kunden ikke har stilt presise nok krav, vil dette kunne få konsekvenser for overlevering av data i forbindelse med håndtering av digitale angrep. Ofte må de nasjonale CSIRT-funksjonene involveres, og informasjonen må gjennom mange ledd før den når de operative miljøene som faktisk kan nyttiggjøre seg den. Ressursgruppen har eksempler på hendelser der data ikke har blitt utlevert på grunn av det politiske forholdet mellom Norge og det aktuelle landet. Dette kan føre til betydelige forsinkelser for håndtering av alvorlige dataangrep.

21.10 Aktuelle dilemmaer i forbindelse med utvidede metoder for å avdekke, håndtere og etterforske digitale angrep

Utvalget er bedt om å beskrive dilemmaer som kan oppstå som følge av behovet for å avdekke, håndtere og etterforske digitale angrep. Ut fra mandatets beskrivelse oppfatter vi at det bes om å redegjøre for vurderinger som må gjøres for å finne en forsvarlig balanse mellom ulike berettigede, men likevel motstridende, hensyn.

Dagens metodebruk er strengt lovregulert og kontrollert. Nye metoder som krever lovendringer, må vurderes konkret ut fra de reelle fordelene, ulempene og de mulige alternativene som kan være egnet for de formålene metodene skal betjene. Et beslutningsgrunnlag for å vurdere etablering av nye skjulte metoder stiller andre krav til mandat enn Lysneutvalgets. Lysneutvalget begrenser seg derfor til å adressere grunnleggende synspunkter på dilemmaer som følge av uttalte behov for å utvide etterretnings- og etterforskningsmetoder, samt å løfte frem enkelte overordnede, prinsipielt motstridende, hensyn. Fremstillingen nedenfor beskriver blant annet nødvendigheten av avveininger og balanse mellom hensyn som nasjonal sikkerhet og den enkelte borgerens personvern og ytringsfrihet.

21.10.1 Behovet for nye etterretnings- og etterforskningsmetoder

Siden Snowden-avsløringene i 2013 har hele verden vært opptatt av myndighetenes overvåking av privatpersoner gjennom bruk av teknologi. I lys av avsløringene har digital kommunikasjon i økende grad blitt kryptert av tjenesteleverandører, og det har vært en vekst i bruk av anonymiseringstjenester. Denne utviklingen setter myndighetene på prøve, idet tidligere skjulte metoder ikke lenger er like effektive.

Utvalget ser at det kan være behov for ytterligere skjulte metoder, men nettopp fordi de skal være skjult, er disse metodene også de mest inngripende. Selv om målet med metodene er rettet mot kriminell aktivitet, vil adgangen til å benytte slike metoder i prinsippet kunne være inngripende overfor den enkelte borger. Angrep på kritisk infrastruktur, kritiske samfunnsfunksjoner og tilsvarende alvorlig kriminalitet er skadelig for samfunnets trygghet, enkeltindividers integritet, økonomiske verdier og stabiliteten og kvaliteten på det samfunnet vi lever i. Effektiv avdekking av angrep og kriminalitetsbekjempelse er viktig, og det er avgjørende å sørge for nødvendige virkemidler for å kunne ivareta denne oppgaven. Det er vesentlig at både E-tjenesten, PST og politiet har anledning til å innhente tilstrekkelige mengder ulik informasjon for å kunne utføre sine oppgaver.

Etterretningstjenestens og politiets oppgave med å bekjempe kriminalitet forutsetter myndighet til å kunne innhente informasjon ved å kunne utøve makt og tvang overfor borgerne. Gjeldende rettslig adgang til å innhente og benytte informasjon for etterretnings- og kriminalitetsbekjempende formål er derfor vurdert ut fra de særlige hensynene som gjør seg gjeldende for disse myndighetene. Den rettslige adgangen til å innhente informasjon er derfor betinget av grenser for bruk og rettssikkerhetsgarantier for borgerne.

Behovet for nye, utvidede metoder for etterretning og etterforskning begrunnes ofte med økende alvorlig IKT-kriminalitet, se punkt 7.2 «Tilsiktede IKT-hendelser». De hensynene som underbygger behovet for nye etterretnings- og etterforskningsmetoder, må baseres på et solid empirisk grunnlag. Dette er vesentlig for å kunne vurdere om tiltakene er nødvendige og proporsjonale i et demokratisk samfunn. Det kreves analyser av mulige konsekvenser for samfunnet som helhet, offentlige myndigheter, næringsliv, interesseorganisasjoner og enkeltindivider.

Å trekke opp grensene for E-tjenestens og politiets adgang til å overvåke og etterforske i digital

nåtid og fremtid byr derfor på krevende avveiinger mellom hensynet til kriminalitetsbekjempelse og det å ivareta de grunnleggende verdiene som ligger til grunn for den tilliten som er opparbeidet mellom stat og borger.

21.10.2 Endring i maktbalansen mellom stat og borger

Dersom spekteret av lovlige skjulte etterretnings- og etterforskningsmetoder skal utvides, er dette også en utvidelse av statens makt overfor den enkelte borger. Den enkelte borger fratas dermed deler av sine rettigheter og friheter. Det rokker ved de konstitusjonelle skrankene for statens myndighet til å gripe inn i borgernes rettighetssfære og stiller krav til hvordan utvidede fullmakter kan komme til.

I et større perspektiv handler det om å ta stilling til på hvilken måte de verdiene og prinsippene som demokratiet og samfunnet vårt bygger på, skal være førende for fremtidens samfunn. Politiets og etterretningsmyndighetenes behov må derfor vurderes opp mot rettsstatsverdier og menneskerettigheter, herunder personvern, ytringsfrihet og forsamlingsfrihet. Dette er forpliktelser som følger av både nasjonalt og internasjonalt regelverk, og det er disse verdiene som utgjør kjernen i et velfungerende og sunt samfunn, som kjennetegnes av gjensidig tillit mellom staten og befolkningen.

En rettsstat kjennetegnes av tydelige og presise regler for den innbyrdes fordelingen av makt mellom statens myndigheter og statens adgang til å bruke makt overfor sine borgere. En omfordeling av maktforholdet mellom stat og borger griper derfor inn i sentrale deler av samfunnets bærende prinsipper og verdier.

Medier som er opprettet for å formidle frie ytringer og intern kommunikasjon i grupper, utgjør grunnleggende verdier i et demokrati. Det må derfor utvises varsomhet med å benytte slike medier for etterretningsformål. Inngrep i ytringsfriheten må tilfredsstille kravene til proporsjonalitet og være nødvendige i et demokratisk samfunn.

Risiko for å bryte ned tillitsforholdet mellom befolkningen og staten

I Norge har offentlig sektor i all hovedsak tillit fra borgerne. Se punkt 23.6.3 «Tillit bør være en forutsetning for digitalisering». Om denne tilliten er gjensidig, det vil si om staten har tillit til sine borgere, kan gjenspeiles i hvilke skjulte inngrep i borgernes rettigheter staten anser som nødvendige. Beslutninger om nye skjulte etterretnings- og etterforskningsmetoder kan derfor også tolkes som statens manglende tillit til befolkningen.

Snowdens avdekking av NSAs omfattende innhenting av informasjon om egne og andre lands borgere illustrerer viktigheten av en balanse mellom nasjonal sikkerhet og den enkeltes personvern. For deler av befolkningen har tilliten til myndighetenes respekt for personvern slått sprekker. Saken sier også mye om den tilliten befolkningen i utgangspunktet hadde til både næringsliv og myndigheter. Uten befolkningens tillit ville informasjonen ikke vært like tilgjengelig. Saken har ført til at stadig flere ønsker å beskytte sin egen informasjon når de benytter Internett. De benytter nettsteder som gjør det vanskelig å spore dem, velger å kryptere sin informasjon, eller begge deler. Det tar lang tid å bygge opp tillit, men kort tid å bryte den ned. Tillit mellom myndigheter og befolkning er særlig viktig og må tillegges betydelig vekt.

21.10.3 Masseinnsamling av personopplysninger til uavklarte formål

Både for næringsutvikling og etterretningsformål er opplysninger om befolkning og enkeltindivider essensielt. I 2012 uttalte Datatilsynet at hele 90 prosent av dagens digitale data er generert bare i løpet av de to siste årene, og at datamengden er antatt å øke med 40 prosent per år fremover. Næringslivets og myndighetenes formål med å samle inn personopplysninger er basert på vidt forskjellige behov. Det er derfor viktig å se nærmere på endringer i hvordan personopplysninger blir samlet inn på, herunder hvilke formål som begrunner innsamlingen.

I Norge har staten frem til relativt nylig vært ansett for å besitte flest opplysninger om borgerne, for å kunne treffe nødvendige beslutninger i egenskap av å forvalte lovbestemt myndighet. Dette bildet er endret til at også aktører i næringslivet er store informasjonsforvaltere av befolkningens opplysninger. For NSAs overvåking av amerikanere og andre lands befolkning var nettopp de private selskapenes informasjon attraktiv for myndighetene.

Det er forståelig at det økende omfanget av informasjon om borgerne hos næringslivsaktører også kan ha nytteverdi for myndighetenes etterretning og for etterforskning av alvorlig kriminalitet. Å åpne for en slik bruk byr imidlertid på mange dilemmaer.

Mens staten har rettsregler for å kunne innhente nødvendig informasjon for spesifikke formål, har næringslivet tilbudt «gratistjenester» med brukervennlige, nyttige og underholdende produkter som grunnlag for å samle inn informasjon. Mens staten er underlagt særskilte krav om å begrense informasjonen til et nødvendig minimum og for konkrete definerte formål, er næringslivets innsamling og lagring ikke underlagt de samme strenge kravene.

Det rettslige grunnlaget for de næringsdrivendes innsamling av personopplysninger er «avtaler» med den enkelte kunde. Da er det rekkevidden av avtalen som setter grensen, og det er tvilsomt om kundene i realiteten har et forhandlingsrom, spesielt når tjenestene tilbys gratis. Forbrukerrådet peker på at majoriteten av forbrukere ofte ikke har forstått betydningen av at de betaler for «gratistjenestene» med opplysninger om seg selv. En uklar avtale om bruken av innsamlet informasjon innebærer tilsvarende utydelige formål, som i neste omgang kan føre til en tilnærmelsesvis grenseløs bruk. Bruk av personopplysninger som er innhentet gjennom avtaler med kunder/brukere der formålet er å tilby en mulighet for å velge tjenester, gir ikke rettslig grunnlag for å benytte opplysningene til etterretnings- og etterforskningsformål.

Næringslivets informasjon er basert på opplysninger om det enkelte individ ut fra aktiviteter og bevegelser som etterlater spor på Internett, som applikasjoner, sosiale medier og e-post. Slike opplysninger omfatter enhver Internett-basert aktivitet – som hvilke søk vi gjør, hvilke annonser vi klikker på, hvilke nettsider vi besøker, hvilke nyhetsartikler vi leser, hva slags musikk vi hører på, hvem vi kommuniserer med, kommentarer vi legger igjen, og hvem vi er i kontakt med per mobiltelefon, herunder når og hvor vi befinner oss. Enkeltvis forteller slike opplysninger lite om oss, men summen av det vi benytter Internett og mobiltjenester til i privat sammenheng, vil kunne gi relativt utførlig informasjon om oss som enkeltindivider.

En tilsvarende kartlegging av aktivitet for å belyse de samme forholdene uten bruk av Internett-baserte tjenester, ville i praksis ikke være mulig for så store deler av befolkningen. Både mengden av informasjon hver og en etterlater seg, og endringen i hvem som samler inn opplysningene, representerer et paradigmeskifte for innsamling og bruk av personopplysninger. Spørsmålet er hva disse omfattende mengdene personopplysninger skal kunne benyttes til, og hvilke formål denne informasjonen skal kunne betjene.

Den teknologiske utviklingen gir nye muligheter for gjenbruk av informasjon til nye formål, såkalt sekundærbruk. Hvilket formål personopplysningene opprinnelig ble samlet inn for, definerer imidlertid en viktig grense for sekundærbruk. Derfor må det vurderes om sekundærbruken er forenlig med det opprinnelige formålet. Da skal det blant annet legges vekt på om det nye bruksområdet for opplysningene skiller seg vesentlig fra det som lå til grunn for den opprinnelige innsamlingen, og om ny bruk av opplysningene kan innebære ulemper for den registrerte. Kravet om at opplysningene skal være *nødvendige* for det formålet de skal tjene, omfatter både at det skal være et minimum av opplysninger, og at opplysningene er relevante for formålet. Dette nødvendighetsprinsippet gjelder for alle deler av håndteringen av personopplysninger, så som hvilke opplysninger som kan registreres, hvem som skal få tilgang til opplysningene, og hvor lenge opplysningene kan lagres. Et eksempel på denne problemstillingen er omtalt i punkt 11.7.5 «Etablere tiltak for å regulere utlevering av trafikkdata til politiet».

Formålsutglidning kan føre til usikkerhet hos brukeren på grunn av mangel på kontroll og oversikt. Dersom opplysninger stadig brukes til andre formål enn det man oppgir, vil det kunne føre til at brukeren mister tillit til det aktuelle mediet og den behandlingsansvarlige.

21.10.4 Balansen mellom effektivitet og sikkerhet

IKT som verktøy kan være et tveegget sverd – den samme effektiviteten som er gunstig for samfunnsutviklingen, kan være tilsvarende effektiv for kriminell aktivitet. Behovet for sikkerhet og aksept av risiko er høyst forskjellig for de ulike brukerne av Internett. Samtlige brukere forventer at informasjonen videreformidles rettidig og til rett mottaker, og at de selv har kontroll over hvilken informasjon som skal deles, og hvilken informasjon som skal beskyttes mot innsyn fra uvedkommende. Informasjonen som skal beskyttes, kan gjelde ivaretakelse av offentlige virksomheters graderte og taushetsbelagte informasjon, næringslivets forretningshemmeligheter eller befolkningens private opplysninger. Samtlige aktørers behov for å ha kontroll over informasjonen er legitime.

Effektive overvåkingstiltak for å avdekke IKT-hendelser kan være varsling ved bruk av sensorer eller logganalyse. Slike tiltak kan være avgjørende for avdekking av angrep og for en samlet risikovurdering. De fleste av disse tiltakene har

kontrollerende, etterforsknings- eller overvåkingslignende karakter rettet mot enkeltindivider, men da uten de prosessuelle rettssikkerhetsgarantiene som følger av straffeprosessloven.

Uttalte behov for å etablere nye etterretnings- og etterforskningsmetoder må også ses i lys av årsakene til økt risiko for alvorlig IKT-kriminalitet. Det er et akseptert syn at økt risiko for alvorlige hendelser og kriminalitet ofte skyldes manglende vektlegging av forebyggende IKT-sikkerhet. Det bør vurderes om også det motsatte er tilfelle – at økt innsats på forebyggende sikkerhet også kan bekjempe og forebygge kriminalitet. Den økende kompleksiteten i sammenkobling av nettverk og programvare kombinert med stadig økende anvendelsesområder for IKT, eksponerer samfunnet for økende grad av sårbarhet og nye muligheter for angrep.

Når det legges til rette for økt tilknytning til og bruk av Internett, bør det fokuseres på sikkerhetstiltak som reduserer risikoen for alvorlige angrep og kriminalitet. Bruk av Internett som kommunikasjonskanal innebærer aksept av en vesentlig risiko. Innebygd sikkerhet og innebygd personvern må vurderes som risikoreduserende tiltak, og det kan i noen tilfeller redusere nødvendigheten av overvåking.

21.10.5 Balansen mellom kriminalitetsbekjempelse og personvern

Retten til personvern er ikke absolutt og må ses i sammenheng med statens øvrige legitime interesser. Hensynet til nasjonal sikkerhet, offentlig trygghet og bekjempelse av alvorlig kriminalitet kan tilsi at det må gjøres inngrep i den enkeltes rett til personvern. Slike inngrep må være lovfestede, nødvendige og proporsjonale, jf. kapittel 3 «Rettsstatsprinsipper og grunnleggende samfunnsverdier». Proporsjonalitetsprinsippet tilsier at det må skilles mellom hvilke metoder som kan brukes i etterforskning av en konkret sak rettet mot enkeltpersoner, og såkalt strategisk kriminaletterretning med generell innhenting og analyse av informasjon med det formål å vurdere kriminalitetsbildet og en sannsynlig utvikling. Etterforskning av konkrete hendelser kan derfor rettferdiggjøre et større inngrep i den enkeltes rett til personvern enn overvåking av befolkningens kommunikasjon generelt, herunder alminnelig meningsutveksling.

Både metodekontrollutvalgets vurderinger og forarbeidene til politiregisterloven[37] er egnet til å vise balansering og ivaretakelse av motstridende hensyn. Politiregisterloven regulerer politiets adgang til å behandle opplysninger og bygger på en avveiing mellom hensynet til personvern og rettsikkerhet og behovet for kriminalitetsbekjempelse. Lovens formål er å regulere politiets bruk av personopplysninger på en måte som også ivaretar personvernet. Det er politiets oppgaver og myndighet knyttet til kriminalitetsbekjempelse som begrunnet behovet for en særlov for politiets behandling av opplysninger.

Politiets behandling av personopplysninger skiller seg fra annen behandling av personopplysninger etter personopplysningsloven på flere måter. Det er ikke krav til samtykke fra den registrerte om at politiet kan behandle opplysninger om en. Politiets myndighet til å innhente opplysninger om borgerne er et inngrep som krever hjemmel i lov. Jo mer inngripende en behandling er, jo strengere krav stilles det til presise lovhjemler.

Politiregisterloven bygger på sentrale personvernprinsipper om formålsbestemthet, nødvendighet og kvalitet. I de tilfellene hensynet til kriminalitetsbekjempelse griper inn i den enkeltes rettigheter, kompenseres inngrepet i enkelte rettigheter ved at andre rettigheter styrkes, for eksempel gjennom å begrense adgangen til å behandle opplysningene videre.

Loven gir for eksempel et tidsbestemt unntak fra kravene til formålsbestemthet, nødvendighet og relevans. Unntaket er begrunnet ut fra hensynet til politiets behov for omfattende tilgang til informasjon i det kriminalitetsbekjempende arbeidet. Det ligger i selve etterforskningens funksjon at politiet er avhengig av å kunne innhente opplysninger uten nødvendigvis å vite om de er nødvendige og relevante. For å ivareta hensynet til personvern ble det innført en tidsbegrensning for unntaket, slik at politiet har fire måneder på seg til å kontrollere om opplysningene er nødvendige og relevante for et politimessig formål. Dersom politiet innen denne fristen ikke kan godtgjøre at opplysningene er nødvendige, må opplysningene slettes. Det tidsbegrensede unntaket fra de grunnleggende kravene til behandling av personopplysninger etter personopplysningsloven er et eksempel på balanseringen av hensynet til kriminalitetsbekjempelse og hensynet til personvernet.

Samtidig er det et faktum at kriminalitetsbekjempelse foretas i en virkelighet der teknologien endrer seg fort. En konsekvens av dette er at de

[37] Justis- og beredskapsdepartementet (2010): *Lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven)*.

som forestår kriminalitetsbekjempelse, må vurdere om virkemidlene deres er tilstrekkelige, og om det trengs endringer i virkemidlene. Ett eksempel på at man ber om endrede virkemidler er da PST ønsket en lovendring slik at de skulle kunne «følge med på Internett», for eksempel ved å lagre informasjon fra sosiale medier og bruke såkalt stordataanalyse på opplysningene. Overvåking av Internett, rettet mot borgere som ikke gjør annet enn å benytte seg av ytringsfriheten og handlingsfriheten, uten mistanke om kriminelle handlinger eller hensikt, kommer potensielt i konflikt med grunnleggende rettssikkerhetshensyn og menneskerettigheter. Dersom slike virkemidler skal kunne tas i bruk, må det foretas tilstrekkelige vurderinger, slik at lovgiver har et grundig, troverdig og fullstendig grunnlag for sine beslutninger, se nærmere om dette i punkt 21.11.8 «Sikre balansen mellom personvern og et sikrere samfunn».

Utvidelser av kriminalitetsbekjempende metoder angår både samfunnet som helhet og det enkelte individ. Dette krever etter utvalgets syn mer enn et vanlig lovendringsarbeid. Det må sikres at denne formen for endringer i maktutøvelse fra staten overfor borgerne utredes av et balansert utvalg som kan stille de kritiske spørsmålene. Det må sikres at hensyn utover myndighetenes egne blir ivaretatt på en forsvarlig måte, og at det skapes en offentlig debatt.

Videre er det behov for ytterligere evaluering av eksisterende metoder som videreføre og utdyper Metodekontrollutvalgets undersøkelse *Kommunikasjonskontroll og betydning for etterforskning, personvern og rettssikkerhet: En studie i erfaringene med bruk av metoden*.[38]

21.11 Vurderinger og tiltak

21.11.1 Etablere og øve et helhetlig rammeverk for digital hendelseshåndtering

Offentlige og private virksomheter blir utsatt for alvorlige dataangrep og opplever usikkerhet og utilstrekkelig koordinering mellom myndighetsaktører som har ansvar for bekjempelsen av digitale angrep. Utvalget har merket seg at det oppleves flere større hindre for effektivt samarbeid mellom myndighetsaktører og med private aktører. Enkelte av disse er inherente problemstillinger, det vil si at problemstillingene i seg selv skaper utfordringer på grunn av motstridende hensyn. Disse skyldes ikke organisering – det kan være kulturelle, tillitsrelaterte eller lovmessige årsaker til at problemstillingene har oppstått. Det kan se ut som det er en manglende forståelse for at motstridende interesser aktørene imellom er legitime. Det stammer fra at aktørene har forskjellige roller og er satt til å ivareta forskjellige samfunnsinteresser. *Utvalget mener det er viktig å maksimere mulighetene innenfor det handlingsrommet som finnes for deling av informasjon.*

Virksomhetene har behov for hyppige oppdateringer av trusselbildet i Norge knyttet til det digitale rom. Flere gode tiltak er påpekt i tidligere utredninger, og utfordringen ser derfor ikke ut til å være intensjonen og målsettingen om samarbeid. Utvalget stiller derfor spørsmål om hva som er årsakene til at aktørene ikke har etablert et tilstrekkelig samarbeid og mekanismer for informasjonsdeling, og ser potensialet for at økt deling av informasjon vil kunne bidra til eksempelvis større grad av anmeldelser. Nasjonal sikkerhet avhenger av sikkerheten til de enkelte virksomhetene, og en effektiv bekjempelse krever utstrakt samarbeid mellom myndighetene og tett samarbeid med private aktører. *Utvalget mener det er avgjørende å ta tak i disse utfordringene nå, ettersom konsekvensene av mangelfull samhandling vil bli enda tydeligere når sikkerhetsutfordringene øker.*

Utvalget mener at Justis- og beredskapsdepartementet må ta initiativ til å etablere et helhetlig rammeverk[39] *for å avklare og tydeliggjøre innsatsen mellom relevante aktører innen hendelseshåndtering og straffeforfølgning.* Rammeverket bør etableres i tett samarbeid med Forsvarsdepartementet. Etter at rammeverket er besluttet, bør det øves på nasjonalt plan.

Et helhetlig rammeverk for digital hendelseshåndtering må inneholde en presis beskrivelse av relevante myndighets- og virksomhetsaktørers roller og ansvar, samt grensesnittene mellom disse. Der det eventuelt er ønskelig med overlapp, må dette komme tydelig frem i rutiner, og aktørene må ha en felles overordnet prosess. Samarbeid mot det private vil være av avgjørende betydning, og overgangen fra hendelseshåndtering ved en nasjonal krise til en krigslignende tilstand bør beskrives. Ulike aktører har ulikt begrepsapparat, og utvalget anbefaler at rammeverket tydelig defi-

[38] NOU 2009: 15 *Skjult informasjon – åpen kontroll. Metodekontrollutvalgets evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker.*

[39] Med rammeverk henvises det her til konsepter land som blant annet USA har etablert (National Cyber Incident Response Plan (NCIRP)).

nerer et enhetlig begrepsapparat. Eksempelvis er det ikke en omforent forståelse av begrepene *digitale angrep*, *operasjoner* og *IKT-kriminalitet*, slik de hittil er definert. Det samme gjelder *hendelseshåndtering*, som har ulik betydning hos de forskjellige aktørene. *Rammeverket må revideres og harmoniseres opp mot nasjonalt beredskapsplanverk. Blant annet gjelder dette harmonisering av eskaleringsnivåer, som må defineres og ses i sammenheng med det øvrige planverket.*

Ambisjonsnivået til myndighetene

Myndighetenes ambisjonsnivå rundt operativ støtte ved IKT-angrep må fremover være tydelig definert og kommunisert, slik at sektorvise responsmiljøer, offentlige og private virksomheter kan ha en avklart forventning om hva som er deres grensesnitt og bistandsmulighet. *Utvalget mener Norge innen et femårsperspektiv effektivt må evne å håndtere en nasjonal cyberkrise.* Myndighetene må dimensjonere evnen og kapasiteten med en ambisjon om å kunne avdekke og håndtere alvorlige hendelser på en måte som sikrer befolkningens trygghet for liv, helse og viktige verdier.

Utvalget anbefaler følgende ambisjonsnivå for myndighetenes operative evne til å avdekke, håndtere og etterforske alvorlige hendelser:

1. Norske virksomheter må ha evne til grunnleggende egenbeskyttelse, avdekking og håndtering i henhold til ansvarsprinsippet, slik at de er i stand til å fylle sin rolle slik det er definert i rammeverket.
2. Myndighetene skal opplyse befolkningen om relevante sårbarheter og trusler og legge til rette for at borgere og virksomheter som opplever digitale angrep mot sine verdier, har et sted å søke råd.
3. Myndighetene må legge til rette for at virksomheter settes i stand til å ta gode risikoavveide, strategiske og operative beslutninger gjennom aktivt å dele betimelig informasjon. Deling må skje tidlig i håndteringsskjeden.
4. Norge skal ha evne til å avdekke alvorlige IKT-hendelser i virksomheter som har ansvar for kritiske samfunnsfunksjoner.
5. Myndighetene skal være i stand til å bistå virksomheter med koordinering av hendelseshåndtering og analyse der skadepotensialet er alvorlig for norske interesser og for samfunnet.
6. Myndighetene skal ha rask reaksjonsevne og kunne skalere sin kapasitet både i normalsituasjoner, ved ekstraordinære hendelser og i nasjonale kriser. For å skalere kapasiteten bør en blant annet benytte kommersielle aktører.
7. Norges innsats mot IKT-kriminalitet skal være blant Europas fremste. Norsk politi skal bidra aktivt i internasjonalt etterforsknings- og irettesettelsessamarbeid. De som utøver IKT-kriminalitet, skal ikke kunne forberede eller gjennomføre kriminelle handlinger uten betydelig risiko for å bli oppdaget og straffeforfulgt.
8. Myndighetenes operative miljøer skal ha klart definerte roller og ansvar og evne å bruke hverandres styrker. Dette må det tilrettelegges for på strategisk nivå.
9. Myndighetene må sørge for at den operative håndteringen av IKT-hendelser har metoder, kildetilgang og øvrige rammebetingelser. Balansen mellom de grunnleggende samfunnsverdiene, som for eksempel ytringsfrihet og personvern, og trusselutviklingen må være godt ivaretatt. Disse vurderingene skal være diskutert og gjort rede for.
10. Myndighetene skal ha et oppdatert og øvd krise- og beredskapssystem som omfatter digitale kriser.
11. Myndighetene skal ha kommunikasjonsløsninger overfor befolkingen som fungerer selv om de utsettes for misbruk og er degradert i visse krisesituasjoner.

21.11.2 Forbedre den nasjonale operative evnen gjennom samlokalisering

Det er flere små operative miljøer i Norge i dag som skal samhandle med hverandre. Flere endringer kan foreslås for at disse bedre kan utnytte hverandres styrker. Et sentralt spørsmål er om Norge, som en liten nasjon, evner å utnytte den samlede nasjonale kapasiteten på området, både på privat og offentlig side. Utvalget observerer at myndighetsorganene i hovedsak oppfatter sin egen rolle som avklart, men at uklarheten ligger hos andre aktører. Utvalget har sett på de styrende dokumentene som foreligger, og opplever at uklarheten i mange tilfeller kan synes å være konstruert. Utvalget observerer også en krasshet i aktørenes omtale av hverandre, og stiller spørsmål om aktørene i tilstrekkelig grad klarer å spille hverandre gode.

Utvalget finner det vanskelig å ha belegg for å si at det er uklare roller, men er bekymret for om samarbeidsklimaet er som det burde være. Inntrykket er at hovedgrunnen til at disse uklarhetene har oppstått, ikke er uavklarte roller og ansvar, men at effekten av eksisterende strukturer ikke er godt nok utnyttet. Utvalget observerer videre at en rekke samfunnsviktige private aktører ikke opplever at dagens samarbeid er basert

på likeverd, men at det offentlige setter premissene. Manglende likeverd oppleves som en svakhet med hensyn til effektiv håndtering av hendelser og rettidig deling av informasjon. Selv om det ofte vil være et naturlig spenningsfelt mellom rikets sikkerhet og et militært etterretningsfokus når det gjelder deling av informasjon og samfunnets øvrige behov, mener utvalget at det ligger et viktig mulighetsrom her.

Utvalgets vurdering er at aktørene i langt større grad bør dele informasjon fra åpne kilder og lovlig delbar informasjon. Utvalget mener videre at samlokalisering kan være et sentralt virkemiddel for å sikre dette. Utvalget foreslår at det legges bygningsmessig til rette for at de som ønsker samlokalisering, kan gå sammen om ett felles bygg. Dette må imidlertid ikke være et premiss for å delta i samhandlingen. Samlokalisering må bygge på frivillighet og være egnet for stor grad av liaisonering for dem som av ulike årsaker ikke har mulighet for eller ønsker full samlokalisering.

Samlokalisering vil kunne bidra til felles forståelse av det operative landskapet og arbeidsmetodene, og mer effektiv informasjonsdeling der dette er mangelvare. Det vil kunne bli en «hub» mellom privat og offentlig sektor for samarbeid og informasjonsdeling for å motvirke cybersikkerhetstrusler. De enkelte enhetene, som er en del av samlokaliseringen, er finansiert fra eksisterende virksomhetsressurser. Ved å samle ressursene for hendelseshåndtering og teknisk analyse kan man oppnå stordriftsfordeler i saker som egner seg for samarbeid, i tillegg til å få kompetansemiljøer som er robuste nok til å vedlikeholde og videreutvikle kapasitetene. Bedre samarbeid kan bidra til mer helhetlig analyse og etterforskning av digitale trusler.

NSM NorCERT har i dag rollen som den nasjonale CERT-funksjonen. Det innebærer at NSM NorCERT er nasjonalt IKT-responsmiljø og koordinerer håndteringen av alvorlige IKT-hendelser rettet mot samfunnskritisk infrastruktur og informasjon. Dette medfører også et ansvar for å detektere hendelser, koordinere og bistå i hendelseshåndteringen, foreta tekniske analyser, dele informasjon og gi råd på overordnet nivå og på tvers av sektorgrenser. Samarbeidet med de øvrige EOS-tjenestene vurderes som særlig viktig for evnen til informasjonsinnhenting, varsling og håndtering av alvorlige digitale trusler. Spesielt gjelder dette samarbeidet med Etterretningstjenesten, som også er nasjonal SIGINT-autoritet. I tillegg til egne innsamlingsressurser er det denne posisjonen som gir eksklusiv aksess til partnermateriale som Norge er avhengig av for å håndtere det digitale trusselbildet.

På dette punktet har utvalget delt seg.

Flertallet, bestående av Olav Lysne, Fredrik Manne, Eva Jarbekk, Kristian Gjøsteen, Einar Lunde, Janne Hagen og Åke Holmgren fremmer følgende:

Ved bruk av samlokalisering som virkemiddel for å forbedre samarbeidet aktørene imellom og lage en arena for rettidig hendelseshåndtering, er det etter utvalgets mening mest rasjonelt å ta utgangspunkt i det miljøet som både har en tradisjon for offentlig–privat samarbeid, og er en del av EOS-miljøet. I tillegg vurderes det som sannsynlig at å forankre en samlokalisering i EOS-miljøet er et premiss for at EOS-tjenestene er med, noe som vurderes helt nødvendig for etablering av ett nasjonalt miljø. *Utvalget konkluderer derfor med at den mest naturlige verten for en samlokalisering er NSM NorCERT.* I denne rollen som vert er det viktig at NSM er seg bevisst toveiskommunikasjon og likeverdig behandling av sivile aktører. *Justis- og beredskapsdepartementet må følge opp, særlig overfor de sivile aktørene i samarbeidet, og definere klare, målbare suksesskriterier for samarbeidet, som skal evalueres innen henholdsvis to og fem år.* Basisen for kriteriene er ambisjonsnivået, slik det er beskrevet tidligere i kapittelet.

Mindretallet, bestående av Kristine Beitland og Sofie Nystrøm, fremmer følgende:

Utvalgsmedlemmene Kristine Beitland og Sofie Nystrøm anbefaler at Justis- og beredskapsdepartementet i politikkutformingen vurderer et mer ambisiøst forslag hva gjelder det å forbedre den nasjonale operative evnen gjennom samlokalisering. De to utvalgsmedlemmene understreker at departementet bør søke å etablere en styringsstruktur for det operative arbeidet som prinsipielt følger roller og ansvar implementert rundt våre fysiske verdier, og som videreføres inn i det digitale rom.[40]

Det er et naturlig spenningsfelt mellom på den ene siden rikets sikkerhet og vektlegging av militær etterretning med stor grad av gradert informasjon og delingsbegrensninger, og på den andre siden samfunnets behov for åpenhet og informa-

[40] Styringsprinsipp fra myndighetene i Nederland: «The underlying fundamental principle is that the responsibilities that apply in the physical domain should also be taken in the digital domain.»

sjonsdeling sett fra et sivilt samfunnsperspektiv. For Norge er det viktig å ha operativ kapasitet og reaksjonsevne i begge spor, idet et digitalt angrep kan være avsluttet i løpet av minutter eller timer og ramme flere sektorer samtidig. Internasjonalt er det vanskelig å peke på gode eksempler fra andre land som har lyktes med å etablere et effektivt samarbeid og informasjonsdeling på tvers av et etterretningsspor og et samfunnssikkerhetsspor i én og samme organisasjon.

De to utvalgsmedlemmene foreslår en betydelig styrking av samfunnets samlede evne til hendelseshåndtering og etterforskning av digitale angrep for å nå det foreslåtte ambisjonsnivået som er beskrevet i punkt 21.11.1 «Etablere og øve et helhetlig rammeverk for digital hendelseshåndtering». For å øke den samlede nasjonale kapasiteten på håndtering av hendelser er det viktig å fokusere på et tettere tverrsektorielt privat–offentlig samarbeid. Det er en oppfatning at NSM NorCERT i dag først og fremst er opptatt av og prioriterer koordinering av hendelseshåndtering og samarbeid mellom myndighetene.[41] Dette gjør de i tett samarbeid med de andre EOS-tjenestene. Justis- og beredskapsdepartementet og Forsvarsdepartementet bør i samråd, på kort sikt, evaluere hvordan NSM NorCERT forvalter rollen som den nasjonale CERT-funksjonen ut fra et samfunnssikkerhetsspor med vekt på tillit, samarbeid og rask informasjonsdeling fra og til virksomheter med samfunnskritiske funksjoner.

I tillegg bør Justis- og beredskapsdepartementet og Forsvarsdepartementet i samråd etablere en pilot (første fase 1–2 år) som inkluderer noen av liaison-ressursene til politiets nye nasjonale enhet «Cyber Crime Center», se punkt 21.11.5 «Etablere et nasjonalt «Cyber Crime Center». Denne samlede nasjonale operative kapasiteten bør fysisk samlokaliseres i ett felles bygg med det eksisterende EOS-miljøet/etterretningssporet. Det bør også legges til rette for at samlokaliseringen omfatter liaisoner fra sektorvise responsmiljøer og sertifiserte leverandører[42]. Det privat–offentlige samarbeidet må bygge på frivillighet. Det bør også dimensjoneres bygningsmasse for at sentrale offentlige og private virksomheter med kritiske samfunnsfunksjoner kan inngå i dette fagmiljøet, enten regelmessig eller ved alvorlige hendelser.

I andre fase (2–4 år) bør Justis- og beredskapsdepartementet legge til rette for et ytterligere samarbeid mellom de sektorvise responsmiljøene, sertifiserte leverandører og akademia. Det anbefales at politiet, ved Kripos' nye nasjonale «Cyber Crime Center», gis i oppdrag å etablere et nasjonalt cybersikkerhetssenter.[43] Det er i dette forslaget lagt vekt på viktigheten av at et cybersikkerhetssenter etableres med et samfunnssikkerhetsperspektiv med likeverdig samarbeid mellom offentlig og privat sektor, der en evner å dele kunnskap og utnytte hverandres styrker. En del av senteret bør ha et særskilt ansvar for koordinering med de hemmelige tjenestene. Cybersikkerhetssenteret skal fungere som et felles kontaktpunkt til hjelp ved hendelser. I tillegg bør senteret ha ansvar for å gjennomføre flere årlige nasjonale cybersikkerhetsøvelser.[44]

Politiet har en helt sentral rolle i samfunnssikkerhetssporet. Forebygging av kriminalitet er en av politiets mest sentrale samfunnsoppgaver, sammen med etterforskningsansvaret og et sektorovergripende ansvar for å håndtere ulykker og katastrofer i fred, på alle samfunnsområder. Nærpolitireformen, som reduserer antall politidistrikter fra dagens 27 til 12, vil innebære en kompetanse- og kapasitetsmessig kraftsamling, noe som vil kunne skalere politiets innsats på området. I politiets forebyggende arbeid er det allerede etablert en landsdekkende struktur for et mer operativt privat–offentlig samarbeid gjennom næringslivskontakter i flere politidistrikter. Dette gjør at politiet er særlig egnet som vert og leder av et cybersikkerhetssenter der det totale samfunnssikkerhetsperspektivet forsterker det privat–offentlige samarbeidet basert på likeverd. Politiet har således et helhetlig ansvar på området som omfatter å forebygge, avdekke og stanse kriminell virksomhet, forfølge straffbare forhold og håndtere hendelser ved en krise.

21.11.3 Øke deteksjonsevnen og sammenstille et felles situasjonsbilde

For effektiv avdekking av digitale angrep trengs det gode deteksjonsmekanismer som dekker de kanalene angrepene gjennomføres gjennom. Dette innebærer mer enn teknologiske tiltak. Ressursgruppen har stilt spørsmål ved om det kan

[41] Internasjonalt ofte omtalt som govCERT-funksjon.

[42] Leverandører som har møtt visse kriterier satt opp av myndighetene, som kan bistå med å rydde opp etter IKT-sikkerhetshendelser etter modell fra Storbritannia og «CIR»-sertifisering.

[43] Begrepet *cybersikkerhetssenter* i stedet for *IKT-sikkerhetssenter* blir her brukt for å være sammenlignbart med andre lands oppbygging av slike sentre, for eksempel i Nederland og Finland.

[44] Nederland avholdt tre nasjonale cybersikkerhetsøvelser i perioden 2007–2014.

være slik at IKT-hendelser ved NSM NorCERT blir sikkerhetsgradert selv om kildene i utgangspunktet er av ugradert karakter. *Informasjonsdeling i forbindelse med hendelser må starte tidligere enn det som er vanlig i dag.* Man bør i større grad løsrive seg fra behovet for forståelse og ferdigstilte rapporter før informasjon deles.

Inntrengingstesting er en viktig del av det forebyggende IKT-sikkerhetsarbeidet, og er primært et virksomhetsansvar. NSM anbefaler i sikkerhetsfaglig råd at Sikkerhetsutvalget bør vurdere om «NSM bør gis hjemmel til å gjennomføre inntrengingstesting uten forutgående samtykke fra virksomheten». Utvalget er prinsipielt uenig i at man bør tillate å gjennomføre inntrengingstesting uten samtykke fra virksomheter. Dette begrunnes med at det kan undergrave tillit, samt sektorenes og virksomhetenes selvstendige ansvar.

Tiltaket omfatter følgende områder:

1. *Aktiv og rettidig informasjonsdeling ved å etablere en hensiktsmessig teknisk plattform*

Utvalget mener NSM NorCERT må etablere en teknisk informasjonsdelingsplattform for ugradert informasjon mot virksomheter for å kunne dele informasjon raskt og sikkert. Dette vil kunne være en viktig tjeneste for et enda tettere privat–offentlig samarbeid. NSM bør måles på gjennomføringen av denne informasjonsdelingen. Dette forutsetter at det er etablert en hensiktsmessig infrastruktur, se tiltak foreslått i kapittel 20 «Styring og kriseledelse».

2. *Styrke deteksjonsevnen gjennom tilpasset monitorering i den enkelte sektor.*

Utvalget ser behovet for en styrket nasjonal evne til å detektere hendelser i det digitale rom. Utvalget er av den oppfatning at lovfesting av VDI-funksjonen er hensiktsmessig i den grad det formaliserer dagens eksisterende ordning. Når det gjelder utplassering av VDI-sensorer, er det viktig å bygge opp sektormyndighetenes ansvarsutøvelse på dette området. *Justis- og beredskapsdepartementet må innta en pådriverrolle overfor sektormyndighetene, slik at sektorene har tilstrekkelige deteksjonsmekanismer.* Teknologien bør være den samme, og driftes av NSM NorCERT. Imidlertid må ansvar for utrulling og beslutning om plassering tilligge sektorene. *Utvalget anbefaler at det etableres en årlig økonomisk ramme, forvaltet av NSM i samarbeid med sektormyndighetene, som kan brukes til spesifikke myndighetspålagte tiltak.* Dette må ses i sammenheng med 21.11.2 «Forbedre den nasjonale operative evnen gjennom samlokalisering», der en forutsetning for virksomhetene er at det blir en tydelig tilbakemelding og verdiøkning tilbake fra NSM NorCERT.

Neste generasjons VDI bør videreutvikles i samarbeid med de sektorvise responsmiljøene for å ivareta sektorenes behov på en god måte. De sektorvise responsmiljøene må ha mulighet til å tilpasse deler av signaturene til sektorens behov. Gjennom dette vil man kunne ivareta både det nasjonale og det sektorvise perspektivet. Utvalget mener dette også vil bidra til større helhetsforståelse og bedre samarbeid. Behovet må ses i sammenheng med punkt 21.11.8 «Sikre balansen mellom personvern og et sikrere samfunn».

3. *Etablere et felles situasjonsbilde og automatisert informasjonsdeling.*

Utvalget mener det bør legges til rette for et felles situasjonsbilde, basert på åpne kilder, som kan deles med sektorvise responsmiljøer og andre relevante aktører. Nasjonal kommunikasjonsmyndighet bør vurdere å etablere en automatisert prosess for å dele informasjon om norske datamaskiner som er brukt i digitale angrep mot norske telekomoperatører. Eventuelle lovmessige implikasjoner må utredes. Det er primært utstyr hos sluttkunder som er målgruppen her. Tiltaket er inspirert av den finske ordningen, der den nasjonale CERT-en har automatisert deling av informasjon til finske ISP-er.

21.11.4 Styrke kapasitet og kompetanse knyttet til håndtering av digitale angrep

Utvalget registrerer at det er kapasitets- og kompetanseutfordringer knyttet til håndtering av digitale angrep. For å sikre rekruttering av relevant kompetanse i fremtiden er det viktig at fagmiljøene har en aktiv rolle overfor akademia. På den måten kan akademia tilføres praktisk erfaring som har verdi for kunnskapsutviklingen, som igjen kan tilbakeføres til de operative kapasitetene.

Tiltaket omfatter følgende områder:

1. *Evaluere ordningen med sektorvise responsmiljøer*

Utvalget mener det er viktig at det støttes opp om etableringen av de sektorvise responsmiljøene. De sektorvise responsmiljøene er imidlertid svært ulike, noe som kan medføre at samarbeid

og koordinering mellom dem fungerer mindre hensiktsmessig. Det er også en utfordring at sektor-CSIRT ikke nødvendigvis favner hele sektoren, og at ikke alle virksomheter har en sterk og naturlig tilhørighet i én sektor. Videre stiller utvalget spørsmål ved om Norge har tilstrekkelig kompetanse til å bemanne flere små miljøer. Utvalget mener at oppbyggingen av sektorvise responsmiljøer har foregått noe ukoordinert, og at Justis- og beredskapsdepartementet var sent ute med å gi retningslinjer for etableringen. *Utvalget mener det er behov for en evaluering av ordningen med sektorvise responsmiljøer sett opp mot det tverrsektorielle behovet for hendelseshåndtering.* Dette bør gjøres i etterkant av Øvelse IKT 2016. Det er en forutsetning at de sektorvise responsmiljøene involveres tett i evalueringen. Gjennom evalueringen bør det blant annet ses på om inndelingen i sektorvise responsmiljøer er hensiktsmessig, eller om responsmiljøer for sektorer med tilsvarende utfordringer bør slås sammen.

2. *Utrede nasjonal cyberreserve for digital hendelseshåndtering*

Utvalget stiller spørsmål om hvilke skaleringsmuligheter som finnes ved større kriser som krever innsats utover ordinær bemanning, samt hvordan man vil kunne nyttiggjøre seg andre miljøer. *Utvalget mener det må etableres en nasjonal cyberreserve for digital hendelseshåndtering.* Målet er å kunne skalere opp innsats ved store hendelser og kriser, for eksempel ved å opprette avtaler med tidligere ansatte fra relevante fagmiljøer. Dette er et forslag Nederland har fremmet, og det er paralleller i Norge med innkalling av ekspertise på andre områder. Storbritannia og Estland har etablert lignende «cyberreserver».

Det daglige virket for dem som inngår i cyberreserven, vil ikke endres. Utvalget erkjenner at det er begrenset levetid på kompetanse, og at det derfor bør ses på hvilke kriterier som skal ligge til grunn for utvelgelse av personell, og hva ambisjonsnivået bør være, knyttet til størrelse på cyberreserven. Utvalget har respekt for at etablering av en cyberreserve har mange komplekse sider som utvalget ikke har beskrevet. Utvalget har som tidligere beskrevet ikke gjort en analyse av Forsvarets kapasiteter, men tiltaket kan være egnet som et område for sivilt–militært samarbeid. *Utvalget mener at et naturlig første steg vil være at Justis- og beredskapsdepartementet og Forsvarsdepartementet utreder hvordan en slik cyberreserve kan bygges opp, driftes og organiseres.*

21.11.5 Etablere et nasjonalt «Cyber Crime Center»

Det er utvalgets oppfatning at Politiets beredskapsevne og oppgaveløsning i det digitale rom er langt fra tilstrekkelig og ikke tilpasset samfunnets forventninger og den risikoen samfunnet står ovenfor. *Utvalget støtter Justis- og beredskapsdepartementet forslag om å opprette et nytt nasjonalt senter for å forebygge og etterforske kompleks og grenseoverskridende IKT-kriminalitet.* Senteret bør ha et utvidet og nasjonalt fagansvar for forebygging og etterforskning av alvorlig og kompleks IKT-kriminalitet med en særskilt bistandsfunksjon for å støtte politidistriktene, både polititaktisk og påtalefaglig. Senteret skal også drive fag- og metodeutvikling. Det er viktig å tydeliggjøre at et slikt særskilt nasjonalt senter alene gis ansvaret for metodeutvikling og håndtering av skjulte digitale metoder. I tillegg bør senteret ha et særskilt nasjonalt ansvar for kunnskaps- og metodeutvikling i samarbeid med PHS og andre kunnskapsmiljøer. Behovet for et spisset nasjonalt fagmiljø vil ha avgjørende betydning for politiets innsats på området, og økt betydning i tiden fremover. Et nasjonalt senter vil også lettere kunne møte et økende krav til nasjonalt og internasjonalt samarbeid. Utvalget presiserer at det ikke foreslås å gi senteret ansvar som per i dag faller inn under PSTs ansvarsområde.

Utvalget mener at senteret ikke bare kan, men skal, etterforske alvorlig IKT-kriminalitet. Det er ønskelig at Riksadvokaten gir klare føringer for hva som ligger i begrepet alvorlig IKT-kriminalitet.

Utvalget vurderer at det ikke er realistisk nå å opprette et slikt senter som et eget særorgan. Dette er begrunnet i at Regjeringen har vedtatt en utredning av fremtidig organisering av særorganene. *Utredningen bør vurdere om kapasitetsoppbyggingen har svart til intensjonen, og om alternative organisasjonsformer er mer hensiktsmessige.*

21.11.6 Sikre sterke fagmiljøer for IKT-kriminalitet i politidistriktene

Digital kompetanse i politiet må bygges i bredden, det vil si i alle politidistrikt. I politidistriktene er det behov for bedre og mer spesialisert kompetanse, ferdigheter og økt kvalitet på politiarbeidet.[45] Alle tjenestemenn og -kvinner trenger økt forståelse for digitalt politiarbeid, herunder å

[45] Justis- og beredskapsdepartementet (2015): *Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet.*

bekjempe IKT-kriminalitet, behandle elektroniske spor, arbeide på Internett, samt generell etterforskningskompetanse når det gjelder IKT-kriminalitet.

PHS' studieprogram innenfor grunnutdanningen og etter- og videreutdanningen må i tilstrekkelig grad vektlegge IKT-kriminalitetsbekjempelse, behandling av elektroniske spor og arbeid på Internett. *Utvalget anbefaler at det gjennomføres et stort løft innenfor etter- og videreutdanning for allerede uteksaminerte tjenestemenn og -kvinner. Utvalget mener også at Justis- og beredskapsdepartementet bør gi klare føringer til politidistriktene for å sikre nødvendig tverrfaglig kompetanse i politiet, herunder sivilt ansatte med teknisk bakgrunn.*

Politidistriktenes fagmiljøer for sikring av elektroniske spor og etterforskning av IKT-kriminalitet er ulike og ofte kritisk små. Organisatoriske endringer som følge av nærpolitireformen og sammenslåingen av politidistrikter og større fagmiljøer vil ikke alene gi den nødvendige kapasiteten politiet trenger for å møte fremtidens IKT-kriminalitetsutfordringer. *Utvalget anbefaler, i tråd med Politidirektoratet, at politidistriktenes fagmiljøer styrkes betraktelig. Ved politiets arbeid på Internett bør den åpne tilstedeværelsen, herunder «politistasjon og patruljering på nett», ligge til det enkelte politidistrikt for å ivareta politiets primæroppgave med å sikre trygghet, lov og orden.*

Utvalget mener at et klart grensesnitt mellom hva et nasjonalt «Cyber Crime Center» håndterer, og hva politidistriktene selv forventes å håndtere, er avgjørende. Politidistriktenes fagmiljøer må være dimensjonert til å håndtere oppgavene sine når det gjelder bekjempelse av IKT-kriminalitet. *Utvalget støtter Justis- og beredskapsdepartementets forslag om at Oslo politidistrikt kan være pilot for en slik satsing.*[46]

Utvalget har vurdert ulike modeller for organisering. PST har i dag en organisasjonsmodell med én sentral enhet og dedikert personell lokalt i distriktene. Ordningen med etablering av tverrfaglige økoteam i samtlige politidistrikter har vært vellykket, og de fleste politidistriktene er i dag i stand til å håndtere også kompliserte økonomiske straffesaker i eget distrikt.[47] I Norge står politidistriktenes autonomi og politimestrenes frihet til å prioritere innenfor egen ramme sterkt. *Utvalget mener denne styringsmodellen ikke må være til hinder for å vurdere ulike modeller for organisering av IKT-kriminalitet, blant annet ved utredningen av den fremtidige organiseringen av særorganene.*

21.11.7 Sikre en IKT-infrastruktur til støtte for politiets kriminalitetsbekjempelse

Utvalget er av den oppfatning at IKT-situasjonen i politiet er kritisk. Det er behov for langsiktige og omfattende løft med tanke på stabilitet i grunnleggende infrastruktur og sikkerhet i applikasjoner og tjeneste. I tillegg er det et stort behov for å etablere felles nasjonale løsninger som erstatning for ulike lokale løsninger. Utvalget ser det som helt grunnleggende for å kunne understøtte en større satsing i politiet mot IKT-kriminalitet. Det er også behov for utvidet funksjonalitet, slik som digitalisering av samhandling mot domstolene, kriminalomsorgen og mot innbyggerne.

Det er ikke funnet grunnlag for å si at dette skyldes manglende investeringer til IKT i politiet. Utvalget merker seg politiets bekymring over IKT-situasjonen og manglende langsiktig satsing ved at Merverdiprogrammet ble besluttet delt opp i mindre prosjekter for å redusere risikoen i IKT-fornyingen i politiet. Utvalgets bekymring knytter seg særlig til to mulige konsekvenser – ineffektivitet i politiarbeidet og uroen for at hele IKT-systemet politiet baserer arbeidet sitt på, ikke har nødvendig robusthet og sikkerhet. Utdaterte IKT-systemer er ikke unikt for justissektoren. Det er imidlertid summen av disse faktorene som gjør IKT-infrastrukturen i politiet særlig sårbar. *Utvalget mener at Justis- og beredskapsdepartementet bør iverksette tiltak for å sikre politiet et teknologiløft, med fokus på IKT-ledelsen og -styringen, øke bestillerkompetansen og gi klare prioriteringer for ressursutnyttelse i et langsiktig perspektiv.*

21.11.8 Sikre balansen mellom personvern og et sikrere samfunn

Utvalget har merket seg at inngripende metoder foreslås for å få et sikrere samfunn, uten at balansen mot personvern og ytringsfrihet er tatt tilstrekkelig stilling til og redegjort for. Slike teknologi- og personvernspørsmål blir i stor grad overlatt til politiske myndigheter. Utvalget fremmer derfor to områder der det må foretas viktige avveininger for å finne den rette balansen mellom motstridende hensyn.

1. *Utrede innføring av digitalt grenseovervåking ved en NOU eller annen offentlig utredning.*

---

[46] Ibid.

[47] Politidirektoratet (2012): *Organisering av økoteamene*. Forankret i regjeringens handlingsplan mot økonomisk kriminalitet (2011) ble økoteamene opprettet i 2005 ved alle politidistrikter som tverrfaglige team for å behandle komplekse økonomiske straffesaker.

Utvalget registrerer at det oppgis at noen land vi gjerne sammenligner oss med, har digital grenseovervåking, og forstår det etterretningsfaglige behovet for å vurdere innføring også i Norge.[48] *Utvalget er imidlertid av den oppfatning at digital grenseovervåking ikke bør innføres uten en forutgående offentlig debatt. Denne debatten bør forberedes gjennom en Norsk offentlig utredning (NOU) eller et tilsvarende utredningsdokument. På den måten vil man sikre at virkemiddelet blir diskutert i større bredde enn det dette utvalget har hatt anledning til å gjøre.* Vi foreslår derfor at det settes ned et eget utredningsutvalg med et mandat som inkluderer at utvalget skal

- ha en presis formulering av formålet med innsamlingen og tilgang til bruk av data
- vurdere implementasjonsmetoder for å nå dette målet
- utrede hvilke tilleggsgevinster man får av digital grenseovervåking, sammenlignet med de overvåkingstiltakene som allerede er iverksatt i regi av NSM NorCERT og andre CERT/CSIRT-er og sensorsystemer, og den tilgangen til informasjon som EOS-tjenestene i dag har fra andre kilder
- vurdere den teknologiske realismen i disse tilleggsgevinstene
- vurdere alternative tilnærminger til å oppnå de samme gevinstene
- vurdere forholdsmessigheten i disse tilleggsgevinstene i relasjon til hvor inngripende de er i forhold til personvern og menneskerettigheter
- vurdere mulige konsekvenser for individer, næringsvirksomhet og nasjonal sikkerhet dersom utenforstående skulle ta kontroll over overvåkingsutstyret og/eller få innsyn i data
- vurdere proaktive tiltak for å hindre fremtidig formålsutglidning, og slik sikre at innsamlede data og tekniske installasjoner tilknyttet digital grenseovervåking ikke benyttes til andre formål enn de som er forutsatt.

Deltagerne i dette utvalget må ha en erfaringsbase som gjør at hensyn til etterretningsbehov, teknologisk kompetanse og personvernhensyn ivaretas, og at man sikres en grundig redegjørelse for de teknologiske, rettslige og samfunnsmessige spørsmålene saken reiser.

2. *Utrede politiet og PSTs skjulte metodebruk på Internett.*

Utvalget legger til grunn at politiet og PST i lys av den digitale utviklingen har behov for å være aktivt til stede i det digitale rom, med både åpen og skjult tilstedeværelse på Internett. Den åpne tilstedeværelsen til politiet er uproblematisk og en forutsetning for et effektivt og moderne politi. Den skjulte tilstedeværelsen reiser grunnleggende verdispørsmål om balansen mellom samfunnets behov for å bekjempe IKT-kriminalitet med alle midler og grunnleggende samfunnsverdier som menneskerettigheter, personvern, rettssikkerhet og ytringsfrihet. Metodebehovet reiser også spørsmål knyttet til utvikling og utøvelse av etterforskningsmetoder, som søkemetodikk, opptreden på et «digitalt åsted», politiets egen sikkerhet og eksponering, samt mer komplekse spørsmål knyttet til skjult innsamling av informasjon.

Utvalget mener at Justis- og beredskapsdepartementet bør sette rammene for utviklingen av justissektorens skjulte digitale metoder. Dersom PST igjen reiser forslag om å registrere ytringer på sosiale medier og analysere informasjon fra åpne kanaler, mener utvalget at det er et særskilt behov for en full offentlig utredning. De hensynene som må ligge til grunn for beslutningen om hvorvidt vi skal overvåke sosiale medier, vil ha mye til felles med de hensynene som ligger til grunn for grenseovervåking.

[48] Utvalget har mottatt utdypende beskrivelser knyttet til det etterretningsfaglige behovet fra Etterretningstjenesten.

Kapittel 22
Felleskomponenter

I offentlig sektor finnes det funksjoner som det er naturlig å sentralisere. Folkeregisteret er ett eksempel. Når Norge først har valgt å registrere alle innbyggerne, er det mest naturlig å ha ett sentralt register. Det finnes også andre funksjoner som man kan velge å sentralisere. Matrikkelen (se punkt 22.4.1) hos Kartverket er et eksempel på en funksjon samfunnet har valgt å sentralisere, men som kunne ligget for eksempel hos kommunene.

Digitalisering kan også forårsake sentralisering der sentralisering ville gitt liten eller ingen mening i en analog verden. Et eksempel er Altinn, som kan håndtere kommunikasjon mellom offentlige virksomheter og borgere og private virksomheter. Altinn gjør det lettere for offentlig sektor å kommunisere digitalt med brukerne.

Sentralisering kan eliminere dobbeltarbeid. Når offentlige virksomheter kan gjenbruke Altinns funksjonalitet for innsending av skjemaer, slipper hver offentlig virksomhet å utvikle denne funksjonaliteten. En annen fordel er at et godt sikkerhetsarbeid hos fellesfunksjonen automatisk kommer alle virksomheter til gode.

Samtidig kan sentralisering påvirke sikkerhetsnivået negativt. Først av alt blir mange virksomheter avhengige av fellesfunksjonene, av og til uten at de er klar over det. Dersom en fellesfunksjon har for dårlig sikkerhet, kan det være vanskelig for enkeltvirksomheter å lage sin egen variant med høyere sikkerhet, selv om de reelt sett har behov for det.

Sårbarheter i fellesfunksjoner vil dermed ha særlig store konsekvenser. Derfor er det viktig at vi har et overordnet grep om disse sårbarhetene, at de som eier felleskomponentene, forstår hvilke samfunnsverdier som hviler på dem, og at de som bruker felleskomponentene, forstår hvilke sårbarheter de arver.

Felles infrastruktur for e-ID er særlig viktig for kommunikasjon mellom offentlige virksomheter og borgerne. Samtidig er dette et krevende felt der vi i nær fremtid ikke kan forvente at tekniske løsninger har svært høy sikkerhet. Det betyr at det er særskilt viktig å håndtere den arvede sårbarheten.

Mange felleskomponenter innebærer lagring av informasjon. Utfordringene knyttet til lagring av informasjon er stort sett de samme overalt, og funnene i dette kapittelet vil i stor grad også gjelde for de ulike samfunnsfunksjonene.

22.1 Utvalg av felleskomponenter

I utviklingen av digital forvaltning har man satset på enkelte felleskomponenter. Dette er komponenter som kan gjenbrukes i flere IKT-løsninger i offentlig sektor. Enkelt kan man si at felleskomponenter er felles «byggeklosser» for å kunne utvikle elektroniske tjenester. Se forøvrig punkt 23.6 «Næringsutvikling og IKT-sikkerhet» der behovet for effektivisering utdypes nærmere.

Direktoratet for forvaltning og IKT (Difi) har identifisert fem felleskomponenter med stort tverrsektorielt behov som de anbefaler får status som nasjonale felleskomponenter.[1] Disse fem er:

- Grunndata om virksomheter: Enhetsregisteret i Brønnøysundregistrene
- Grunndata om personer: Folkeregisteret hos Skatteetaten
- Grunndata om eiendom: Matrikkelen hos Kartverket
- Altinn-komponentene hos Brønnøysundregistrene
- Felles infrastruktur for e-ID i offentlig sektor hos Difi

Utvalget finner det naturlig å se nærmere på disse felleskomponentene. Det er andre felleskomponenter utvalget kunne sett nærmere på, men det er naturlig å tro at de som er nevnt over, gir god dekning av problemstillingene vi ser ved felleskomponenter.

[1] Direktoratet for forvaltning og IKT (2010): *Nasjonale felleskomponenter i offentlig sektor - Forslag til hvordan nasjonale felleskomponenter bør styres, forvaltes, finansieres og utvikles.*

22.2 Roller og ansvar

Kommunal- og moderniseringsdepartementet (KMD) har et særskilt ansvar for å arbeide for en styrket og mer helhetlig tilnærming til informasjonssikkerhet i statsforvaltningen. KMD har også ansvaret for personvernpolitikk. På informasjonssikkerhetsområdet omfatter ansvaret blant annet valg av felles standarder, krav til bruk av styringssystemer for informasjonssikkerhet, veiledning på overordnet nivå, tilrettelegging for en bedre koordinering av etatenes arbeid med informasjonssikkerhet og understøttelse av samordnede løsninger tilpasset det rettslige rammeverket.

Oppgaven med å følge opp KMDs særskilte ansvar for å arbeide for en styrket og mer helhetlig tilnærming til informasjonssikkerhet i statsforvaltningen er delegert til *Direktoratet for forvaltning og IKT (Difi)*. Grunnprinsippet er at alle har ansvar for å sikre egen informasjon, og Difi skal bistå.

Difi er KMDs fagorgan for IKT-politikken i offentlig sektor og retter seg i hovedsak mot statsforvaltningen, men arbeider også mot kommunal sektor, næringsliv, frivillige organisasjoner og enkeltmennesker. Et av Difis fagområder er digitalisering av offentlige tjenester og arbeidsprosesser, herunder utvikling og forvaltning av fellesløsninger. Direktoratet arbeider med offentlige anskaffelser og forebyggende IKT-sikkerhet i statsforvaltningen, og har ansvar for Kravspesifikasjon for PKI (Public Key Infrastructure) i offentlig sektor. De forvalter ID-porten som er innloggingsportal for offentlig sektor, og MinID, som er en e-ID på nivå 3.

Justis- og beredskapsdepartementet har ansvaret for det nye nasjonale ID-kortet. ID-kortet kan bli en vesentlig faktor i det norske e-ID-landskapet dersom kortet blir utstyrt med en e-ID og ID-kortet blir utbredt.

Nærings- og fiskeridepartementet har ansvaret for lov om elektronisk signatur (esignaturloven).[2]

Nasjonal kommunikasjonsmyndighet (Nkom) fører tilsyn med sertifikatutstedere.

[2] Nærings- og fiskeridepartementet (2001): *Lov om elektronisk signatur (esignaturloven)*.

22.3 Hjemmelsgrunnlag og tilsynsvirksomhet

Det er en rekke lover og forskrifter som regulerer felleskomponenter. I den videre kartleggingen har følgende lover og forskrifter særlig relevans:

Lovgivning for personopplysninger. Personopplysningsloven er generell lov som gjelder for både offentlig og privat sektors behandling[3] av personopplysninger,[4] med mindre særlovgivningen eksplisitt regulerer bruk av personopplysninger som for eksempel helseregisterloven og politiregisterloven. Formålet med loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger, slik at personlig integritet, privatlivets fred og kvalitet på personopplysninger blir ivaretatt. Personopplysninger krever ekstra beskyttelse dersom de er sensitive. Behandling av personopplysninger krever et rettslig grunnlag og skal være saklig begrunnet for et definert og avgrenset formål. Forskrift om behandling av personopplysninger kapittel 2 regulerer krav til informasjonssikkerhet. Det stilles blant annet krav til å sikre opplysningenes konfidensialitet, tilgjengelighet og integritet samt utarbeide sikkerhetsstrategi, risikovurdering, internkontroll, revisjon og avvikshåndtering.

Sikkerhetsloven skal motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Loven er tverrsektoriell, og den skal sørge for at informasjon og objekter som er skjermingsverdige, har tilstrekkelig sikkerhet. Skjermingsverdig informasjon klassifiseres etter sensitivitet i kategoriene begrenset, konfidensielt, hemmelig og strengt hemmelig. Det er opp til objekteieren å melde inn skjermingsverdige objekter, og loven gjelder bare for disse og de som får tilgang til sikkerhetsgradert informasjon fra et forvaltningsorgan.

Regulering av elektronisk ID (e-ID). Det er esignaturloven som regulerer e-ID i Norge. Loven er basert på EU-direktivet om elektroniske signaturer.[5] I praksis er det to styrende dokumenter for e-ID, Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor og Kravspesifikasjon for PKI i offentlig sektor. Rammeverket tar utgangspunkt i fire risi-

[3] Enhver bruk av personopplysninger, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

[4] Opplysninger og vurderinger som kan knyttes til en enkeltperson.

[5] Europaparlaments- og rådsdirektiv 1999/93/EF av 13. desember 1999 om en fellesskapsramme for elektroniske signaturer.

konivåer og definerer fire tilsvarende sikkerhetsnivåer. Kravspesifikasjonen har to sikkerhetsnivåer for personer. Disse identifiseres med rammeverkets to høyeste sikkerhetsnivåer. Den nye ID-kortloven og påfølgende forskrifter vil regulere en e-ID knyttet til det nye ID-kortet. Reguleringen på området vil endre seg, siden en ny EU-forordning erstatter det gamle esignatur-direktivet.[6]

22.4 Beskrivelse av felleskomponenter

22.4.1 Kartverket

Kartverket har det nasjonale ansvaret for geografisk informasjon i Norge og driver en rekke registre relatert til geografisk informasjon. De mest essensielle registrene er:

- Matrikkelen. Dette er Norges offisielle register for eiendom, adresser og bygninger, og oppdateres av kommunene via matrikkelklienten. Matrikkelen er en sammensmelting av Grunneiendom-, adresse- og bygningsregisteret og Digitale eiendomskart. Matrikkelinformasjon er sentral i mye av saksbehandlingen i kommunene og i en del statlige virksomheter og for alle innbyggere og virksomheter som eier eiendommer. Matrikkelloven pålegger alle offentlige virksomheter å benytte matrikkelen i behandling av saker om matrikkelenheter, bygninger, boliger og offisiell adresse.
- Grunnboken. Dette er Norges offisielle register for tinglysing av fast eiendom og borett. Elektronisk tinglysing er på vei inn, og det er hovedsakelig historiske grunner til at grunnboken og matrikkelen er adskilt. Disse to behandles derfor etter de samme sikkerhets- og arkitekturprinsippene i dag.
- Sentralt stedsnavnregister og Nasjonalt register over luftfartshindre.

Kartverkets geografiske informasjon er til en viss grad sensitiv. Dybdedata og landmålinger ved en viss måletetthet er sikkerhetsgradert etter ønske fra Forsvaret og er begrunnet i ønsket om informasjonsoverlegenhet på norsk territorium. Fotografier fra luften er også gradert i visse områder av hensyn til skjermingsverdige objekter.

Kartverket gjør kartdata tilgjengelig både for publikum og andre parter. Svært mange tjenester er avhengige av å kunne lese eller endre data i matrikkelen. Tilgjengelighet blir dermed stadig viktigere.

Manglende integritet i kartdata kan for eksempel skape problemer innen skipsfart. Under granskingen av Rocknes-ulykken i 2004 var manglende merking i båtens kartsystemer ett av flere funn, og eksemplet viser behovet for integritet i alle ledd fra primærkilden til sluttbrukeren.

22.4.2 Brønnøysundregistrene

Brønnøysundregistrene forvalter 18 nasjonale registre og har forvaltningsansvaret for fellesløsningen Altinn. Driften av Altinn er satt ut til en underleverandør.

Enhetsregisteret inneholder grunndata om virksomheter som er sentral informasjon for at offentlige virksomheter skal kunne utføre oppgavene sine på en god måte. Alle offentlige virksomheter som har behov for grunndata om virksomheter, har plikt til å bruke Enhetsregisteret, og private virksomheter får tilgang til offentlige opplysninger gjennom en kommersiell distributør. Tilgjengelighet er svært viktig.

Litt forenklet er Altinn et mellomledd mellom forskjellige offentlige virksomheter, enkeltmennesker og næringsliv. Altinn tilbyr en felles plattform for at forvaltningen skal kunne tilby elektroniske tjenester til innbyggere og næringsliv, og er et sentralt system i digitaliseringen av offentlig sektor. I hovedsak skjer dette gjennom et system for innsending av skjemaer og utsending av meldinger. Det finnes også en arkivfunksjonalitet i systemet.

Mye av informasjonen som passerer gjennom Altinn, er sensitiv, og det er avgjørende at informasjonen er korrekt. Svært mye av informasjonen som passerer gjennom Altinn, lagres også i Altinn over tid. Dersom Altinn blir utilgjengelig, får det raskt store konsekvenser for svært mange offentlige virksomheter, enkeltmennesker og private virksomheter. Systemet er dimensjonert for periodisk stor belastning, for eksempel i forbindelse med selvangivelsen, som det historisk har vært utfordringer med å håndtere.

22.4.3 Skatteetaten

Skatteetaten forvalter en rekke registre og arkiver som inneholder mye sensitiv eller viktig informasjon om enkeltmennesker og virksomheter. For eksempel inneholder Aksjonærregisteret svært mye informasjon om aksjeselskaper, og det er viktig at denne informasjonen er korrekt.

[6] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Folkeregisteret inneholder grunndata om alle borgere og andre som har tilknytning til Norge, og er en viktig nasjonal felleskomponent i elektronisk forvaltning. Her tildeles fødsels- eller D-nummer. Folkeregisteret reguleres av folkeregisterloven. De fleste offentlige virksomheter er avhengige av rask og enkel tilgang til oppdatert og korrekt personinformasjon for å kunne utføre oppgavene sine. Siden disse virksomhetene stoler på informasjonen de får fra Folkeregisteret, er det viktig at informasjonen er korrekt.

Mange offentlige etater har mulighet til å endre eller legge til data i Folkeregisteret. Kvaliteten på dataene i Folkeregisteret er dermed avhengig av kvalitetssikring hos mange andre etater. Et kjent problem er at det registreres flere innslag på én enkelt fysisk person.

22.5 Identifisering av sårbarhet

Utvalget har konsentrert seg om noen få sentrale fellesfunksjoner, innhentet informasjon om disse fellesfunksjonene skriftlig og deretter fulgt opp med møter. Sårbarhetsbeskrivelsene som følger, er oppsummeringer av generelle trekk.

22.5.1 Generelt om sikkerhetsarbeidet

Styring og styringssignaler. Generelt benyttes styringssystemer basert på standard metodikk, der ISO 27 000-serien og ITIL[7] blir nevnt spesifikt. Dette er i henhold til Difis retningslinjer. Sårbarhets-, konsekvens- og risikovurderinger utføres både på systemnivå og på overordnet nivå i de etatene vi har snakket med.

Drift og utvikling. Det er stor variasjon i hvem som utvikler og drifter systemene. Noen svært gamle systemer går på stormaskiner, der man i praksis er tvunget til å sette ut driften til eksterne aktører. Der deler av kritisk infrastruktur er satt ut, benyttes store norske leverandører. Ingen av de utvalgte etatene har plassert kritisk infrastruktur i datasentre utenfor Norge. Det er eksempler på at deler av katastrofeløsninger[8] er plassert utenfor Norge, men disse defineres da ikke som kritiske. Noen av etatene vurderer fremtidig bruk av leverandører innenfor EU, mens andre har det som et prinsipp at deres data skal være lagret i Norge.

Noe programvareutvikling skjer internt i etatene selv, men noen etater har i stor grad tatt i bruk eksterne leverandører og konsulenter. Det er eksempler på at etatene har brukt utviklere fra land utenfor EU. Det oppleves særlig vanskelig å skaffe kompetanse innen sikker utvikling og applikasjonssikkerhet. Utvikling og testing skal ifølge beste praksis være adskilt fra produksjonssystemer og distribusjonssystemer, og det virker som om dette følges opp for fellesfunksjonene. NSM NorCERT bistår med penetrasjonstesting, men har ikke kapasitet til å dekke bistandsbehovet. Det oppleves vanskelig å finne tilsvarende gode tjenester for dette i markedet.

Tilsyn. Riksrevisjonen blir av de spurte nevnt som den mest aktive tilsynsmyndigheten, men de fører ikke tilsyn når det gjelder IKT-sikkerhet. Datatilsynet og DSB har i mindre grad hatt tilsyn med de utvalgte registeretatene. NSM fører tilsyn med de skjermingsverdige objektene og hjelper til med dokumentasjonsprosessene knyttet til dette. De etatene som velger å ikke melde inn objekter, faller naturligvis ikke inn under dette regimet.

Objektsikkerhetsregimet stiller kun funksjonelle krav til sikring av objekter og spesifikke krav til dokumentasjon og sikkerhetsadministrasjon. Det er utfordringer ved å definere registre med stor geografisk redundans[9] som et objekt på samme måte som en fysisk installasjon. Det er funksjonen felleskomponenten har, som er samfunnskritisk, mens det er datahallene som gjerne blir betraktet som skjermingsverdige objekter.

Eksisterende tekniske og organisatoriske tiltak. Alle etatene har tatt i bruk tiltak som tilgangsstyring, slik at ikke alle har tilgang til alt. Endringslogger er et annet mye brukt tiltak.

I all hovedsak er kommunikasjon med brukere beskyttet med hensyn til konfidensialitet og integritet. Noen bruker en egen nøkkelinfrastruktur (PKI) for kommunikasjon med virksomhetskunder, mens andre bruker en offentlig PKI, ofte den samme som brukes for nettsteder på det åpne Internettet. Kryptering og integritetsbeskyttelse er imidlertid mer uvanlig der informasjonen oppbevares.

Knyttet til hendelseshåndtering er det særlig to punkter som blir nevnt. Det oppleves som vanskelig å rekruttere spesifikk IKT-sikkerhetskompetanse innen beskyttelse mot målrettede angrep,

[7] Information Technology Infrastructure Library (ITIL).

[8] Med katastrofeløsninger menes her løsninger for redundans som kan ta over for normal drift eller brukes for gjenoppretting i tilfeller der datasenter rammes av katastrofale hendelser.

[9] Med stor geografisk redundans menes at det er mange kopier, inkludert kriseløsninger, spredt på mange geografiske lokasjoner.

og det stilles spørsmål om det er fornuftig å bygge opp kapasitet i hver etat. Noen av fellesfunksjonene er dekket gjennom NSM NorCERTs varslingssystem for digital infrastruktur (VDI). Vi viser for øvrig til kapittel 21 «Avdekke og håndtere digitale angrep», der hendelseshåndtering blir omtalt.

Det er få øvelser utover ytelsestesting og redundanssjekker. Det kan forklares ved at det i gamle systemer ikke har vært en forventning om at reservesystemer vil overta. Systemene har blitt mer modne, og nå forventes det stort sett at reserveløsninger vil fungere.

Personvern. Omfanget av etatenes arbeid med personvern varierer. Noen har egne personvernombud. Kobling av data fremheves som et økende problem.

22.5.2 Sårbarhetsbeskrivelser

Avhengighet. Alle digitale tjenester er avhengige av infrastruktur som leverer strøm og elektronisk kommunikasjon. Brudd på disse er stort sett en trussel mot tilgjengelighet, ikke mot konfidensialitet eller integritet. Sikkerhetsarbeidet er også avhengig av kompetanse hos dem som leverer digitale tjenester.

Etatene er generelt vant med å vurdere egne sårbarheter, men har i varierende grad oversikt over omfanget av eksterne aktører som er avhengige av etatens tjenester. For eksempel utfører noen etater interessentanalyser og har møter med primæraktørene. De bruker så innspill derfra som grunnlag for egne krav til IKT-sikkerhet. For noen fellesfunksjoner oppfattes det som krevende å bygge opp et komplett bilde av alle som er avhengige av funksjonen, og dermed hvilke verdier som skal sikres.

Sikkerhetskrav og balansering. Sikkerhetskrav formuleres på forskjellige måter. Det kan være krav til tilgjengelighet og kapasitet samt krav til spesifikke teknologiske valg. Krav kan også formuleres som evne til å motstå bestemte trusselaktører eller situasjoner. Eksempel på sistnevnte er at visse endringer ikke skal kunne utføres alene.

Noen opplever også utfordringer knyttet til balansen mellom forskjellige sikkerhetsmål. For eksempel er detaljerte dybdedata sikkerhetsgradert i henhold til sikkerhetsloven, samtidig som dette har nyttige bruksområder innen kartlegging av økologisk liv på havbunnen og planlegging av fiskeoppdrettsfelt. Skjermingsbehovet reduserer i praksis muligheten for andre bruksområder.

Tradisjonelt har integritet og konfidensialitet veid tyngst, men også nye måter å arbeide på kan utfordre dette, for eksempel krav om tilgang til data fra mobile enheter. Spesielt for fellesfunksjoner er det krevende å balansere noen kunders krav om funksjonalitet mot andre kunders krav om sikkerhet.

Styring og styringssignaler. Det er høy grad av bevissthet hos etatene om at ansvaret for sikkerhet ligger hos dem. Etatene får i noen grad sikkerhetskrav utenfra, for eksempel gjennom tildelingsbrev, den nasjonale informasjonssikkerhetsstrategien eller forskrifter, men disse er ofte vage. Dette er forskjellig fra en del andre områder, som for eksempel utforming av webinnhold for svaksynte, der det er veldig strenge og konkrete krav. Dette bidrar til en ubalanse.

Det oppleves som om sikkerhetsnivået må settes av etaten selv. Det kan være positivt, siden etaten selv får «eierskap» til sikkerhetskravene. Det oppleves også som vanskelig å avgjøre hva som er et forsvarlig nivå på sikkerhet. I stor grad blir det faktiske sikkerhetsnivået personavhengig. Utvalget merker seg at etatene i praksis gjør risikovurderinger på samfunnets vegne.

Beskyttelse mot sofistikerte angripere.[10] Det er hovedsakelig enighet blant etatene om at det er utfordrende for dem å oppdage og håndtere sofistikerte angripere. Det er forståelse for at ikke alle uønskede hendelser kan forebygges, og at ressurser må brukes på å oppdage og håndtere slike situasjoner. Utfordringene ligger i at evnen til å oppdage uønskede hendelser ikke er stor, og det vil være behov for ekstern hjelp i håndteringen.

Etatene har tro på at det vil være mulig å hente seg inn igjen fra integritetsbrudd, men i stor grad vil dette skje på improvisert vis, ikke ved å følge et planverk.

22.5.3 Andre observasjoner

Krav til utstedelse og bruk av elektronisk identitet. ID-porten er en innloggingsportal som lar offentlige nettsteder akseptere mange forskjellige løsninger for elektronisk identitet, men likevel forholde seg til bare én teknisk løsning og bare én avtalepart. ID-porten har i dag både Difis egen e-ID og flere fra private leverandører.[11] Difis e-ID har forholdsvis svake rutiner for utstedelse, mens de private leverandørene holder en høyere stan-

[10] Se definisjon i punkt 6.5 «IKT-sikkerhet på den strategiske agendaen».

[11] Difis løsning er på sikkerhetsnivå 3, mens de private aktørenes løsninger alle er på nivå 4.

dard. Når det gjelder bruken av en utstedt e-ID, er sikkerheten svært varierende, men typisk ganske lav i forhold til de anvendelsesområdene som skisseres i Kravspesifikasjon for PKI i offentlig sektor. På kort sikt er det vanskelig å se at det er praktisk å lage e-ID-er med et svært høyt sikkerhetsnivå, men det er fortsatt rom for forbedringer.

Utstedelse av e-ID er knyttet til registreringer i Folkeregisteret. Det betyr at en fysisk person med flere registreringer i Folkeregisteret også kan få utstedt flere elektroniske identiteter. I utgangspunktet er dette ikke en digital sårbarhet, men det kan tenkes at digitalisering av andre tjenester kan få problemer som en følge av dette. Utvalget finner det ikke naturlig å foreslå tiltak mot dette problemet.

Fragmenterte IKT-sikkerhetskrav og motstridende prioriteringer fra myndighetene. Registereiere har påpekt problemstillinger knyttet til inkonsistente krav og prioriteringer mellom Difi og NSM. Det finnes to tilnærminger til sikkerhetsarbeid: Først bestemmer man seg for et sikkerhetsnivå, og deretter ser man hva man kan få til, eller: Først bestemmer man seg for hva man ønsker å gjøre, og deretter ser man hva slags sikkerhetsnivå man kan oppnå. Til en viss grad kan vi se på NSM og Difi som eksponenter for hver sin tilnærming. Evalueringen av Difi belyser grenseflaten mellom Difi og NSM.[12]

Utvalget vurderer kjernen i konflikten til å handle om prinsipielle forskjeller på risikoaksept, nemlig at det på den ene siden handler om ønsket om å hindre uønskede hendelser, og på den andre siden ønsket om tilgjengeliggjøring og effektivisering gjennom digitalisering.

Diskusjoner mellom NSM og Difi rundt sikker digital postkasse dreier seg om hvilket sikkerhetsnivå løsningen skal ha, og hva denne digitale postkassen kan brukes til. Utvalget har valgt å ikke diskutere denne spesifikke problemstillingen, men våre forslag til tiltak vil også påvirke digital postkasse.

22.6 Vurderinger og tiltak

Våre vurderinger og tiltak er i hovedsak basert på sårbarhetsfunn hos eiere av fellesfunksjoner. Utvalget mener det er problematisk at etatene alene bestemmer sikkerhetsnivået til fellesfunksjonene, uten at det sikres at de totale verdiene blir tatt hensyn til. Tiltak for å bøte på dette blir diskutert i punkt 23.1 «Etablere et nasjonalt rammeverk for å ivareta en helhetsvurdering av verdikjeder».

[12] Agenda Kaupang (2014): *Evaluering av Difi.*

22.6.1 Følge utviklingen av IKT-utsetting for felleskomponenter

En opptelling av offentlige datasentre i Norge i regi av KMD[13] konkluderer med et estimat på 150–200. Det er rimelig å tro at det vil bli færre datasentre, at flere av datasentrene blir drevet av eksterne, og at flere samfunnsfunksjoner vil dele infrastruktur som datasentre. Dette kan endre sårbarhetsbildet. *Utvalget er positivt til at offentlig forvaltning tar ut effektivitetsgevinster i bruken av IKT, men mener at KMD bør følge med på sårbarhetsutviklingen knyttet til utsetting av IKT-tjenester for offentlige registre og fellestjenester.* Se diskusjon i punkt 23.7 «Utkontraktering og skytjenester». Se også punkt 23.1 «Etablere et nasjonalt rammeverk for å ivareta en helhetsvurdering av verdikjeder».

22.6.2 Utvikle felles beskyttelsestiltak mot sofistikerte IKT-angripere

Litt forenklet kan vi si at dagens avanserte angrep er morgendagens gjengse angrep, som igjen er neste ukes trivielle angrep. Metodene til sofistikerte angripere blir i økende grad tilgjengelige for mindre sofistikerte aktører. Samtidig ser vi for oss en økning i antallet fysisk samlokaliserte offentlige datasentre, noe som kan føre til økt sårbarhet på grunn av avhengigheter.

Virksomhetene påpeker selv at de ikke har mekanismer på plass for å sikre seg mot sofistikerte angripere. *Det er urealistisk at alle virksomhetene umiddelbart utvikler og setter i drift slike mekanismer. Utvalget mener derfor det er behov for å starte utviklingen av mekanismer som eierne kan bruke for å sikre fellesfunksjoner mot sofistikerte angripere. Difi bør ta en koordinerende rolle, for eksempel ved å sette i gang prøveprosjekter. Dette bør gjøres i samarbeid med forskningsmiljøene, og med bistand fra NSM.* Målet er at gode løsninger gradvis kan tas i bruk i offentlig sektor.

22.6.3 Regulere elektronisk identitet

E-ID-feltet har vært noe preget av ubesluttsomhet siden arbeidet startet rundt årtusenskiftet. Gjentatte ganger har et offentlig ID-kort med tilhørende e-ID vært på trappene, uten at det har blitt

[13] Nexia International (2015): *Kartlegging og analyse av landskapet for offentlige datasentre i Norge 2015* - Utarbeidet for Kommunal- og moderniseringsdepartementet.

noe av. ID-porten var på mange måter et gjennombrudd som gjorde det enklere for offentlige virksomheter å ta i bruk e-ID for innlogging, delvis fordi de fikk én teknisk løsning å forholde seg til, men også fordi de fikk én enkelt avtalepart å forholde seg til.

Private utstedere av e-ID har lenge vært aktive i markedet, med løsninger av varierende kvalitet. Løsningene på høyeste sikkerhetsnivå bruker alle sertifikater, også de som er basert på tiltrodde tredjeparter. Hver leverandør har sitt eget rotsertifikat som ligger til grunn for alle utstedte sertifikater. Dette er en ordning som fungerer greit, både praktisk og prinsipielt. *Utvalget ser ikke noen grunn til å endre på dagens praksis med at hver e-ID-leverandør har sitt eget rotsertifikat.*

Det er behov for e-ID innenfor noen virksomheter og sektorer. Det kan være problematisk å gjenbruke e-ID-er fra andre sektorer eller samfunnsområder, for eksempel på grunn av forskjellige sikkerhetskrav eller forskjellig sikkerhetskultur. Et eksempel er at ansatte bruker sine private e-ID-er for å få tilgang til virksomhetens datasystemer. De ansatte bruker også sine private e-ID-er på sine private datamaskiner, som gjerne har et lavere sikkerhetsnivå. Hvis den private datamaskinen til en ansatt blir kompromittert kan dette også kompromittere den ansattes private e-ID, noe som igjen kan kompromittere virksomhetens datasystemer. Gjenbruk av god e-ID-teknologi kan derimot være fornuftig.

Utvalget anbefaler følgende fem tiltak, med begrunnelse:

1. Kartlegge personinformasjon som tilflyter e-id-leverandørene ved bruk.

Det er vesentlige utfordringer knyttet til bruk av e-ID og personvern. Løsninger med tiltrodde tredjeparter innebærer at e-ID-leverandøren får vite hva brukere gjør med sin elektroniske identitet på nettet. Løsninger basert på smartkort kan komme i tilsvarende situasjon, for eksempel hvis det lagres svar på forespørsler om sertifikatstatus,[14] hvis bruken av kortene overvåkes av sikkerhetshensyn, eller hvis tilbyderen tar betalt for bruken av kortet. Det vil være gunstig å ha en samlet oversikt over hvor mye informasjon som av ulike grunner tilflyter leverandørene. I utgangspunktet bør ikke informasjon om brukernes oppførsel lagres, men der den av forskjellige grunner likevel må lagres, må den beskyttes. Det er også viktig at ikke lovverk og regulering påbyr unødvendig lagring.

Nkom bør sammen med utstederne lage en samlet oversikt over hvor mye personinformasjon som tilflyter de forskjellige e-ID-leverandørene ved bruk av e-ID-en, og hvordan denne informasjonen lagres. Videre bør KMD gjennomgå reguleringen på området, slik at e-ID-leverandørene ikke tvinges til å oppbevare unødvendig personinformasjon.

Problemstillingen er like aktuell for leverandører av elektronisk signatur.

2. Utarbeide én tydelig definisjon av sikkerhetsnivåene.

Til en viss grad er sikkerhetsnivåene i Kravspesifikasjon for PKI i offentlig sektor basert på konsekvenser, men i stor grad snakkes det om teknologivalg. Erfaringsmessig kan det være vanskelig å si om en konkret e-ID oppfyller kravene til et sikkerhetsnivå, eller ikke. Spesielt mener utvalget det bør skilles sterkere mellom sikkerhet ved utstedelse av en e-ID og sikkerhet ved bruk av en e-ID.

KMD bør utarbeide én tydelig definisjon av sikkerhetsnivåene. Den bør ta utgangspunkt i kombinasjoner av angriperens evne og konsekvens. Det må være enkelt å avgjøre om en e-ID når et sikkerhetsmål. Dette bør gjøres samtidig med tilpasningene i forbindelse med den nye EU-forordningen.[15]

3. Begrense bruk av innloggingsportaler til engangspålogging.

I praksis bruker forskjellige e-ID-er forskjellige tekniske løsninger, og de kan dermed vanskelig brukes om hverandre. Et vanlig triks er å bygge en innloggingsportal[16] som «pakker» inn et antall andre e-ID-er. Innloggingsportalen gjør alt arbeidet med å snakke med de forskjellige tekniske løsningene e-ID-ene bruker, og tilbyr ett enhetlig teknisk grensesnitt mot virksomhetene. Innloggingsportalen kan også ta seg av bruksavtaler med e-ID-ene. På denne måten kan virksomheter gjennom innloggingsportalen forholde seg til én teknisk løsning og én avtalepart, i stedet for mange tekniske løsninger og mange avtaleparter.

Siden innloggingsportaler typisk vil observere all innlogging til svært mange tjenester, gjelder til-

[14] Dersom det brukes OCSP (Online Certificate Status Protocol), vil OCSP-tjeneren få mye informasjon om hvem som snakker med hvem. Se også krav 5.3.6 i «Kravspesifikasjon for PKI i offentlig sektor».

[15] Electronic identification and trust services (eIDAS).

[16] Se punkt 5.8 «Elektronisk identifisering» for forklaring av innloggingsportal.

taket om å kartlegge personinformasjon også for innloggingsportaler.

Feilaktig integrasjon av e-ID-ene i innloggingsportalen kan svekke sikkerheten. Et eksempel er at en e-ID brukes til å logge inn på innloggingsportalen. Siden brukeren egentlig ønsker å logge inn hos en virksomhet, øker denne feilen brukerens sårbarhet overfor visse typer angrep der brukeren tror han logger inn på ett nettsted, mens han i realiteten logger inn på et annet nettsted. Økt bruk av innloggingsportaler kan på denne måten svekke sikkerheten og redusere effekten av sikkerhetsforbedringer i eksisterende e-ID-er.

Innloggingsportaler muliggjør såkalt engangsinnlogging («single sign-on»). Her delegerer brukeren rett til å logge seg på en (stor) gruppe nettsteder til terminalen sin. Dette er nyttig dersom en bruker trenger tilgang til mange nettsteder på kort tid. Dersom brukerens terminal er kompromittert, får imidlertid angriperen tilgang til mange nettsteder samtidig, noe som øker konsekvensen av kompromitteringen.

Dersom en virksomhet har flere separate tjenester, kan det være enklere for virksomheten å lage en egen innloggingsportal for disse tjenestene, i stedet for å knytte hver enkelt tjeneste opp mot en felles innloggingsportal som ID-porten eller de enkelte e-ID-ene. Som beskrevet over kan egne innloggingsportaler redusere sikkerhetsnivået til tjenestene vesentlig.

Leverandører av e-ID bør tilstrebe å bruke standard tekniske løsninger, slik at innloggingsportaler kan unngås så langt som mulig. Det bør ikke opprettes flere innloggingsportaler enn strengt tatt nødvendig, spesielt bør det ikke opprettes sektorspesifikke innloggingsportaler. Bruken av innloggingsportaler til engangspålogging bør begrenses til nettsteder av forholdvis triviell karakter, og eieren av innloggingsportalen bør sørge for begrensninger i det totale omfanget av tilgang én enkelt innlogging gir.

4. Forbedre eksisterende e-ID-løsninger fremfor å vente på det nasjonale ID-kortet.

En e-ID tilknyttet det kommende nasjonale ID-kortet har vært under utvikling og planlegging over lang tid og flere ganger vært nær utrulling. Utvalget mener det ikke er klart at e-ID-en som tilhører det kommende ID-kortet vil komme i utbredt bruk eller fortrenge eksisterende e-ID-er. Utvalget mener det derfor er hensiktsmessig å bruke ressurser på å forbedre eksisterende private og offentlige e-ID-er.

Forbedringer av eksisterende e-ID-løsninger bør ikke vente på det nasjonale ID-kortet. Difi bør videreutvikle den eksisterende MinID-løsningen, blant annet ved å tilby en sikrere utstedelse av identiteter, tilsvarende «kvalifiserte sertifikater», samt bedre tekniske løsninger. Difi og Nkom bør sammen oppmuntre til og kreve økt sikkerhet og åpenhet hos private leverandører, fortrinnsvis basert på standard tekniske løsninger.

5. Varsomhet med å rulle ut tjenester med sensitive personopplysninger til hele befolkningen.

Utvalget legger til grunn at e-ID-løsningene ikke vil kunne beskytte gjennomsnittsborgeren mot målrettede angrep de nærmeste årene. Det vil også kunne gjennomføres ikke-målrettede angrep mot mange borgere. Enkeltborgeren har normalt ikke forutsetninger for å forstå hvor stor risiko dette medfører, og det er ikke heldig. Dersom tjenester som inneholder sensitive personopplysninger, rulles ut til befolkningen som helhet, vil man utsette enkeltborgere for en vesentlig risiko som de ikke har akseptert.

Situasjonen er annerledes dersom borgeren selv, etter å ha fått forståelig informasjon om hvilken risiko tilgang til tjenesten medfører, likevel ønsker å bruke tjenesten og eksplisitt ber om tilgang til tjenesten. Det er viktig at de virksomhetene som har slike tjenester legger til rette for at borgerne kan be om tilgang på en god og smidig måte. Et eksempel er at borgerne kan be fastlegen sin om tilgang til kjernejournalen på nett.

Det offentlige bør aktivt gjøre bruk av ID-porten og den tilhørende e-ID-infrastrukturen til å digitalisere samhandlingen med borgerne. Likevel, gitt forventet sikkerhetsnivå i nærmeste fremtid bør tjenester som omhandler sensitive personopplysninger og er avhengige av e-ID, være varsomme med utrulling. Slike tjenester bør ikke rulles ut til befolkningen som helhet uten særskilt god grunn, men heller begrenses til dem som eksplisitt ber om tilgang til tjenesten.

Kapittel 23
Tverrsektorielle sårbarhetsreduserende tiltak

Avhengigheter mellom samfunnsfunksjoner gir tverrsektorielle utfordringer. Sårbarheter i én samfunnsfunksjon kan potensielt få innvirkning på samfunnet som helhet. Det stiller særlige krav til å ha virkemidler, kapasitet og kompetanse til å følge opp problemstillinger som går på tvers av sektorene. Dette kapittelet gir en oversikt over tverrsektorielle sårbarhetsreduserende tiltak, i hovedsak basert på summen av sårbarheter som er identifisert i utredningen.

23.1 Etablere et nasjonalt rammeverk for å ivareta en helhetsvurdering av verdikjeder

En vesentlig årsak til at det er vanskelig å få oversikt over reell digital sårbarhet, er at den ofte ligger skjult og akkumuleres i lange og kompliserte verdikjeder. For eksempel kan en tilsynelatende enkel maskinell verdikjede som gjør det mulig å levere en elektronisk betalingstjeneste, bestå av et tosifret antall systemer som driftes av et tilsvarende antall virksomheter eller organisasjoner, se boks 23.1. Et annet eksempel er følgefeilene som oppstod som følge av et strømbrudd i en mobilsentral i Ålesund, se boks 23.2.

Slike digitale verdikjeder har noen kjennetegn som gjør dem spesielt utfordrende i et sårbarhetsperspektiv.

- *Feil propagerer momentant og noen ganger på uforutsigbare måter.* En feil hos en nettleverandør kan få hele betalingssystemet til å svikte umiddelbart – dette til forskjell fra lange og komplekse verdikjeder i den analoge verden, der følgefeilene av en sviktende tjeneste skjer på en tidsskala av timer, dager eller uker.
- *Tjenestene som inngår i verdikjedene, spenner gjerne over flere sektorer, og de er underlagt forskjellige lovverk og tilsynsregimer i Norge og i utlandet.* I eksempelet med betalingstjenester vil lovverk og tilsynsmyndigheter fra finanssektoren, ekomsektoren, justissektoren og energisektoren virke inn på sårbarheten til den leverte tjenesten. Andre tjenester vil befinne seg i et landskap som ikke er like regulert eller gjenstand for tilsyn av myndighetene. Eksempler på dette er store globale skyleverandører.
- *For dem som utvikler en tjeneste på toppen av slike verdikjeder, er det svært utfordrende å skaffe seg oversikt over hvilke sårbarheter tjenesten er eksponert for lenger nede i verdikjeden.*

Boks 23.1 Avhengigheter via mobilbetaling

Tjenestene som tilbyr betaling via mobiltelefon, trenger velfungerende mobilnett for å virke. Mobiloperatørene leverer tjenestene sine ved å ha avtaler med et antall regionale nettleverandører som de kobler basestasjonene sine til. Disse regionale nettleverandørene har i sin tur avtaler med en operatør av et landsdekkende transportnett. Denne nettinfrastrukturen kobler mobiltelefonen som skal utføre en betaling, til en server som eies av banken som telefoneieren er kunde av. Serveren til banken kommuniserer – igjen over en kompleks nettinfrastruktur som involverer flere nettleverandører – med systemene til den banken som skal motta betalingen.

I tillegg til dette er det en helt annen og like kompleks digital verdikjede som står for autentisering av den som betaler. På toppen av det hele har vi i denne fremstillingen ikke tatt høyde for at driftssystemene til nettoperatørene kan være outsourcet til en annen virksomhet, at selve betalingstjenesten kan være en tredjepartstjeneste som ligger i et driftsmiljø i skyen, at de involverte bankene har latt et eksternt firma utvikle og drive banktjenestene sine, eller at alle disse systemene er avhengige av stabile kraftleveranser og derfor også av kraftbransjens digitale styringssystemer for produksjon og leveranse av kraft.

Boks 23.2 Ekomutfall i Ålesund 6. mars 2014

Natt til torsdag 6. mars mottok Telenors operasjonssenter en alarm som indikerte at et aggregat i Ålesund sentral hadde startet opp på grunn av en forstyrrelse i strømnettet. En ny alarm ble utløst på grunn av lav batterispenning, men denne alarmen ble ikke tolket som en indikasjon på at det var noe unormalt med driftsstatus for sentralen.

Noen timer senere på natten gikk det nye alarmer, og disse alarmene viste at batteriene var i ferd med å gå tomme. Dette medførte at operasjonssenteret til Telenor analyserte alarmene og bestilte en entreprenør som skulle rette opp feilen. På grunn av at sentralen ikke fungerte, fungerte heller ikke mobiltelefonien i området, og det tok lang tid å få tak i en entreprenør. Reparasjonen av sentralen tok ytterligere tid fordi kortleseren man bruker for å komme inn i sentralen, ikke virket på grunn av strømutfallet. Fra den første alarmen gikk, til entreprenøren klarte å ta seg inn i bygget, gikk det nesten ni timer.

Konsekvensene var blant annet utfall av mobil, bredbånd og fasttelefoni i Møre og Romsdal og Sogn og Fjordane. 700 basestasjoner ble berørt, noe som resulterte i varierende grad av utfall av både mobil, bredbånd og fasttelefoni for operatører som Telenor, Broadnet, TeliaSonera, Norkring og TDC.

I enkelte tilfeller fører dette til at tilsynelatende god redundans langt oppe i verdikjeden blir ødelagt av at redundante alternative tjenester er sårbare for den samme hendelsen lenger nede i verdikjedene. Et eksempel på en slik hendelse var da en svikt i hjelpeteknisk utstyr førte til at Telenors sentral i Ålesund mistet elektrisk kraft (se boks 23.2).

– *Noen tjenester er grunnmuren i mange slike verdikjeder, og deres sårbarhet får innvirkning på sårbarheten lenger ute i mange verdikjeder.* Eksempler er tjenester innen telekommunikasjon, energiforsyning og databehandling i skyen. Eierne av disse sentrale tjenestene utfordres ved at det er vanskelig for dem å holde oversikt over hvilke samfunnsverdier systemene deres er bærer av. En ytterligere utfordring er at verdikjedene endres raskt, enkelte ganger også uten at de sentrale tjenestene er involvert i eller informert om endringene.

Det er utvalgets syn at lange og uoversiktlige verdikjeder som spenner over flere sektorer, nivåer og landegrenser, er en kjerneutfordring ved vurdering av digital sårbarhet. Vi mener at komplekse digitale verdikjeder er et vesentlig hinder for å kunne fastslå hvilken digital sårbarhet vi har. Dette finner vi igjen i alle sektorer vi har omhandlet i denne rapporten.

Spørsmålet om hvilken sårbarhet samfunnet bør være beredt til å leve med, anser vi som prematurt på mange områder, all den tid det ikke finnes noe begrepsapparat som hjelper oss med å forstå hvilken sårbarhet som reelt sett foreligger. Utvalget foreslår tiltak som gir en prinsipiell tilnærming til hvordan samfunnet kan få et grep om hvordan digital sårbarhet oppstår og utvikler seg i verdikjedene.

Utvalget mener at Justis- og beredskapsdepartementet bør utvikle et rammeverk for å ivareta helhetsperspektiver i verdivurderinger og sårbarhetsvurderinger. Et slikt rammeverk kan også være nyttig for å forstå ansvarsfordelingen i verdikjedene vi her snakker om. Grunnsteinene i dette rammeverket bør være følgende:

– *Veiledning for å fastsette digitale verdier.* Det bør utarbeides veiledninger som er anvendbare på tvers av sektorer, og de må kunne danne grunnlag for presis informasjon om hvilke verdier som bæres. De må være egnet til bruk for tilsynsmyndigheter og for informasjonsflyt nedover i verdikjedene. Vi understreker at de verdiene vi her snakker om, ikke umiddelbart kan tallfestes økonomisk. De inkluderer blant annet også verdien av en nødmelding på vei til en AMK-sentral, et styringssignal med beskjed om at et tog må stoppe for å unngå kollisjon, informasjon om at noen har utløst en voldsalarm, samt verdien av at en lege har tilgang til journalen til en pasient.
– *Veiledning for å nivåspesifisere akseptert digital sårbarhet.* Aktører må gjøre en ROS-analyse for å identifisere ulike tenkte hendelser som har stor sannsynlighet og store konsekvenser. På bakgrunn av dette må det gjøres en vurdering av hvilken akseptert sårbarhet en er villig til å ha. For tilsiktede handlinger bør disse retningslinjene ta utgangspunkt i trusselaktører, uten nødvendigvis å spesifisere hvilke kapabiliteter disse trusselaktørene besitter. Det bør for eksempel være mulig for ledelsen i en virksomhet å formulere akseptert sårbarhet ved å si at organiserte kriminelle ikke skal kunne bryte

seg inn, men at de aksepterer at ressurssterke stater kan være i stand til det. Teknisk ekspertise kan omsette slike utsagn til tekniske tiltak og kommunisere kostnadene ved disse tiltakene tilbake til virksomhetsledelsen. Dette vil tydeliggjøre behovet for å holde seg oppdatert på trusselaktørers kapabiliteter og behovet for at virksomheter får en mulighet til å tilegne seg denne typen informasjon.

Tiltakene som er skissert over, vil gi grunnlag for en mer presis omtale av digitale verdier og akseptert digital sårbarhet. *Utvalget foreslår videre å benytte dette rammeverket til ytterligere tiltak som bidrar til størst mulig åpenhet om hvilken restsårbarhet man har akseptert som bruker av utstyr og tjenester, samt hvilke verdier man betror sine underleverandører*. Åpenhet rundt dette vil bidra til bevissthet om hvordan sårbarheter og ansvar for verdier propagerer gjennom verdikjeder. Disse ytterligere tiltakene er formulert under.

- *Justis- og beredskapsdepartementet bør ta initiativ til at det utvikles virkemidler som sikrer*
  - at sårbarhets- og verdivurderinger blir gjennomført ved større avtaleinngåelser
  - at det blir kommunisert – og om nødvendig reforhandlet – når de digitale tjenestene til en underleverandør blir tatt i bruk til andre formål enn det som opprinnelig var avtalt
  - at det blir kommunisert – og om nødvendig reforhandlet – når en underleverandør endrer tjenesteproduksjonen sin på en slik måte at sårbarhetsbildet endres
  - at aggregering av verdier på enkeltpunkter i verdikjedene blir synliggjort og håndtert
- *For infrastrukturer og systemer som er avgjørende for kritiske samfunnsfunksjoner, bør de relevante myndighetsorganene utarbeide formuleringer om hva som skal være akseptert sårbarhet*. Beskrivelsene må oppdateres jevnlig for å fange opp endringer i sårbarhetsbildet. Formuleringen bør ta utgangspunkt i eksisterende lovverk og forskriftstekst der dette eksisterer og er relevant. I de tilfellene lov/forskrift ikke gir tilstrekkelig mandat, bør det utvikles hjemmelsgrunnlag. Vurderingen av hva som er akseptabel sårbarhet, bør bygge på innsamlet informasjon om hvilke digitale verdier infrastrukturen eller systemet bærer, og hvilke konsekvenser manglende funksjonalitet får for samfunnet. Dette vil bidra til en klargjørende debatt om hva som er akseptabel sårbarhet i disse systemene. Videre vil det tydeliggjøre spørsmålet om hvilke kostnader samfunnet er villig til å ta for å sikre samfunnskritiske systemer, samt hvordan forebyggende tiltak kan prioriteres.
- *I offentlige risiko- og sårbarhetsanalyser bør det inngå en vurdering av hvorvidt eksisterende restsårbarheter er kompatible med besluttet akseptert risiko*. Sammen med tiltakene over vil det kunne bidra til at en kan vurdere om en hendelse med negative konsekvenser var innenfor akseptert risiko. Videre vil det kunne bidra til at verdi- og trusselvurderinger tvinger seg frem i virksomhetene.
- *I enhver analyse av uønskede IKT-hendelser bør det rapporteres om hvorvidt dette hendelsesforløpet var akseptabelt, gitt den besluttede restsårbarheten*. Dersom svaret på dette spørsmålet er negativt, bør det undersøkes hvor i den digitale verdikjeden avviket mellom akseptert og reell restsårbarhet oppsto. Dette kan bidra til å ansvarliggjøre beslutningstakere i både ledelsen, det tekniske miljøet og leverandørkjeden. I problemstillinger av sektorovergripende karakter er Justis- og beredskapsdepartementets rolle i dette arbeidet særlig viktig.

23.2 Tydeliggjøre krav til virksomhetsstyringssystemer

I flere av kapitlene i denne NOU-en er det pekt på behov for virksomhetsstyringssystemer som kan bidra til å redusere digital sårbarhet – både helt overordnet og for den enkelte virksomhet.

I henhold til instruks om departementenes samfunnssikkerhets- og beredskapsarbeid (kgl.res. 2. juni 2012) er det et krav at alle departementer skal synliggjøre mål og prioriteringer for samfunnssikkerhets- og beredskapsområdet i de årlige budsjettproposisjonene. Dette kravet er ikke spesifikt rettet mot IKT-sikkerhet, men omfatter alt samfunnssikkerhetsarbeid.

I tillegg til føringer og krav som fremkommer i den kongelige resolusjonen som er nevnt over, er offentlig styring regulert gjennom retningslinjer gitt av Finansdepartementet via Direktoratet for økonomistyring (DFØ). Blant annet Kommunal- og moderniseringsdepartementet via Difi gir veiledning om bruk av styringssystemer for å ivareta IKT-sikkerheten.

I *Nasjonal strategi for informasjonssikkerhet* vises det til at både private og offentlige virksomheter skal ivareta IKT-sikkerheten på en helhetlig og systematisk måte, og at dette krever en bevisst bruk av virksomhetsstyringssystemer.

Virksomhetens karakter, størrelse og samfunnsmessige betydning er avgjørende for ambi-

sjonsnivået og ressursinnsatsen på sikkerhetsarbeidet. For å kunne definere et riktig sikkerhetsnivå og vurdere risikoaksept er det nødvendig å basere dette på gode risiko- og sårbarhetsvurderinger. Flere av tilsyns- og kontrollmekanismene i Norge har avdekket svakheter i forvaltningens risikovurderinger og risikostyring.[1] Blant annet er dette knyttet til manglende forankring i ledelse og organisasjon og til begrenset systematisk bruk av ROS-analyser i strategisk risikostyring.

IKT-infrastruktur inngår som en innsatsfaktor i nesten samtlige samfunnsfunksjoner og tjenester. Virksomheter må derfor integrere IKT-avhengighet i eksisterende virksomhetsstyring, med tanke på både tilsiktede og ikke-tilsiktede hendelser. Krav, føringer og måloppnåelse knyttet til å ivareta IKT-sikkerhet bør inngå i det ordinære styringssystemet i hvert departement og også i den generelle etatsstyringen. Dette vil sikre bedre kontinuitet og systematikk i arbeidet, da det blant annet bidrar til at temaet kommer på dagsordenen i etatsstyringsmøter og rapporteringer.

Virksomhetsstyringssystemene må kunne synliggjøre et sårbarhetsbilde basert på en risikovurdering av tilsiktede og utilsiktede IKT-hendelser. Virksomhetsstyringssystemene bør videre gi grunnlag for å vurdere effekten av ulike forebyggende tiltak på IKT-sikkerhetsområdet og hvilke konsekvenser svikt vil ha for samfunnet. Dette vil gi et bedre grunnlag for å prioritere ulike kostnadsdrivende forebyggende tiltak.

Utvalget anbefaler at de ulike departementene tydeliggjør krav og føringer for at de vurderingene som er nevnt ovenfor, tas inn i de ulike virksomhetsstyringssystemene, både på sentralt nivå og ute i de ulike sektorene. Tilsynsmyndighetene må følge opp at dette blir ivaretatt. Se punkt 23.4 «Tilpasse tilsynsvirksomheten til å omfatte IKT-sikkerhet».

Utvalget anbefaler at Justis- og beredskapsdepartementet utarbeider et sett med minimumskrav til hvilke elementer som skal inkluderes i virksomhetsstyringssystemene, og det bør utarbeides veiledningsmateriell som kan øke kompetansen på området.

23.2.1 Bevisst bruk av standarder

Kravene til IKT-sikkerhet i offentlig sektor er ofte funksjonsbaserte og med definerte overordnede mål. Det er ofte henvist til bruk av standarder på områder der det eksisterer et funksjonsbasert regelverk. Å bruke standarder for risikostyring av IKT-systemer er nyttig for å sikre at analyser er mest mulig komplette og tar med alle relevante områder. Henvisning til standardisering er også nyttig for å oppnå effektive sikkerhetstiltak. Standardiseringen kan omfatte både organisering av sikkerhetsarbeidet, kompetansetiltak og konkrete tekniske sikkerhetsløsninger.

Det er imidlertid viktig å ha et bevisst blikk på bruk av standarder. Implementering og bruk av standarder krever kunnskap og teknisk innsikt, og fornyelse og utvikling av standarder er ressurskrevende. Videre bidrar det store og økende antallet standarder til kompleksitet.

I Norge er det i dag tre standardiseringsorganer – to private (NEK og Standard Norge) og én offentlig (Nkom). Det er grunn til å se på både hvordan tilblivelsesprosessen av standarder i Norge blir ivaretatt, og hvilke standarder de ulike myndighetene velger å vise til. Det kan oppstå et demokratisk underskudd i den grad berørte parter ikke har mulighet, tilstrekkelig med ressurser eller kapasitet til å delta i standardiseringsprosesser.

Bruken av funksjonsbaserte regler og henvisning til ulike standarder kan bidra til økt kompleksitet og uklarhet i den interne virksomhetsstyringen (risikostyringen), og det kan oppleves som krevende å navigere i handlingsrommet mellom upresise krav, myndighetenes «forventninger» og alternative løsninger.

Utvalget mener at Norge i stor grad bør implementere standarder som er internasjonalt anerkjent, og at det på IKT-området i liten grad er hensiktsmessig eller nødvendig å produsere særnorske standarder. Det er imidlertid viktig at Norge bidrar og er aktive i utarbeidelsen av standarder internasjonalt. Den enkelte sektor har her et spesielt ansvar. Se nærmere omtale i punkt 23.4 «Tilpasse tilsynsvirksomheten til å omfatte IKT-sikkerhet». Justis- og beredskapsdepartementet har et særskilt ansvar for de standardene som omhandler IKT-sikkerhet, og som ikke er direkte relatert til en særskilt sektor, og *utvalget anbefaler at departementet har en strategisk tilnærming til hvordan de skal bidra i standardiseringsarbeidet.*

23.3 Styrke Justis- og beredskapsdepartementet på IKT-sikkerhetsområdet

Tiltak for å styrke det helhetlige blikket på samfunnssikkerhetsområdet er drøftet ved mange anledninger. I Sårbarhetsutvalget[2] ble det fore-

[1] DSB, NSM, Datatilsynet, Riksrevisjonen mfl.

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

slått å etablere et innenriksdepartement, mens det i Infrastrukturutvalget[3] ble foreslått å styrke Justis- og beredskapsdepartementets samordningsrolle. I etterkant av Sårbarhetsutvalget ble DSB etablert som et alternativ til et innenriksdepartement for å styrke samordningsrollen til Justis- og beredskapsdepartementet. I tillegg er samordningsrollen, samt krav og forventninger til sektordepartementene på samfunnssikkerhets- og beredskapsområdet, tydeliggjort i en kongelig resolusjon i 2012. I 2013 ble samordningsrollen ytterligere styrket og ansvaret samlet ved at også ansvaret for forebyggende IKT-sikkerhet i sivil sektor ble overført fra Kommunal- og moderniseringsdepartementet[4] til Justis- og beredskapsdepartementet, og ved at Nasjonal sikkerhetsmyndighet ble styrket som IKT-sikkerhetsdirektorat.

23.3.1 Tydeliggjøre Justis- og beredskapsdepartementets rolle og ansvarsområde

Utvalget er kjent med at det fortsatt diskuteres hva som tilligger JDs «nye» rolle for samordning av IKT-sikkerhet, og at det synes å være noe uenighet rundt hvilken samordningsrolle JD skal ha knyttet til IKT-sikkerhet i statsforvaltningen.

Utvalgets vurdering er at JDs samordningsansvar for forebyggende IKT-sikkerhet i sivil sektor omfatter både privat og offentlig sektor. Utvalget mener, og finner det hensiktsmessig, at JD i sivil sektor dekker det overordnede nasjonale ansvaret for IKT-sikkerhet, herunder å fastsette minimumskrav til IKT-sikkerhet. Det enkelte fagdepartement har ansvar innen egen sektor.

Utvalget anbefaler derfor at ansvaret for IKT-sikkerhet konkretiseres ytterligere, slik at det går klart frem at JDs samordningsansvar gjelder både offentlig og privat sektor. Om nødvendig kan en slik klargjøring komme i form av en revisjon av Kgl.res. 22. mars 2013.[5]

23.3.2 Styrke Justis- og beredskapsdepartementets virkemidler

Utarbeide en helhetsoversikt over digitale sårbarheter

Etter utvalgets vurdering må JD gjøre ytterligere grep for å få oversikt over digitale sårbarheter på tvers av sektorer. Førstehåndskunnskapen om digitale sårbarheter ligger i den enkelte sektor. Utvalget mener at JD må etablere mekanismer og egnede metoder for å benytte denne kunnskapen. En rapportering fra de ulike sektorene til Justis- og beredskapsdepartementet vil bidra til at departementet i større grad kan sammenligne på tvers av områder og sektorer og bidra i diskusjoner om tverrsektorielle prioriteringer. Omforente krav til styringssystemer som vist i punkt 23.2 vil her være sentralt. Utvalget er kjent med at Justis- og beredskapsdepartementet har fått bistand til å etablere nasjonale indikatorer for IKT-sikkerhet. Dette synes å kunne være en god start, men utvalget vil påpeke viktigheten av at et slikt oversiktsbilde inkluderer et helhetsbilde og ikke bare er knyttet til tilsiktede hendelser.

Et godt metodisk rammeverk er nødvendig, både for å kunne samle inn relevante data og for at en helhetsoversikt over sårbarhetene skal kunne benyttes på en hensiktsmessig måte. På dette området foreligger det allerede mye relevant arbeid i JDs underliggende etater, blant annet DSBs nasjonale sårbarhetsrapport og NSMs årlige IKT-risikobilde. Utvalget ser det som hensiktsmessig at det ikke bygges opp doble kapasiteter i forbindelse med å fremskaffe en helhetlig oversikt, og at oversikten i stor grad bør bygges på det arbeidet som per i dag gjøres på området i DSB og NSM. *Utvalget anbefaler at departementet ber NSM og DSB om å utarbeide et felles metodisk rammeverk i samarbeid som kan ligge til grunn for en helhetlig årlig oversikt over digital sårbarhet.*

Ulike sektoroversikter som Finanstilsynets årlige ROS-analyse og Nkoms tilstandsvurdering av ekom vil være eksempler på relevante kunnskapsgrunnlag i en overordnet nasjonal vurdering av digitale sårbarheter.

Utvalget anbefaler at JD utarbeider en helhetsoversikt over digitale sårbarheter. Oversikten skal kunne bidra til komparative tverrsektorielle sammenligninger og gi et kunnskapsgrunnlag for virkemiddelbruk og prioriteringer på tvers av sektorer.

Følge opp arbeidet med NIS-direktivet og etablere en minstestandard

Utvalget mener at Justis- og beredskapsdepartementets samordningsansvar bør omfatte samord-

---

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

4 Statsministerens kontor (2013): *Overføring av samordningsansvaret for forebyggende IKT-sikkerhet fra Fornyings-, administrasjons- og kirkedepartementet til Justis- og beredskapsdepartementet.* Kgl. res. 22.03.2013.

5 Ibid.

ning av minstekrav til IKT-sikkerhet i sivil sektor og harmonisering av regelverk på området, slik at regelverket ikke skaper dysfunksjonalitet, men synergi på tvers av sektorer. Utvalget observerer at sektorene tidvis har vansker med å enes om en gjennomføring av sektorovergripende tiltak. Samtidig erkjenner utvalget at behovene innen de enkelte sektorene varierer, noe som tilsier at sektorene må kunne ha stor grad av frihet både til operasjonalisering og til å heve ambisjonsnivået utover minstekravet.

Utvalget anbefaler at Justis- og beredskapsdepartementet aktivt følger opp prosessen rundt EUs NIS-direktiv[6] *og vurderer hvilke konsekvenser direktivet kan få for Norge, og hvordan dette kan påvirke JDs samordningsrolle på området, særlig med tanke på å gi føringer og stille krav til andre departementer og forberede sektorene på å implementere direktivet.* Behovet for å etablere en felles minstestandard for beskyttelse av kritisk infrastruktur bør vurderes og ses opp mot resultatet av NIS-direktivet og eventuelt andre krav fra EU. I denne sammenhengen vil konklusjoner fra Traavik-utvalget være viktig.

Ivareta hensyn til IKT-sikkerhet ved teknologiskifter og strukturelle samfunnsendringer

Samfunnets teknologiske avhengighet gjør at teknologiskifter og større strukturelle endringer har konsekvenser for den digitale sårbarheten. Ved beslutninger som kan føre til større teknologiske og strukturelle endringer i samfunnet, mener utvalget at det bør etableres en ordning som ivaretar konsekvensvurderinger og eventuelle tiltak knyttet til IKT-sikkerhet.

Utvalget anbefaler å se hen til hvordan Konkurransetilsynet ivaretar konkurransehensyn ved organisatoriske og strukturelle endringer i markedet. Ordningen bør ivaretas av Justis- og beredskapsdepartementet.

Etablere en arena for privat–offentlig samarbeid

Utvalget vil særlig peke på viktigheten av samarbeid med privat sektor. Slikt samarbeid foregår i dag på mange nivåer i offentlig forvaltning, blant annet innen beredskap. Alle sektorer har et ansvar for å legge til rette for et offentlig–privat samarbeid, men JD har et overordnet ansvar også på dette området.

Utvalget anbefaler at JD vurderer hvorvidt det privat–offentlige samarbeidet på IKT-sikkerhetsområdet er tilstrekkelig ivaretatt og hensiktsmessig, og hvorvidt det er behov for en strategisk arena for samarbeid med eiere av kritisk infrastruktur og kritisk informasjon, samt akademia, som ledes av JD. Utvalget anbefaler å se til tilsvarende ordninger i blant annet Nederland og Tyskland.

23.3.3 Øke kapasiteten innen IKT-sikkerhet i Justis- og beredskapsdepartementet

For utvalget fremstår det som usikkert hvorvidt den kapasiteten som JD i dag besitter, er tilstrekkelig til å ivareta utfordringene på IKT-sikkerhetsområdet. For å kunne ivareta den utvidede rollen som JD har fått, og i tillegg de tiltakene som utvalget her foreslår, anbefaler vi å styrke JDs ressurser vesentlig på området. Utvalget anerkjenner den eksisterende IKT-sikkerhetskompetansen i JD, men anser kapasiteten som for lav med tanke på gjennomføringsevne. Dersom kapasiteten i JD ikke styrkes tilstrekkelig, vil det ikke være mulig å ta ut effektene av de sistnevnte tiltakene, de vil snarere virke mot sin hensikt.

23.4 Tilpasse tilsynsvirksomheten til å omfatte IKT-sikkerhet

Departementene har gjennom ulike direktorater og tilsyn en viktig rolle når det gjelder å stille krav til og følge opp IKT-sikkerhet i virksomheter innenfor egen sektor. Et av funnene i utvalgets arbeid er at det stilles svært ulike krav fra de ulike myndighetsaktørene. Enkelte myndigheter synes å stille svært detaljerte krav, mens andre stiller mer åpne krav.

Økt teknisk kompleksitet på IKT-området øker utfordringene på tilsynsområdet. Regelverk som ikke henger med i den tekniske utviklingen, gjør at tilsynene mangler retningslinjer å utøve tilsyn etter. Økt bruk og avhengighet av IKT er med på å skape kompetanseutfordringer for tilsynene, som tradisjonelt har ført tilsyn som i større grad har vært basert på faglige krav og føringer.

23.4.1 Vurdere funksjonsbasert regelverk

Både nasjonalt og internasjonalt har det de siste par tiårene vært en utvikling av reguleringsregimer der rettsregler i større grad har vært rettet mot styring og formål og i mindre grad mot spesifiserte (tekniske) løsninger eller metoder. Dette gjelder blant annet – og kanskje særlig – regimer rettet mot risiko og sikkerhet. Utviklingen har dels skjedd parallelt, ved at regulering av styrings-

[6] Se punkt 10.6.1 for mer informasjon om NIS-direktivet.

krav er knyttet direkte til regulering av formålskrav. I begge tilfeller er målet å ansvarliggjøre virksomhetene, eksempelvis gjennom krav til risikostyring. Samtidig gis de større frihet til å sikre at reguleringsformålene ivaretas, for eksempel om et forsvarlig sikkerhetsnivå. Førstnevnte betegnes gjerne i faglitteraturen som «management-based regulations» og sistnevnte som «principles-based regulation». Grunnen til at disse utviklingstrekkene ses i sammenheng, er at de i en viss forstand forutsetter hverandre. Når virksomheter får større frihet, må samtidig kravene til styring være tydeligere. Omvendt gir krav til styring ikke så mye mening dersom svarene/løsningen allerede er gitt i regelverket i form av spesifiserte krav.

Begrepet *funksjonsbasert regelverk* har ikke et helt entydig innhold. I St.meld. nr. 17 (2002–2003) *Om statlig tilsyn* legges det vekt på at slike regler i større grad retter seg mot mål og resultater og i mindre grad mot bestemte metoder eller løsninger. *Funksjonskrav* forstås også ofte som generelle krav – i motsetning til spesifiserte krav. Disse dimensjonene knyttes gjerne sammen ved at funksjonsbaserte krav forstås som generelle krav rettet mot et formål. Men det kan også tenkes andre kombinasjoner, der man har generelle krav rettet mot prosesser og ikke mot resultater. Kravene til internkontroll og systematisk HMS-arbeid i virksomheter er et eksempel. Den vanligste forståelsen av funksjonskrav er likevel gjerne at begge disse elementene er inkludert.

Begrunnelsene for utvidet bruk av funksjonskrav er flere:

- Regelverk er ikke tilstrekkelig dynamiske til å følge utviklingen av de beste løsningene innen forskjellige fagområder (teknologi, behandlingsformer med videre).
- Virksomhetene får handlefrihet og kan utnytte lokal og situasjonsspesifikk kunnskap til å finne egnede løsninger innenfor regelverkets rammer.
- Funksjonsregelverk ansvarliggjør i større grad virksomhetene for egen drift og de konkrete løsningene de velger.
- Funksjonsbaserte regler kan i større grad bidra til at man unngår «creative compliance», at hensikten med reglene oppnås, og at virksomhetene også kan strekke seg lenger enn til fastsatte minimumskrav.

Funksjonskrav er ofte utformet som *rettslige standarder* der innholdet i bestemmelsene utledes av normer utenfor de tradisjonelle juridiske rettskildene, men er knyttet til hva som er ansett som god faglig praksis/standard på området, noe som endrer seg i takt med utviklingen. Det er valgt ulike løsninger i ulike sektorer for hvor konkret disse standardene angis. Virksomhetene kan ha ulike utfordringer med å klarlegge hvordan de rettslige standardene skal forstås og fortolkes, og dermed hvilke konkrete krav som følger av disse.

I Norge har funksjonskrav i særlig grad vært utviklet innenfor petroleumssektoren, men er også utbredt innenfor andre reguleringsområder. Internasjonalt har funksjonskrav vært assosiert med EUs såkalte «new approach» – eller «ny metode» – og brukes til regulering av produktsikkerhet. Hovedtilnærmingen har vært at selve regelverket angir overordnede formål som skal ivaretas, men med henvisninger til anerkjente normer som kan benyttes, og som angis som tilstrekkelige for å oppfylle de rettslige kravene. Det gis imidlertid anledning til å velge andre løsninger, men virksomheten pålegges da i ulik grad å dokumentere at disse tilfredsstiller de overordnede kravene.

Generelt innebærer utvikling og bruk av funksjonsbaserte regler en rekke avveiinger og dilemmaer. Erfaringene internasjonalt er også blandet. De generelle begrunnelsene – ansvarliggjøring, handlefrihet, fleksibilitet og endringstilpasning – må avveies mot generelle rettssikkerhetshensyn som tradisjonelt er blitt vektlagt når det gjelder utforming av rettsregler, slik som klarhet, tydelighet og forutberegnelighet. Regulerte virksomheter må kunne danne seg en begrunnet oppfatning av hva som ligger innenfor regelverkets krav og myndighetenes forventninger. I tillegg kommer at reguleringsmyndigheten i mange sammenhenger vil ha en privilegert oversikt og kunnskap som kan formidles gjennom forståelige og praktisk anvendbare regler og derved bidra til mer forutsigbare og forsvarlige resultater. Sentralisert standardfastsetting kan i praksis fungere som kompetanseoverføring og nødvendig implementeringsstøtte. For vage regler kan gi stor variasjon i resultater i form av etterlevelse og håndhevingspraksis fra myndighetene og i tillegg gi legitimitetsutfordringer dersom den utøvende forvaltningsmyndigheten i praksis fremstår som normsettende for akseptable forsvarlighetsnivåer uavhengig av demokratiske beslutningsprosesser.[7]

Forståelse av de regulerte virksomhetenes forutsetninger for å etterleve de overordnede reguleringshensynene vil måtte spille inn i valget av reguleringsstrategi. Dersom det er stor variasjon i målgruppen, vil avveiingen mellom praktiske opp-

[7] Jacob Kringen (2014): Bidrag til Lysneutvalget.

skrifter og funksjonsbaserte regler være særlig utfordrende. Viktige faktorer i den sammenhengen vil være de regulerte virksomhetenes ressurser, kapasitet, motivasjon og behov (eksempelvis knyttet til tempo i teknologisk utviklingstakt). Men avveiinger må også ses i lys av myndighetenes evne og kapasitet til å tilby tilstrekkelig veiledning i regelverksforståelse, samt til kontinuerlig å vurdere om etterlevelsesmønstre reflekterer kravene til tilstrekkelige og forsvarlige løsninger.

Utvalget anbefaler at når tilsynsmyndighetene skal utforme nye krav og føringer til regulerte virksomheter, er det viktig at det tas hensyn til vurderingene av funksjonsbasert regelverk, som drøftet over. Når det skal stilles krav til IKT-sikkerhet, bør funksjonsbasert regelverk og tilsyn vurderes – dette for å kunne følge med på raske teknologiske endringer og legge til rette for sikkerhetstiltak som er tilpasset den enkelte virksomhet. Som nevnt må det tas hensyn til både virksomhetenes og tilsynsmyndighetenes ressurser og kompetanse på IKT-sikkerhetsområdet. Det er videre viktig å ha et bevisst forhold til anbefalte standarder, jf. punkt 23.2.1 «Bevisst bruk av standarder».

23.4.2 Øke IKT-sikkerhetskompetanse og kapasitet hos tilsynene

Utvalget ser en økende digitaliseringstakt innenfor sektorene som er beskrevet i denne utredningen. Dette krever at tilsynsmyndighetene har kompetanse og kapasitet til både å gjennomføre relevante tilsyn og ivareta sin veiledningsplikt på IKT-sikkerhetsområdet. Et annet aspekt er at tilsynene må delta aktivt i det internasjonale arbeidet som foregår på IKT-sikkerhetsområdet innenfor deres sektorer.

Etter utvalgets vurderinger er det derfor behov for å styrke IKT-sikkerhetskompetansen innenfor flere sektortilsyn. På kort sikt kan det være hensiktsmessig med felles ressurser, slik at ulike sektortilsyn kan tilføres kompetanse fra for eksempel NSM i enkelttilfeller. På lengre sikt tilsier utviklingen at tilsynsmyndighetene må etablere egen kompetanse. Utvalget anbefaler i denne utredningen at en rekke tilsynsmyndigheter styrker både kompetansen og kapasiteten på IKT-sikkerhetsområdet.

Mange av problemstillingene knyttet til IKT-sikkerhet som går frem av denne rapporten, vil være felles for de fleste sektorer, og for å møte behovet for IKT-fokus hos tilsynsmyndighetene bør det etableres fellesarenaer for erfaringsutveksling og dialog mellom sektormyndigheter og tverrsektorielle myndigheter. Et økt tilsynssamarbeid etter for eksempel modell fra HMS-myndighetene kan være en måte å gjøre dette på. Der er det blant annet utviklet en nettside som samler alt av relevant regelverk.[8] En felles møtearena for IKT-sikkerhet bør omfatte regelmessige kontaktmøter på praktisk nivå, ikke bare på ledernivå. Innenfor ekomsektoren er det etablert et ekomsikkerhetsforum som samler de fire viktigste teleselskapene, E-tjenesten, PST og NSM under ledelse av Nkom for nettopp å dele informasjon og trusselinformasjon på gradert nivå. Dette er en modell som fungerer godt, er gjensidig forpliktende og har overføringsverdi til andre sektorer. Et annet eksempel er NVEs initiativ til Samvirkegruppe for infrastruktur, som kan videreutvikles og omfatte erfaringsutveksling av felles problemstillinger og utfordringer relatert til tilsynsmetode og -utøvelse.

Utvalget anbefaler at Justis- og beredskapsdepartementet tar initiativ til å etablere en fellesarena for tilsynssamarbeid på IKT-sikkerhetsområdet. Samarbeidsarenaen bør omfatte erfaringsutveksling, muligheter for kompetanseheving, metodeutvikling og utarbeidelse av ulike tilsynsvirkemidler, som anbefaling av ROS-metoder, veiledningsmateriell, håndtering av underleverandører, og så videre.

23.5 Redegjørelse for IKT-sikkerhet bør inngå i årsmeldinger

Ansvaret for IKT-sikkerhet ligger hos den øverste ledelsen både i privat og i offentlig virksomhet. Utvalgets undersøkelser tyder på at arbeidet med IKT-sikkerhet ikke alltid får den prioriteten det bør ha. *For å sikre at arbeidet med IKT-sikkerhet prioriteres høyere, bør det innføres et krav til at ivaretakelse av IKT-sikkerhet beskrives i virksomhetenes årsmelding.* Dette bør gjelde uavhengig av om virksomheten er i privat eller i offentlig sektor. Utvalget har merket seg at et relatert forslag som gjelder personvern, er fremmet av EU i utkastet til ny personvernforordning, men når denne NOU-en skrives, er det uklart om dette vil bli vedtatt.

Krav til å inkludere redegjørelse for IKT-sikkerhet kan utformes på flere måter, men nødvendigvis slik at man krever en generell redegjørelse for hvordan IKT-sikkerheten er ivaretatt. Utvalget går ikke nærmere inn på hvordan dette konkret bør formuleres, *men oppfordrer Nærings- og fiskeridepartementet og Kommunal- og moderniseringsde-*

[8] Se http://www.regelhjelp.no.

partementet til å utarbeide en regelendring i lovverket for henholdsvis privat og offentlig sektor.

23.6 Næringsutvikling og IKT-sikkerhet

Norge ligger i verdenstoppen når det gjelder å ta i bruk digital teknologi og Internett. Den digitale teknologien er en katalysator som kan effektivisere nær sagt alle sider ved samfunnet. Dette har innvirkning på norsk næringsliv, som i hovedsak består av små og mellomstore virksomheter. Ferske tall fra Statistisk sentralbyrå viser at det ved inngangen til 2015 var 547 232 virksomheter i Norge, hvorav 96 prosent hadde færre enn 19 ansatte.

23.6.1 Behov for balanse mellom verdiskaping og IKT-sikkerhet

Fremtidens IKT-sikkerhet er ikke bare avhengig av teknologien, men også av hvilken politikk som føres på området. Myndighetene har en tredelt rolle i dette bildet – som *bruker* av digitale tjenester, som *beskytter* av befolkningen og som *utnytter* av det mulighetsrommet digitaliseringen gir.

Konkurransekraft for norske arbeidsplasser er et av regjeringens viktigste satsingsområder. Norsk økonomi og næringslivet skal utnytte ressursene smartest mulig og mest mulig effektivt gjennom teknologi, innovasjon og kunnskap.[9] Bruken av IKT skal styrke næringslivets konkurransedyktighet og øke samfunnets totale produktivitet og innovasjonsevne.[10]

Produktivitetsveksten er avgjørende for konkurranseevnen og velstandsutviklingen i Norge i årene fremover. Ifølge Produktivitetskommisjonen utnytter Norge i dag i for liten grad potensialet ved bruk av digital teknologi. Kommisjonen har blant annet uttrykt: «Vår fremtidige velstand og velferd forutsetter at produktiviteten fortsetter å vokse» og: «En liten, åpen økonomi må utnytte internasjonal teknologiutvikling, og det må legges større vekt på forutsetninger for teknologisk adopsjon».[11]

Internasjonalt peker cyberstrategiene til England, USA og Nederland alle på viktigheten og prioriteringen av velfungerende IKT-systemer og deres særskilte betydning for økonomisk vekst og økt velferd. Den nederlandske cyberstrategien går langt i å vise til viktigheten av næringsaspektet ved sikkerhetsløsninger. I strategien fremheves det at innovasjon, sikkerhet og personvern i designfasen av produkter og systemer er initiativer myndighetene og næringslivet skal fokusere på og belønne. Tilsvarende peker flere internasjonale IKT-leverandører på fremtidens muligheter og utfordringer utover teknologiske trender.

Kommunal- og moderniseringsdepartementet (KMD) har uttrykt at det EU gjør for det digitale indre markedet, får direkte betydning for Norge. Regjeringen har derfor satt i gang et arbeid med en ny digital agenda som vil bli lagt frem for Stortinget i 2016.

Mulighetsrommet i Norge for å utnytte ny teknologi ligger i et kompetent og omstillingsvillig næringsliv og i offentlig sektor, samt i høy grad av tillit mellom næringsliv, innbyggere og myndigheter.[12] Befolkningens digitale vaner og adferd viser at nordmenn er opptatt av ny teknologi, og at vi er raske til å ta den i bruk. Hele 90 prosent av innbyggerne har bredbåndstilknytning.

Mørketallsundersøkelsen for 2014 viser at bruken av skytjenester har steget betraktelig. I 2012 benyttet halvparten av virksomhetene seg av en eller annen form for skytjeneste, mens det nå er to av tre virksomheter som gjør det. En undersøkelse gjort i EU i 2014 av virksomheters bruk av skytjenester viser at de nordiske landene med Finland i spissen ligger på topp.

Sikkerhet oppgis som den mest begrensende faktoren for virksomheters bruk av skytjenester. Det er vanskelig for lovgiverne å holde tritt med denne teknologiutviklingen, og det skaper et behov for å tenke annerledes. Mange land har derfor utarbeidet strategier for bruk av skytjenester. Et hovedhensyn er at lovgivning ikke skal hindre økt konkurransekraft ved å gjøre det vanskelig å ta i bruk ny og mer hensiktsmessig og kostnadseffektiv teknologi. Norge har i dag ikke noen offisiell IKT-politikk for bruk av skytjenester, men KMD tar sikte på å legge frem en nasjonal strategi for bruk av skytjenester i løpet av 2015. Utvalget mener at regjeringens påbegynte arbeid med en gjennomgang av regelverket for å fjerne unødige hindringer og rydde opp i uklarheter er viktig for å fremme sikker og forutsigbar bruk av IKT-tjenester. Se nærmere beskrivelse i punkt 23.7 «Utkontraktering og skytjenester».

---

9 Regjeringen (2013): *Tiltredelseserklæring fra regjeringen Solberg 18. oktober 2013, Sundvolden-plattformen* 16.10.13.

10 Meld. St. 23 (2012–2013) *Digital agenda for Norge – IKT for vekst og verdiskaping.*

11 NOU 2015: 1 *Produktivitet – grunnlag for vekst og velferd.*

12 Meld. St. 23 (2012–2013) *Digital agenda for Norge – IKT for vekst og verdiskaping* og Meld. St. 39 (2012–2013): *Mangfold av vinnere*, kap 3.8.

Boks 23.3 Nasjonal kryptopolitikk

NSMs *Sikkerhetsfaglig råd 2015* peker på at bruk av kryptografiske mekanismer har stor betydning for IKT-sikkerhet. NSM har et tett samarbeid med norsk kryptoindustri for utvikling av høygraderte kryptoløsninger. Uten et velfungerende samarbeid mellom industri og myndigheter ville nasjonen ikke evnet å utvikle kryptoløsninger for å sikre informasjon som er viktig for nasjonens sikkerhet. I *Sikkerhetsfaglig råd 2015* er det fremmet en anbefaling om at «Forsvarsdepartementet og Justis- og beredskapsdepartementet bør videreutvikle en nasjonal kryptopolitikk for å sikre nødvendig nasjonal kryptokompetanse og utvikling av kryptoutstyr for høygradert informasjon» for å stimulere til innovasjon og produktutvikling. NSM har i tillegg tatt til orde for at det stilles krav til bruk av godkjente krypteringsløsninger for annen sensitiv informasjon, og at NSM blir gitt i oppdrag å legge til rette for dette.

23.6.2 Økt veiledning for særlig sårbare grupper i næringslivet

I *Risiko 2015* omtaler NSM særskilt sårbarheten i leverandørkjeden. Rapporten viser til flere eksempler på digitale angrep i 2014 mot underleverandører til større virksomheter og til viktigheten av økt bevissthet og krav til sikkerhet også for små og mellomstore bedrifter (SMB). Det er eksempler på at leverandører med dårlig informasjonssikkerhet verken lykkes med å få kunder eller med å komme inn på markedet. Mørketallsundersøkelsen for 2014 viser at små virksomheter kommer svakest ut når det gjelder oppfølging av tjenesteleverandør.

Det oppgis at bare to av fem virksomheter i offentlig sektor har avsatt interne ressurser til å følge opp leverandøren. I privat sektor har halvparten av virksomhetene slike ressurser. Dette er et bekymringsfullt lavt antall i lys av en økende trend, der virksomheter benytter underleverandører til drift av IKT-løsninger. Bestillerkompetanse er i undersøkelsen vist til som helt avgjørende for å sikre egne data hos en underleverandør. Tallene indikerer at både private og offentlige virksomheter bør vie større oppmerksomhet til kontroll og oppfølging av leverandørene. Små og mellomstore virksomheter vil ha behov for nødvendig veiledning og hjelp på informasjonssikkerhetsområdet. Et systematisk veiledende og rådgivende arbeid er svært viktig av hensyn til både næringsutvikling og nasjonal sikkerhet. Arbeidet må skje i takt med digitaliseringen og et økende trusselbilde. Dette er utfordrende å styre både politisk, økonomisk og organisatorisk, og forutsetter en evne til å håndtere akselererende endringer og legge inn mekanismer for å følge opp og vurdere sikringsbehovet.

Etter utvalgets vurdering vil manglende digital sikkerhet i små og mellomstore virksomheter, og særskilt underleverandørkjeden utgjøre en nasjonal sårbarhet det er viktig å rette oppmerksomhet mot i tiden fremover.

23.6.3 Tillit bør være en forutsetning for digitaliseringen

KMD viser i sin handlingsplan for informasjonssikkerhet i statsforvaltningen (2015–2017) til at informasjonssikkerhet er en forutsetning for digitalisering i offentlig sektor. I *Digital agenda for Norge* fremgår det at:

> «Forebyggende IKT-sikkerhet er […] en viktig del av samfunnssikkerheten, og vi må ha på plass systemer og rutiner for å forebygge og håndtere uønskede hendelser til IKT. Dette er viktig for at alle skal ha tillit til de IKT-løsningene som tilbys, både fra private aktører og fra det offentlige».[13]

Studier har vist at folks tillit til et samfunn har betydning for økonomisk vekst, og at høy grad av tillit bidrar til økonomisk vekst.[14] Arbeidsgiverforeningen Spekter mener at digitale sårbarheter på samfunnsnivå og økte kostnader ved hendelser over tid kan påvirke denne nødvendige tilliten mellom innbyggere og myndigheter/institusjoner. Kunder og brukere vil kunne akseptere at hendelser skjer, men ikke at selskapene mangler forberedelser og evne til effektiv håndtering.

Tillit som grunnmuren for digitalisering har slått sprekker de siste årene. Siden Snowdens avsløringer i 2013 har hele verden hatt oppmerksomhet rettet mot myndighetenes tilgang til personopplysninger. Det utløste en stor offentlig debatt om overvåking, teknologi og personvern. Avsløringene førte også til en bredere debatt om

[13] Meld. St. 23 (2012–2013) *Digital agenda for Norge – IKT for vekst og verdiskaping.*

[14] Meld.St. 39 (2012–2013): *Mangfold av vinnere.*

Boks 23.4 NY Warrant-saken

NY Warrant-saken er en pågående rettssak knyttet til en tvist om amerikanske myndigheters rett til å hente inn data utenfor landet. Saken gjelder en rettslig ransakelsesordre i en narkotikasak, der Microsoft ble pålagt å utlevere kundeinformasjon knyttet til en e-postkonto fra et datasenter i Dublin, Irland. Microsoft nektet å etterkomme ransakelsesordren, idet informasjonen er lagret utenfor amerikansk territorium, og viste til gjeldende internasjonale prosedyrer for utlevering av data mellom land, herunder avtalen mellom USA og Irland om utlevering av data (Mutual Legal Assistance Treaties, MLAT). Microsoft er i to rettsinstanser pålagt å utlevere informasjonen. Dommen er anket og under behandling. I tillegg til myndighetene i Irland har en rekke selskaper tatt ut stevning til støtte for Microsoft, herunder Apple, Amazon, Cisco, AT&T, eBay, Verizon, Harvard, Stanford, US Chamber of Commerce, the National Association of Manufacturers, ABC, CNN, Fox News og the Guardian, for å nevne noen. Saken har vakt politisk interesse også i Norge, der det er vist til at utfallet av saken kan få store konsekvenser for folks person- og rettsvern i EU og Norge. I Finland har justisministeren i et brev fra 2014 til EU-kommisjonen uttrykt bekymring for de potensielle alvorlige konsekvensene utfallet av saken kan få for EU ved at lands direkte tilgang til data lagret i EU gir mulighet for å omgå gjeldende internasjonale prosedyrer (MLAT).

leverandørenes bruk av kundedata og en større diskusjon om balansen mellom nasjonal sikkerhet og personvern. Folks tillit og krav til åpenhet har i senere tid også vært et tema politisk i Norge. For nasjonale og internasjonale leverandører av IKT-produkter og -tjenester er kundens tillit til at selskapet forvalter og sikrer kundens persondata og sensitive virksomhetsdata, helt avgjørende.

23.6.4 IKT-sikkerhet som hinder for verdiskaping?

Det kan være en utfordring å prioritere informasjonssikkerhet i et marked som i økende grad preges av behovet for fellesløsninger og kunders ønsker om økt tilgjengelighet, mobilitet og funksjonalitet, der alle enheter snakker med hverandre. Dette legger press på leverandørene med hensyn til å balansere disse behovene mot personvern og informasjonssikkerhet. Flere virksomheter opplever derfor at de må gjennomføre skadebegrensende eller utbedrende tiltak i ettertid, når produktet allerede er ute i markedet.

Høye etablerings- og driftskostnader i Norge forutsetter at virksomhetene er produktive for å kunne være konkurransedyktige internasjonalt.[15] Det er fremdeles private og offentlige virksomheter som ser på sikkerhetstiltak som en ren utgiftspost og del av en operasjonell risiko. Andre private nasjonale og internasjonale virksomheter ser strategisk på sikkerhet som et rent konkurransefortrinn og som en naturlig måte å ta vare på bedriftens vekstmuligheter på.

Dette reiser også spørsmål om digitalisering og balansen mellom samfunnshensynene sikkerhet og næringsutvikling. Utvalget har spurt flere sentrale aktører om sikkerhetskrav er til hinder for produktivitetsvekst og innovasjon i næringslivet. Utvalget mener det er påfallende få, både offentlige og private myndigheter og interesseorganisasjoner, som har problematisert dette noe videre. Mye kan tyde på at diskusjonen om nødvendigheten av balanse mellom så viktige hensyn i et samfunn ikke har vært særlig fremme verken i den offentlige debatten eller i fagmiljøene.

Utvalget ser noen gryende tegn til diskusjon om dette hos for eksempel KMD og Finans Norge. Ifølge departementet er IKT-sikkerhet ikke det eneste kriteriet når det foretas strategiske valg, men en svært viktig dimensjon. Vekting av IKT-sikkerhet i for stor grad vil etter departementets syn i noen tilfeller kunne hemme produktiviteten.[16] Finans Norge viser til at næringen i vurderingen av mulighetsrommet for næringsutvikling må veie flere hensyn mot hverandre, som for eksempel forretningsdrift/inntjening, taushetsplikt, sikkerhet, kundevennlighet og hensynet til den enkeltes personvern.

Høye nasjonale krav, sammenlignet med internasjonale, kan virke konkurransevridende. På den annen side kan sikkerhetsfokus også bidra til næringsutvikling. Innovasjon Norge har stilt spørsmål om det er realistisk og mulig å skape vekst med de høye sikkerhetskravene som er i Norge. De høye miljøkravene til oljebransjen er

[15] Meld. St. 23 (2012–2013) *Digital agenda for Norge – IKT for vekst og verdiskaping.*

[16] Kommunal- og moderniseringsdepartementet (2015): *Handlingsplan for informasjonssikkerhet i statsforvaltningen (2015–2017)* s. 11.

en medvirkende årsak til at Norge har klart å produsere olje på en miljøvennlig måte og bli verdensledende. En viktig forutsetning for dette er god økonomi og med det tilstrekkelige rammer for å klare å etterleve kravene. Mange av de større teknologiselskapene ser til Norden som et særskilt satsingsområde.

En sterk IKT-sikkerhetsindustri i Norge vil være et positivt bidrag til reduksjon av digitale sårbarheter. Dette vil sikre kompetanse og bidra til oppmerksomhet og kunnskapsspredning i hele det norske samfunnet. Utvalget anbefaler derfor at regjeringen forsterker arbeidet med å se etter virkemidler for å stimulere til næringsutvikling på dette området, eksempelvis gjennom skattepolitikk, tilskuddsordninger og kompetansebygging i dialog med næringslivet.

23.7 Utkontraktering og skytjenester

Utkontraktering og skytjenester kan bidra til økt teknisk IKT-sikkerhet når leverandøren har bedre kompetanse og ressurser enn kunden. Forholdet mellom digitale sårbarheter og næringsutvikling er nærmere behandlet i punkt 23.6 «Næringsutvikling og IKT-sikkerhet».

Hvilke tekniske muligheter som representerer et mulighetsrom for effektivitet, konkurranseevne, innovasjon og IKT-sikkerhet, vil utvikle seg over tid. I dag er det moderne å snakke om skytjenester, men det man nå opplever som siste nytt, kan raskt bli erstattet av andre løsninger som gir andre muligheter og utfordringer.

Næringsliv og offentlig sektor må fortløpende være oppmerksom på hvilke teknologiske muligheter som blir aktuelle, og vurdere fordeler og ulemper samt være villige til omstilling der dette er nødvendig. Det er også viktig at de juridiske rammene fremover settes slik at det er grunnlag for reell tillit mellom næringsliv, innbyggere og myndigheter. I dette ligger at beslutninger om rettslige rammevilkår må tas på grunnlag av realistiske, grundige og troverdige vurderinger.

Gjennomgående vil det være slik at juridiske rammevilkår som kommer til gjennom grundige demokratiske prosesser, har vanskelig for å dekke nye teknologiske tilbud på en god måte. Myndighetene må sikre at norsk lovgivning ikke hindrer økt konkurransekraft ved å gjøre det vanskelig å ta i bruk mer hensiktsmessig og kostnadseffektiv teknologi så lenge det er tilstrekkelige sikre løsninger. Når det gjelder skytjenester, arbeider Kommunal- og moderniseringsdepartementet med en nasjonal strategi for bruk av skytjenester som planlegges lagt frem i løpet av 2015.[17] Også andre departementer arbeider med å finne ut hvordan man skal forholde seg til skytjenester.

Under går vi først kort inn på hva utkontraktering og skytjenester er, før vi ser på det eksisterende juridiske mulighetsrommet og tilhørende rammer. Deretter angir vi noen hovedfunn før vi kommer med forslag til konkrete tiltak.

23.7.1 Hva er utkontraktering – internasjonale forhold

Det finnes ingen entydig definisjon av hva utkontraktering er, men det er en gjengs terminologi for det at et selskap eller en virksomhet inngår en kontrakt med en ekstern leverandør om å levere en vare eller tjeneste i stedet for å utføre dette internt i egen virksomhet. Ulike aspekter av IKT-drift er et område som typisk har vært gjenstand for utkontraktering de siste årene. Det ligger ingen begrensninger på hva som kan utkontrakteres, og det å benytte skytjenester fra en ekstern leverandør er en type utkontraktering.

For de fleste utkontrakteringer gjelder at man øker antall ledd i verdikjeden for de tjenestene man leverer, sammenlignet med om tjenesten hadde blitt utført internt. Ettersom utkontraktering forutsetter en kontrakt med den eksterne tjenesteleverandøren, må den som bestiller utkontrakteringen, ta stilling til om kontrakten i tilstrekkelig grad regulerer de forholdene som tjenesten skal bygge på.

Et særlig fenomen ved utkontraktering er at den eksterne tjenesteleverandøren kan befinne seg i et annet land og under en annen jurisdiksjon enn den som bestiller tjenesten. Bakgrunnen for dette er enkelt nok at IKT-tjenester kan leveres over nettet, og med like god kvalitet som om de som utfører tjenesten, og bestilleren satt i samme land og i samme virksomhet.

I denne sammenheng reises spørsmålet om hva som er konsekvensene av at en del av tjenesten utføres under et annet lands rett. Dette beskrives noe nærmere i avsnittet om hva skytjenester er, og er også behandlet flere andre steder i dette kapittelet. Da slike internasjonale aspekter også henger sammen med Norges internasjonale

[17] Arbeidsgrupperapport 2015, s. 4-5 Kartlegging av hindringer i regelverk for bruk av skytjenester. Dette er et ledd i regjeringens arbeid med å utforme en norsk politikk for bruk av skytjenester forankret i Meld. St. 23 (2012–2013) *Digital agenda for Norge: IKT-politikk for vekst og verdiskapning.* Meldingen viser til at departementet ønsker «å legge til rette for sikker og forutsigbar bruk av slike tjenester innenfor rammene av det norske regelverket.»

forpliktelser og internasjonale rammer, viser vi også til kapittel 10 «Folkerett og internasjonalt samarbeid».

23.7.2 Hva er skytjenester?

Skytjenester er en felles betegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet Internett. Det finnes flere konkurrerende definisjoner av skytjenester. En definisjon fra National Institute of Standards and Technology er at «Skytenester (cloud computing) er en modell som gjør det mulig å få tilgang til et sett konfigurerbare dataressurser (for eksempel nettverk, servere, lagring, applikasjoner og tjenester) som: er lett tilgjengelige over alt, blir levert og priset etter behov (on demand) og kan skaffes raskt og gjøres tilgjengelig med minimalt med administrasjon eller involvering fra tilbyderen».[18] Denne definisjonen omfatter langt flere tjenester enn mange tenker seg. I Norge benyttes i dag skytjenester innen områder som er så ulike som parkeringsvakters overvåking av kommunale parkeringsplasser, administrasjon av HR-data og systemer for administrasjon av ungdomsskoleelevers personopplysninger. Leverandører av skytjenester er ofte store aktører som leverer standardiserte tjenester, men det finnes også mange mindre leverandører.

I tillegg til at bruken av skytjenester øker i privat og offentlig virksomhet, bruker mange forbrukere skytjenester mer eller mindre bevisst – både i privat og i virksomhetsrelatert sammenheng.

Noen eksempler på privat bruk av skytjenester er bildedelingstjenester, Facebook, Dropbox, Instagram og annet. Bruken av slike tjenester reiser mange problemstillinger for private, for eksempel hvem som har tilgang til informasjonen som lastes opp, hvem den distribueres til, og om forbrukeren har mulighet til å kreve den slettet. Her vil utvalget avgrense mot å behandle disse problemstillingene.

Et beslektet forhold er når privatpersoner som er ansatt i en bedrift eller virksomhet, benytter private skytjenester i virksomhetsrelatert sammenheng.[19] Typisk skjer dette ved at en ansatt lagrer virksomhetsrelatert materiale på for eksempel sin private Dropbox-konto for å kunne arbeide videre hjemmefra. Enhver virksomhet må ha retningslinjer og rutiner som setter rammer for ansattes bruk av private skytjenester på en slik måte. Hvordan slike rammer skal utformes, vil avhenge av sensitiviteten til den aktuelle informasjonen. Noe informasjon kan lagres uten omfattende sikkerhetstiltak, mens annen informasjon må sikres grundig.

I noen henseender er det fremdeles uklare juridiske og tekniske forhold ved anskaffelse og bruk av skytjenester. Likevel er databehandlingstjenester fra eksterne tjenesteleverandører teknisk sett ikke noe nytt og har eksistert siden midten av 1900-tallet. De tekniske og juridiske problemstillingene som oppstår ved bruk av tradisjonelle eksterne driftstjenester, er langt på vei de samme også ved bruk av skytjenester. Noen problemstillinger blir imidlertid mer fremtredende ved bruk av skytjenester, særlig når skytjenestene åpner for lagring og behandling av data i utlandet, da det reiser særlige juridiske problemstillinger.

Skytjenestene kan som nevnt ha svært ulik karakter og beskrives på flere måter. Det er vanlig å skille mellom programvare som tjeneste (Software as a Service, SaaS), plattform som tjeneste (Platform as a Service, PaaS) og infrastruktur som tjeneste (Infrastructure as a Service, IaaS). I en SaaS vil tjenesteleverandøren typisk tilby mer programvare og tjenester enn dersom man «kun» leverer en IaaS. Skytjenester kan leveres i form av en offentlig tilgjengelig sky (Public Cloud), en privat tilgjengelig sky (Private Cloud, som benyttes innenfor en bedrift eller et konsern) eller en hybrid sky (Hybrid Cloud, som er en kombinasjon av de to alternativene). Tjenestene kan også leveres fra en server som er plassert hos kunden (On Premises). Hvordan dette organiseres, er i stadig endring. De juridiske og informasjonssikkerhetsmessige problemstillingene vil langt på vei være de samme, uavhengig av tjeneste- eller leveranseform, selv om de konkrete vurderingene og tiltakene som kan og må iverksettes, kan være forskjellige. I noen tilfeller kan man løse sikkerhetsmessige utfordringer ved å velge en kombinasjon av alternativene.

Skyløsninger oppleves som effektive på grunn av enkel tilknytning via en nettleser, fleksibilitet, mobilitetsfrihet og stor skalerbarhet for brukeren. Mange leverandører garanterer god sikkerhetskopiering, og mange tilbyr ulike former for

[18] Peter Mell og Timothy Grace (2011): *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology.* U.S. Department of Commerce, NIST Special Publication 800-145.

[19] Her gås ikke nærmere inn på problemstillinger med såkalt BYOD (Bring Your Own Device), det at ansatte benytter privat IKT-utstyr når man behandler informasjon som tilhører arbeidsgiver. BYOD reiser flere utfordringer knyttet til digital sårbarhet, men de er ikke spesifikt knyttet til utkontraktering eller skytjenester.

krypteringstjenester. Løsningene presenteres ofte som rimeligere enn tradisjonelle løsninger, men dette bildet er ikke entydig,[20] og det er usikkert hvordan det vil utvikle seg over tid. Denne NOU-en går ikke inn på de økonomiske aspektene ved skytjenester.

En leverandør av skytjenester vil ofte ønske å kunne flytte data til den fysiske lokasjonen som er mest datateknisk optimal. Ofte foretas reservelagring/backup av den behandlede informasjonen i flere land/kontinenter av sikkerhetsårsaker, og det er ikke alltid kjent hvilke land dette er, eller hvilke underleverandører som er involvert. Da vil brukeren ikke alltid vite hvor dataene befinner seg. I tillegg kan leverandøren ha servicepersonell som er plassert i mange ulike land. Når data lagres eller er tilgjengelige fra andre land og jurisdiksjoner, reises en rekke juridiske problemstillinger. Det ikke å vite i hvilke land data befinner seg, og fra hvor de aksesseres, er problematisk fordi rettsreglene for hvordan data kan brukes, vil være annerledes i andre lands jurisdiksjoner. Norske myndigheter har ikke sanksjonsmulighet overfor tjenesteleverandører utenfor Norge og EU/EØS.

23.7.2.1 Datatekniske forhold ved skytjenester

Bruk av skytjenester innebærer i utgangspunktet en tilsvarende risiko som ved tradisjonell tjenesteutsetting av IKT-drift, der risiko og sårbarhet er knyttet til valg av leverandører, lokalisering, kommunikasjonskanaler og arkitektur. Da Snowden avslørte at den amerikanske etterretningsorganisasjonen NSA hentet inn store datamengder fra amerikanske selskaper, ble risikobildet endret til også å omfatte om og hvordan myndigheter i det landet serverne står, eventuelt velger å skaffe seg tilgang til informasjonen. Her vises også til at EUs generaladvokat i en ny beslutning har vektlagt dette sterkt i en vurdering av europeiske borgeres personvern. Generaladvokatens beslutning er videre lagt til grunn i EU-domstolens nye avgjørelse om at Safe Harbour-ordningen er ugyldig. Avgjørelsen er noe nærmere omtalt i punkt 23.7.3 om juridiske forhold ved skytjenester.

Noen leverandører tilbyr krypterte løsninger for å trygge informasjonen. For å ha kontroll på kryptert informasjon må man imidlertid være oppmerksom på hvem som har tilgang til krypteringsnøklene. Man må også vurdere om krypteringen er i kraft hele tiden, særlig om den er i kraft når opplysningene skal endres, og ikke bare når de lagres. Det er sannsynlig at løsninger på dette feltet vil utvikle seg raskt fremover, samtidig som det også er et politisk press i flere land på at krypterte løsninger ikke skal være ugjennomtrengelige for offentlige myndigheter.

Fordi mange skytjenester faktureres i forhold til faktisk bruk, er det viktig å sikre at brukeren belastes for reell bruk. Hvordan dette sikres, vil variere i de ulike systemene og kan være vanskelig for kunden å overskue og kontrollere.

Avhengig av det tekniske oppsettet hos den enkelte leverandøren og den enkelte skytjenesten, kan skytjenester være sårbare for nedetid og skifte av leverandør. Å få sine data ut av systemet og inn i et annet system hvis man ønsker å bytte tjenesteleverandør, kan være utfordrende. Det kan også være utfordringer knyttet til at signaler blir forsinket dersom det er lange fysiske strekk mellom brukere og datasentre og datasentre imellom. Enkelte skybrukere har opplevd begrensninger i båndbredden, og det gjenstår å se om båndbredden er tilstrekkelig når flere ting og objekter blir koblet til Internett (tingenes Internett) og disse kommuniserer med hverandre. Dersom mange brukere velger samme leverandør, kan driftsforstyrrelser ramme mange.

Mørketallsundersøkelsen 2014 viser at norske virksomheter har høy grad av tillit til skyleverandørene og leverandørenes evne til å beskytte data, men sikkerhetsbevisstheten er relativt lav.

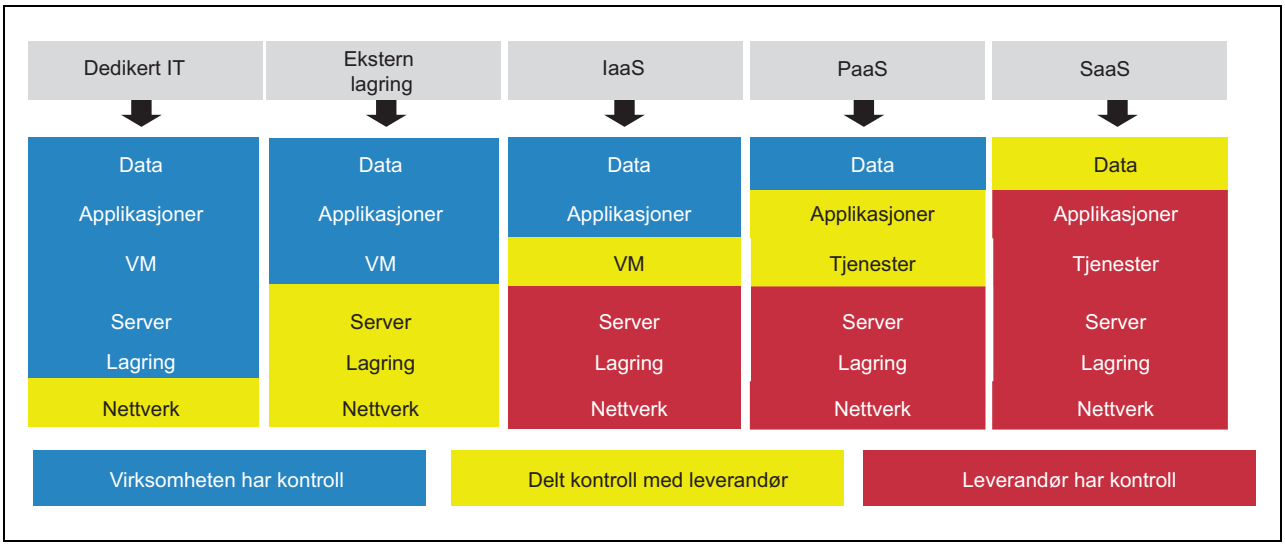
De ulike typene skytjenester gir brukeren ulik grad av kontroll og teknisk innsikt i arkitektur og konfigurasjon av systemene vedkommende bruker (se figur 23.1).

Det finnes en rekke internasjonale standarder for informasjonssikkerhet i skytjenester, og disse videreutvikles fortløpende. Større leverandører er ofte sertifisert i henhold til disse. Slik sertifisering erstatter ikke nasjonalt lovverk. Ofte benyttes tredjepartsrevisjoner som dokumentasjon på at leverandøren har tilstrekkelig og adekvat sikkerhet.[21] Slike revisjoner utføres normalt i henhold til en standard og ikke etter et nasjonalt lovverk, og det kan være forskjeller i reelt innhold mellom standarder og lovverk.

---

[20] KS-undersøkelsen viste at noen kommuner fant at skytjenester ble dyrere enn tradisjonelle løsninger.

[21] Slike tredjepartsrevisjoner skal ikke forveksles med tredjepartsbistand ved lisensrevisjoner som skal verifisere om kunde betaler riktig vederlag for en tjeneste.



Figur 23.1 Kontroll delt mellom virksomhet og leverandør i ulike driftsmodeller.

Kilde: Burton Group (oversatt av NVE).

23.7.3 Juridiske forhold ved skytjenester

23.7.3.1 Utgangspunkt

For en mer detaljert gjennomgang av juridiske utfordringer ved bruk av nettskyløsninger viser vi til en rapport fra Kommunesektorens organisasjon (heretter KS), *Utredning av juridiske forhold ved bruk av nettsky i kommunal sektor – en mulighetsstudie,*[22] og Kommunal- og moderniseringsdepartementets rapport fra en interdepartemental arbeidsgruppe som har vurdert hindringer for bruk av skytjenester i det norske regelverket. I tillegg til rettslige utgangspunkt baserer rapporten fra KS sine anbefalinger på en spørreundersøkelse blant mange kommuner og flere dybdeintervjuer av både brukere og leverandører av skytjenester.

Når personopplysninger skal legges ut i en skytjeneste, er det rettslige utgangspunktet at det er den som er behandlingsansvarlig for personopplysningene, som er ansvarlig for hvordan opplysningene behandles. Dette gjelder også når det brukes en skytjenesteleverandør som utfører en del av databehandlingen. Her vil vi legge til at definisjonen av hva som er en personopplysning, er så vid – se personopplysningsloven § 2 – at dette gjelder svært mange data. For eksempel omfatter det alt fra de fleste IP-numre til datalogger som viser enkeltpersoners bruk av ulike datamaskiner. Dette rettslige utgangspunktet kan være en utfordring for de behandlingsansvarlige, da det å kunne vurdere og ta stilling til om tjenesteleverandørens sikkerhetstiltak er gode nok, forutsetter spesialisert datateknologisk kompetanse.

Det er i tillegg flere regelverk som får anvendelse (ofte samtidig). Her nevnes forvaltningsloven, lov om offentlige anskaffelser og GPA-avtalen, personopplysningsloven, sikkerhetsloven, bokføringsloven og arkivloven. De største juridiske utfordringene er knyttet til arkivloven, bokføringsloven og personopplysningsloven. Under angir vi kort hovedreglene etter arkivloven og bokføringsloven, mens personopplysningslovens bestemmelser tas opp i neste avsnitt.

I arkivloven (LOV-1992–12–04–126) § 9 bokstav b er utgangspunktet at offentlig arkivmateriale ikke kan føres ut av landet uten etter særskilt samtykke fra Riksarkivaren. Så langt har Riksarkivaren ikke gitt samtykke til slik lagring, og arkivaren viser blant annet til manglende mulighet til å foreta revisjon. Dette får stor betydning for muligheten til å benytte skytjenester for arkivverdig materiale. Det kan likevel stilles et overordnet spørsmål ved om denne bestemmelsen, som ble til for over 20 år siden, i dag tar hensyn til en moderne teknologisk utvikling og nye behov. I KMDs rapport om skytjenester angis i punkt 7.1 at lovgiveren må se på endringer i arkivloven, og i punkt 7.3 heter det at såkalte tredjepartsrevisjoner kan være en mulig løsning på hvordan man kan utføre kontroll med systemene. Her nevnes at Datatilsynet har godtatt tredjepartskontroll med lagringsfasiliteter som vitnemål om at sikkerheten i mange tilfeller er god nok. KMDs interdepartementale arbeidsgruppe trekker også frem at det

[22] KS, FoU (2015): *Utredning av juridiske forhold ved bruk av nettsky i kommunal sektor – en mulighetsstudie.* Utarbeidet av Advokatfirmaet Føyen Torkildsen.

bør tas initiativ til å harmonisere tilsynspraksis når det gjelder data lagret i skytjenester.

I henhold til bokføringsloven § 13 annet ledd skal som hovedregel regnskapsmaterialet oppbevares i Norge. Dette begrenser muligheten til å bruke skytjenester der leverandørene ikke har servere plassert i Norge. Det finnes imidlertid enkelte unntak: Bokføringsmateriale kan oppbevares i Danmark, Sverige, Finland og Sverige samt i andre land etter dispensasjon fra Skattedirektoratet. Til tross for unntakene vil bokføringsloven ofte være til hinder for bruk av enkelte typer skytjenester. Noe av grunnen til det er at de store leverandørene ofte ikke tilbyr mulighet for å oppbevare opplysningene i EØS-landene som er nevnt ovenfor, men på servere andre steder i verden. I tillegg er Skattedirektoratet restriktive med å gi dispensasjon. KMDs interdepartementale arbeidsgruppe trekker frem at det bør tas initiativ for å utvide antall land der man tillater lagring av bokføringsdata.

23.7.3.2 Særlig om skytjenester i og utenfor EU/EØS-området i henhold til personvernregelverket

Mange skytjenester leveres av store internasjonale aktører, og de legger vekt på å ha et nettverk som er tilgjengelig over hele verden. Som nevnt er det vanlig at den lagrede informasjonen flyttes rundt i leverandørens nett. Dersom det ikke foreligger geografiske begrensninger i utkontrakteringsavtalen, vil slik flytting kunne skje over landegrenser og på tvers av kontinenter. Det er også vanlig at leverandørens servicepersonale som kan aksessere opplysningene, er lokalisert i mange land. Da vil data, ofte personopplysninger, overføres over landegrenser. I personopplysningloven er det detaljerte regler for overføring av personopplysninger over landegrensene. I denne sammenhengen må man huske at det er den behandlingsansvarlige (i Norge) som er ansvarlig for forvaltningen av opplysningene, selv om en tjenesteleverandør (databehandler) velger sikkerhetstiltak og hvor dataene fysisk skal oppbevares.

I personopplysningsloven § 29 heter det:

> «Personopplysninger kan bare overføres til stater som sikrer en forsvarlig behandling av opplysningene. Stater som har gjennomført direktiv 95/46/EF om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, oppfyller kravet til forsvarlig behandling.»

Alle land innenfor EØS/EU anses som følge av dette å ha et tilstrekkelig beskyttelsesnivå for behandling av personopplysninger. I den grad en norsk behandlingsansvarlig virksomhet overfører personopplysninger til for eksempel en engelsk databehandler/leverandør av skytjenester, behøves derfor ikke et særskilt hjemmelsgrunnlag for selve overføringen. Det er tilstrekkelig at behandlingen reguleres av en tilfredsstillende databehandleravtale, eller at klausuler om databehandling tas inn i tjenesteavtalen. Dette gjelder på samme måte som når en norsk leverandør av skytjenester skal behandle personopplysninger på vegne av den behandlingsansvarlige.

Et spesielt viktig punkt i databehandleravtaler om skytjenester er reguleringen av hvordan eventuelle underleverandører skal benyttes. Leverandører av skytjenester vil som nevnt i visse tilfeller ønske å benytte flere lokasjoner. Ofte vil disse lokasjonene tilhøre underleverandører. Når slike underleverandører har egne organisasjonsnumre, er de å anse som selvstendige underleverandører selv om de tilhører samme konsern som tjenestetilbyderen.

Det vil derfor kunne oppstå tilfeller der en databehandler innenfor EU/EØS benytter seg av underleverandører (underdatabehandlere) både innenfor og utenfor EU/EØS. Når opplysningene er tilgjengelige for en leverandør eller underleverandør utenfor EU/EØS, må situasjonen håndteres i henhold til reglene om overføring av personopplysninger til land utenfor EU/EØS.

Europakommisjonen mener at nærmere bestemte land utenfor EU/EØS oppfyller kravene til å sikre forsvarlig behandling av personopplysningene. For disse landene gjelder i utgangspunktet dermed de samme reglene som for overføring innenfor EU/EØS. Det samme gjaldt, frem til EU-domstolens avgjørelse som er omtalt nedenfor, ved overføring til amerikanske bedrifter som er tilsluttet Safe Harbour-avtalen.

Safe Harbour-avtalen er en egen avtale mellom EU og USA fra 2000 som utelukkende gjelder overføring av personopplysninger fra EU/EØS-området til amerikanske bedrifter. Det er en selvsertifiseringsløsning der amerikanske bedrifter erklærer at de oppfyller en rekke personvernkrav som er angitt i Safe Harbour-avtalen. Når denne NOU-en skrives, er det nye forhandlinger mellom EU og USA om innholdet og forvaltningen av Safe Harbour fordi en intern undersøkelse i USA avdekket store mangler i forvaltningen av personopplysninger hos mange Safe Harbour-bedrifter.

Samtidig har som nevnt EU-domstolen kommet med en avgjørelse som fastslår at Safe Har-

bour-avtalen er ugyldig fordi europeiske borgeres personvernrettigheter ikke er godt nok ivaretatt i USA. Bakgrunnen for beslutningen er Snowdens avsløringer om NSAs omfattende overvåking, som domstolen mener er i strid med europeiske personvernrettigheter og EMK. Avgjørelsen legger også vekt på at europeiske borgere ikke har noen rettslig mulighet til å gripe inn eller bestride NSAs innhenting av informasjon. Avgjørelsen er svært prinsipiell og har skapt store personverndebatter både i EU og i USA. Dommen er samtidig utfordrende fordi dens hovedpoeng om at etterretningens overvåking av informasjon kan true personvernet, medfører at det blir stilt spørsmål ved om selve grunnlaget for internasjonal flyt av personopplysninger er godt nok. Dette har store potensielle konsekvenser for de næringslivsinteressene som en slik flyt er ment å ivareta. Som følge av dommen reises det i personvernmiljøer også spørsmål om USA står i en særstilling når det gjelder de underliggende spørsmålene om etterretningers avlytting av informasjon, eller om tilsvarende spørsmål gjør seg gjeldende også for andre nasjoner. Denne NOU-en går ikke nærmere inn på konsekvensene av dommen, da de foreløpig ikke er avklart.

Et annet og beslektet spørsmål, uavhengig av hvor serveren står rent geografisk, er: «Hvem eier selskapet som eier serveren?» Noen lands myndigheter stiller krav til selskaper i sitt eget land når det gjelder retten til å få tilgang til data i selskapets systemer. For amerikanske myndigheters krav om innsyn i data som lagres hos amerikanske selskaper utenfor USA, viser vi til punkt 23.6.3 «Tillit bør være en forutsetning for digitaliseringen».

For bruk av skytjenester som lagrer og behandler informasjon i land utenfor EU/EØS-området, og som ikke er etablert i de landene Europakommisjonen har godkjent, eller bruker underleverandører fra godkjente land, gjelder egne regler. Hovedtrekkene i disse er som beskrevet under.

Personopplysningsloven § 30 første ledd angir en rekke mulige grunnlag for slik overføring, for eksempel at den registrerte samtykker i overføringen. Det å benytte samtykke som grunnlag er imidlertid ikke særlig hensiktsmessig verken for den behandlingsansvarlige eller for databehandleren, ettersom samtykket kan trekkes tilbake når som helst. I praksis er det derfor ofte unntaket i personopplysningsloven § 30 annet ledd om at Datatilsynet kan tillate overføring til tredjeland dersom det gis «tilstrekkelige garantier for vern av den registrertes rettigheter», som benyttes som hjemmel. Dersom man benytter en av EUs standardkontrakter som grunnlag for overføringen til en databehandler i tredjeland, er det tilstrekkelig å varsle Datatilsynet om overføringen ved å sende inn en kopi av en signert standardavtale.[23]

En utfordring med standardvilkårene er at de ikke kan benyttes direkte i situasjoner der personopplysninger skal overføres fra en EU/EØS-basert behandlingsansvarlig til en EU/EØS-basert databehandler og derfra til en underdatabehandler i et tredjeland. Denne begrensningen går frem av vedtaket som standardvilkårene bygger på, samt av selve standardvilkårene. I en situasjon som nevnt over identifiserer Artikkel 29-gruppen følgende alternative fremgangsmåter:[24]

1. Det inngås direkte kontrakt mellom den behandlingsansvarlige i EU/EØS og underdatabehandleren i tredjelandet.
2. Den behandlingsansvarlige gir databehandleren i EU/EØS et klart mandat til å bruke EUs standardvilkår på vegne av den behandlingsansvarlige og i den behandlingsansvarliges navn.
3. Det inngås «ad hoc-kontrakter» (det vil si ikke-standardvilkår som ivaretar prinsippene i standardvilkårene).

Ved grenseoverskridende bruk av databehandler(e) kreves altså en grundig tilnærming for å kunne opprette et juridisk dekkende avtaleverk etter europeiske personvernregler. En av forutsetningene for å kunne gjøre dette er åpenhet fra databehandlerens side når det gjelder hvilke underleverandører (underdatabehandlere) som benyttes i forbindelse med leveransen, hvor disse befinner seg, og hvilken rolle de har i forbindelse med databehandlingen. EU arbeider nå med et nytt regelverk for personvern, og det er i skrivende stund ikke kjent hvordan detaljene i dette vil bli, men det er etter det utvalget er kjent med, grunn til å tro at hovedprinsippene for overføring av personopplysninger til utlandet vil forbli omtrent som de er i dag, særlig for overføring av personopplysninger utenfor EU/EØS.

---

23 Dette gjelder dersom man benytter modellavtalen for overføring til databehandler. Dersom man bruker modellavtalen for overføring til en selvstendig behandlingsansvarlig i USA, må Datatilsynet godkjenne avtalen, avtalen skal da ikke bare sendes inn til tilsynet.

24 EU (2010): *Article 29 Data Protection Working Party*. 00070/2010/EN WP 176.

23.7.3.3 Særlig om sikkerhetsgradert informasjon

Dersom virksomheten behandler informasjon som er underlagt sikkerhetslovens bestemmelser, er det flere forhold som kan begrense bruken av skytjenester. Sikkerhetsgradert informasjon er informasjon som skal merkes med BEGRENSET, KONFIDENSIELT, HEMMELIG eller STRENGT HEMMELIG i henhold til sikkerhetsloven §§ 3 og 11. Hvis en løsning for skytjenester vil involvere overføring av sikkerhetsgradert informasjon og å gi leverandøren tilgang til slik informasjon, kommer sikkerhetsloven med forskrifter til anvendelse. Rent juridisk vil det være vanskelig å benytte internasjonale skytjenester for denne typen informasjon fordi det som hovedregel forutsetter at det involverte personalet kan sikkerhetsklareres i Norge.[25] Videre skal virksomheter som behandler sikkerhetsgradert informasjon elektronisk, ha sikkerhetsgodkjente informasjonssystemer for håndtering av denne typen informasjon.[26] [27]

23.7.4 Observasjoner og funn

Utvalget mener at ressurssterke tilbydere av skytjenester i mange tilfeller kan tilby en bedre teknologisk sikkerhet enn mange mindre virksomheter kan klare selv. Bakgrunnen for dette er at ressurssterke tilbydere av skytjenester har tilgang på spesialisert IKT-sikkerhetskompetanse som kan sørge for adekvate sikringstiltak. Imidlertid er utbudet av leverandører og tjenester svært uensartet, og man kan derfor ikke si at dette gjelder generelt uten å ha foretatt en vurdering av både den aktuelle tjenesten og den aktuelle leverandøren. Viktige momenter er følgende:

- Skytjenester kan ikke omhandles under ett. Den enkelte skytjeneste må vurderes konkret ut fra den aktuelle tjenesten og den aktuelle leverandøren.
- Sikkerheten må vurderes i forhold til ulike aspekter og risikoer, for eksempel vil tilgjengelighet og rutiner for sikkerhetskopiering ofte være svært gode ved skytjenester, samtidig som skytjenester og transport på offentlige nett kan medføre en større risiko for lekkasjer og tapping enn ved lokal lagring.
- Det kan være vanskelig for den jevne brukeren av slike tjenester å foreta tilstrekkelige vurderinger. Mange vil ikke ha nødvendig teknisk kompetanse til å foreta slike vurderinger, og for internasjonale skytjenester med lokasjoner og tjenester i andre land kan det være praktisk vanskelig å gjennomføre en konkret risikovurdering.

Det er en utfordring i det digitale samfunnet at informasjon og data flyter så fritt mellom ulike land med tilhørende ulike rettslige rammer for hvordan informasjon og data skal håndteres.[28] Mens man før den internasjonale digitale tidsalder kunne anta at informasjon og data som ble brukt i Norge, ble lagret i Norge og håndtert i henhold til norske rettsregler, er dette ikke alltid lenger tilfellet. Det er ikke lett for brukerne av informasjon eller for dem som er registrert, å oppfatte hvor informasjonen er lagret.

For brukere av skytjenester er det ofte en utfordring å sørge for at avtalen med leverandøren er i samsvar med norsk lovgivning, slik at gjeldende krav i norsk lovgivning til behandling av personopplysninger og sikkerhet til enhver tid kan oppfylles. I KS-rapporten pekes det på at noen brukere opplever at sterke skytjenesteleverandører bruker sin markedsposisjon og krever sine standardvilkår lagt til grunn uten at det gis noe realistisk rom for forhandlinger eller endringer. Også regjeringens interdepartementale gruppe peker på at standardkontraktene er en utfordring for bruk av skytjenester. Videre må det tas hensyn til at eierstrukturen i private selskaper er utsatt for endringer, typisk gjennom oppkjøp og salg, som kundene har liten mulighet til å påvirke. Et selskap kan få nye eiere med en annen nasjonalitet – med de komplikasjoner det medfører. Konsekvenser av dette er følgende:

- Brukere av skytjenester må vurdere om opplysningene de ønsker å legge i skyen, er sårbare dersom de kommer utenfor norsk jurisdiksjon, og veie følgene av dette opp mot fordelene ved tjenesten.
- Mange av de kontraktsvilkårene som i dag tilbys for skytjenester, er kompliserte, og det kan være vanskelig å finne ut i hvilke land dataene faktisk vil bli lagret og behandlet. Det er avgjørende at dette kartlegges. I en slik kartlegging

[25] Innenfor NATO og EU er det muligheter for deling av noe gradert informasjon.

[26] KS, FoU (2015): *Utredning av juridiske forhold ved bruk av nettsky i kommunal sektor – en mulighetsstudie.* Utarbeidet av Advokatfirmaet Føyen Torkildsen.

[27] Kommunal- og moderniseringsdepartementet (2015): *Kartlegging av hindringer i regelverk for bruk av skytjenester.* Interdepartemental arbeidsgruppe.

[28] Her nevnes at Russland nylig i 2015 har iverksatt en lov som innebærer at internettselskaper må flytte data om russiske borgere til servere plassert på russisk jord.

må det ikke bare tas hensyn til lokasjon for hovedlagring, men også til hvor backup lagres, hvor service foretas fra, og i hvilke land underleverandører er plassert fysisk. Det bør foretas landrisikovurderinger (vurdering av et lands politiske stabilitet og korrupsjonsindeks) for å avgjøre om behandling i det enkelte land er ønskelig.
- Enkelte typer materiale bør oppbevares innenfor norsk territorium og jurisdiksjon, særlig gjelder dette gradert informasjon.
- Hvorvidt en bedrift eller virksomhet bør benytte skytjenester, avhenger, i tillegg til en vurdering av skytjenesteleverandørens kvaliteter, av hvilken informasjon man ønsker å verne. Dersom tilgjengelighet til opplysningene er det viktigste, vil skytjenester ofte være hensiktsmessig. Hvis absolutt konfidensialitet er det viktigste, kan konklusjonen bli motsatt. Det siste kan være aktuelt i tilfeller der industrispionasje og lekkasjer kan få store økonomiske konsekvenser.
- Det vil antagelig ofte være slik at en bedrift eller virksomhet vil kunne legge noe av sin informasjon ut i skyen, mens annen informasjon beholdes lokalt/internt. Det kan finnes opplysningstyper som av konkurransehensyn eller sensitivitetshensyn ikke bør legges i en skytjeneste, selv om det er lovlig å legge dem der.

23.7.5 Vurderinger og tiltak

Utvalget mener at regjeringens påbegynte arbeid med en gjennomgang av regelverket som omfatter skytjenester og utkontraktering for å fjerne unødige hindringer, rydde opp i lovtekniske uklarheter og legge til rette for sikre løsninger, er viktig for å ta i bruk ny teknologi på en forsvarlig og trygg måte.

Når det gjelder arbeidet med å se på hvilken informasjon som skal tillates lagret hvor, særlig vedrørende arkivlovens og bokføringslovens bestemmelser, *mener utvalget at det finnes tre alternative kategorier regjeringen må ta stilling til: 1) informasjon som kun bør lagres i Norge, 2) informasjon som kan lagres i utlandet, men som må kunne flyttes tilbake til Norge ved særlige behov og på bestemte vilkår, og 3) informasjon som kan lagres i utlandet uten vilkår.* Antagelig er omfanget av informasjon i kategori 2 størst. Hvilken informasjon dette er i praksis, vil sektorene selv være best i stand til å vurdere.

Utvalget støtter anbefalingen fra KMDs interdepartementale gruppe om at det tas initiativ til å harmonisere tilsynspraksis når det gjelder data lagret i skytjenester, så langt det er mulig. *Det bør gjennomføres en felles utredning på tvers av sektorene, slik at spørsmålene får en overordnet behandling og det kan etableres en felles praksis – dette særlig av hensyn til virksomheter som forholder seg til flere ulike tilsynsorganer.* Gjennomgangen bør omfatte praktiseringen av og behovet for stedlig tilsyn hos kontrollobjektene, og en vurdering av om tilsynenes behov kan løses på andre måter.

KMDs interdepartementale gruppe anbefaler at man ser nærmere på hvordan tredjepartsrevisjoner[29] kan benyttes for å kvalitetssikre skytjenester, og at det gjennomføres en felles utredning av dette.[30] *Lysneutvalget stiller seg bak behovet for en slik redegjørelse, og mener at den ikke bare bør være interdepartemental, men nasjonal, og omfatte behovet i både offentlig og privat sektor. Dette arbeidet må i tillegg gjøres i en internasjonal kontekst, da Norge antagelig vil kunne forhandle frem bedre løsninger i samarbeid med for eksempel EU eller standardiseringsorganisasjoner.* Det er viktig at tredjepartsrevisjoner av serverparker er troverdige, og man bør blant annet se nærmere på hvordan slike revisjoner bestilles, hvem som utfører dem, etter hvilke krav revisjonene utføres, og hvordan de honoreres.

Særmerknad fra utvalgsmedlem Kristine Beitland

Utvalgsmedlem Kristine Beitland vil bemerke at det er viktig at Justis- og beredskapsdepartementet i politikkutformingen knyttet til digitale sårbarheter og skytjenester, ser muligheten teknologien gir for å øke sikkerheten, og ikke utelukkende fokuserer på juridiske hindringer for bruk av skytjenester. Beitland understreker behovet for at Justis- og beredskapsdepartementet i samråd med Nærings- og fiskeridepartementet og Kommunal- og moderniseringsdepartementet, før en endelig politikk utformes, inviterer til en bredere tverrdepartemental vurdering av næringsutvikling og økt produktivitet ved utnyttelsen av teknologiens muligheter som begrenser sårbarheter og øker sikkerheten både for virksomhetene og nasjonalt. Målet må være å legge til rette for økt konkurransekraft gjennom sikker og forutsigbar bruk av skytjenester innenfor rammene av norsk lov.

---

[29] Med tredjepartsrevisjoner menes en sikkerhetsmessig gjennomgang av lokasjon og oppsett som benyttes av skytjenesteleverandøren, ikke lisensrevisjon av tredjepart.

[30] Se punkt 23.7. «Juridiske forhold ved skytjenester».

23.8 Regulering av kryptografi

Politi og etterretning har legitime behov for avlytting av kommunikasjon. I økende grad gjør bruk av kryptografi tradisjonell avlytting umulig. Internasjonalt har det, både fra politi, etterretning og politikere, vært uttrykt et sterkt ønske om å gjøre noe med dette. Kryptografi er nødvendig for å beskytte kommunikasjon. Den enkelte borger, virksomheter og myndigheter er avhengige av trygg kommunikasjon.

Programvare for kryptografi er i dag lett tilgjengelig og lett å lage for programmeringskyndige. Det er svært enkelt å bygge småskalasystemer for kommunikasjon som hindrer tradisjonell avlytting. Når det ikke finnes teknologiske hindringer, vil ikke regulering eller forbud i seg selv hindre kriminelle i å bruke kryptografi.

Formålet med regulering av eller forbud mot kryptografi er derfor ikke å hindre uærlige aktører i å bruke kryptografi, men å gjøre det vanskeligere for dem å bruke vår kommunikasjonsinfrastruktur. Idéen er at om bare uærlige aktører bruker kryptografi, kan vi finne uærlige aktører ved å finne bruk av kryptografi.

Analysen avhenger av hvordan kryptografi forbys eller reguleres. Tradisjonelt har det vært tre måter å regulere kryptografi på: 1) ved å forby all kryptografi, 2) ved å forby sterk kryptografi, det vil si kryptografi som kan motstå ressurssterke aktører, 3) å påby bruk av kryptografi med bakdører, det vil si at myndighetene skal kunne dekryptere ved behov.

1) Forbud mot kryptografi har vært forsøkt. Det er svært negativt for ærlige brukere, siden de ikke lenger kan kommunisere konfidensielt og alt kan avlyttes.

   Ideen bak et forbud er at myndighetene overvåker offentlige nettverk for å lete etter krypterte data. Det typiske kjennetegnet ved chiffertekst er at den ser svært tilfeldig ut. Steganografi er navnet på den underdisiplinen av kryptografi som dreier seg om å skjule kommunikasjon. Steganografi er ikke er så lett som man kanskje skulle tro, men det er rimelig å tro at man kan få etablert skjulte kommunikasjonskanaler, dog med liten båndbredde.

2) Svak kryptografi vil være svært negativt for ærlige brukere, siden hele poenget med svak kryptografi er at den skal kunne brytes. Dermed kan ikke svak kryptografi sikre konfidensiell kommunikasjon.

   Det var lenge forbudt å eksportere sterk kryptografi fra USA. Forbudet gjorde livet vanskeligere for amerikansk IKT-industri og resulterte i dårligere sikkerhet i IKT-systemer både innenfor og utenfor USA. Det er grunn til å tro at dette forbudet bidro til etableringen av kryptoindustri utenfor USA.

   Et forbud mot sterk kryptografi vil være svært vanskelig å håndheve, fordi den eneste måten å avgjøre om det er brukt sterk eller svak kryptografi på, er å forsøke å dekryptere, og uærlige brukere kan dobbeltkryptere og gjemme sterk kryptografi inni svak kryptografi. Dermed kan uærlige aktører mer eller mindre fritt bruke sterk kryptografi.

3) Kryptografi med bakdører har vært forsøkt i USA. Det såkalte Clipper-systemet i USA hadde en bakdør som skulle la myndighetene bryte kryptografien ved behov. Systemet virket aldri etter hensikten fordi det kunne saboteres, slik at myndigheten ikke kunne dekryptere.

   Kryptografi med bakdør er svært komplisert å lage og kostbart å bruke (nettverket må hele tiden sjekke at informasjonen som formidles, kan dekrypteres). Uærlige aktører kan fortsatt dobbeltkryptere, først med kryptografi uten bakdør, deretter med kryptografi med bakdør.

   En bakdør gjør det prinsipielt umulig å bruke en del viktige kryptoteknikker, noe som vil medføre alvorlig sårbarhet i IKT-infrastrukturen vår. Misbruk av bakdøren er en annen alvorlig sårbarhet. I tillegg er spørsmålet hvilke myndigheter som skal kunne bruke bakdøren. Er det norske myndigheter? Er det allierte staters myndigheter? Er det andre staters myndigheter?

   Det er altså svært vanskelig – kanskje umulig – å lage et system som samtidig ivaretar legitime behov for beskyttelse og avlytting. Det er rimelig å tro at begrensninger på lovlig bruk av kryptografi vil ramme norske borgere, virksomheter og myndigheter. Slike begrensninger vil ikke vesentlig hindre uærlige aktørers bruk av kryptografi, og de vil dermed heller ikke løse politiets og etterretningstjenestenes problem.

Utvalget vurderer alle disse tre alternativene som uakseptable. Det er dermed utvalgets oppfatning at

1. *bruk av kryptografi ikke skal reguleres eller forbys i Norge*
2. *norske myndigheter bør arbeide aktivt mot regulering eller forbud internasjonalt*

3. *nye etterforskningsmetoder må utvikles for å sikre effektivt politi- og etterretningsarbeid i en verden der mer og mer krypteres.*

Utvalget mener i likhet med NSM[31] at alle offentlige nettsteder bør kommunisere kryptert med innbyggerne. Utvalget mener at private nettsteder også bør kommunisere kryptert med brukerne sine.

[31] Nasjonal sikkerhetsmyndighet (2015): *Sikkerhetsfaglig råd.*

Del V
Økonomiske og administrative konsekvenser

Kapittel 24
Økonomiske og administrative konsekvenser

Tidligere i rapporten er det vist til et estimat der Norge årlig taper cirka 20 milliarder kroner på grunn av IKT-kriminalitet alene. Imidlertid er det vanskelig å estimere de potensielle økonomiske tapene knyttet til digitale sårbarheter. Dette problemet har blitt adressert i et arbeid i regi av World Economic Forum, der det påpekes at mangel på felles aksepterte metoder for å kvantifisere cybertrusler er et vesentlig hinder for å ta informerte strategiske beslutninger knyttet til optimalt investeringsnivå.[1] En hovedgrunn til det er at de teknologiske endringene har kommet raskt på oss. Det er derfor stor mangel på validerte metoder for å estimere det økonomiske tapspotensialet som ligger i de digitale sårbarhetene, og dermed også utfordrende å skulle måle konsekvenser av svikt i IKT sett opp mot effekten av tiltak. Utvalget omtaler denne utfordringen som del av forslaget til en IKT-kompetansestrategi (se kapittel 19 «Kompetanse»).

Utvalget peker på at en rekke sektorvise tilsyn må øke sin kapasitet og kompetanse, gitt blant annet den teknologiske utviklingen i sektorenes verdikjeder. Utvalget har gjort seg den overordnede betraktning at digitaliseringen av samfunnet har ført til at tilsynsoppgavene har endret seg, og at det kreves stor teknologisk innsikt for å forstå kompleksiteten innenfor ansvarsområdet til hvert tilsyn. Det vil være forskjeller mellom sektorene, og utvalget har ikke analysert situasjonen i hvert enkelt tilsyn i detalj. Det enkelte departement må i samarbeid med tilsynene vurdere om en styrking av IKT-sikkerheten skal foregå ved omdisponering av ressurser, eller om det bør tilføres ekstra midler for å håndtere denne utviklingen.

Sektormyndighetene har et ansvar for å ivareta IKT-sikkerheten i hver enkelt sektor. Gitt de gjensidige avhengighetene mellom samfunnsfunksjonene og behovet for å legge til rette for samvirke på tvers av sektorer mener utvalget at Justis- og beredskapsdepartementet må styrkes i sin samordningsrolle. Samordningsrollen er utfordrende, og utvalget mener at Justis- og beredskapsdepartementet må ha tilstrekkelige virkemidler til å utøve rollen. En styrking innebærer at departementet blir tilført ressurser i form av personell for å kunne ha en effektiv og hensiktsmessig gjennomføringsevne på IKT-sikkerhetsområdet. Utvalget har ikke gjennomført en detaljert analyse av dette ressursbehovet, og anbefaler derfor at Justis- og beredskapsdepartementet utreder behovet videre. Utvalget bemerker spesielt at dette tiltaket har nær sammenheng med tiltakene knyttet til en klargjøring av Justis- og beredskapsdepartementets rolle og styrking av virkemidlene.

Utvalget anbefaler at det etableres en overordnet nasjonal kompetansestrategi innen IKT-sikkerhet for å sikre en langsiktig oppbygging av IKT-sikkerhetskompetanse. Utvalget har videre spesifisert hvilke prioriterte områder en kompetansestrategi bør inneholde. Mange av disse prioriteringene kan gjennomføres innenfor eksisterende rammer. Enkelte prioriteringer vil imidlertid kunne medføre behov for økte ressurser, blant annet i form av en økning av Justis- og beredskapsdepartementets FoU-midler og oppbygging av mastergradstilbud på de stedene som har mange IKT-studenter. De økonomiske og administrative konsekvensene av oppfølgingen av en nasjonal kompetansestrategi må utredes i samarbeid med de berørte sektormyndighetene.

Norge ligger i verdenstoppen når det gjelder bruk av digital teknologi og Internett. Dette krever en robust ekominfrastruktur. Utvalget foreslår at det etableres tiltak som reduserer kritikaliteten av Telenors kjernenett. Tiltaket er estimert til om lag 575 millioner kroner over ti år.[2] I tillegg vil det

[1] World Economic Forum (Januar 2015): *Partnering for Cyber Resilience Towards the Quantification of Cyber Threats.*

[2] Estimerte kostnader er basert på en investeringskostnad på 400 millioner kroner og årlige drifts- og vedlikeholdskostnader, som er anslått å være 2,5 prosent av investeringssummen, i tillegg til 4 prosent diskonteringsrate og en skattefinansieringskostnad på 20 øre per krone. Se elektronisk vedlegg: Konsekvensutredning – Alternativer for styrket robusthet i landsdekkende kjernenett.

påløpe kostnader knyttet til leie av linjekapasitet. Her er det imidlertid usikkerhet knyttet til estimatet – både når det gjelder antall kilometer som trengs, og pris per kilometer. Samlet samfunnsmessig tap ved et bortfall av kjernenettets funksjonalitet er estimert til 2 milliarder kroner per dag, i tillegg til store, alvorlige konsekvenser for liv og helse. Utvalget mener konsekvensene av et utfall av ekomnettet er så store at risikoen ved ikke å etablere tiltak er uakseptabel.

Innenfor norsk romvirksomhet er sårbarheter i et verdikjedeperspektiv en sentral problemstilling. De fleste samfunnsområder er i stor grad avhengige av satellittbaserte tjenester. I dag har vi ingen nasjonal overordnet myndighet som har ansvar for å forvalte dette, og utvalget anbefaler at det tydeliggjøres et myndighetsansvar for norsk romvirksomhet. Utvalget anbefaler at det opprettes en mindre enhet under enten Nkom eller DSB, bestående av om lag fem stillinger. Fem stillinger er estimert til om lag 5,5 millioner kroner per år.

Utvalget anbefaler samlokalisering av responsmiljøer for å forbedre den nasjonale operative evnen til å avdekke og håndtere digitale angrep. Etter utvalgets vurdering må det legges bygningsmessig til rette for at de som ønsker samlokalisering, kan inngå i ett felles bygg. Bygget skal være egnet for stor grad av liaisonering for dem som av ulike årsaker ikke kan delta i eller ikke ønsker en permanent samlokalisering. De økonomiske og administrative konsekvensene må konkretiseres nærmere i arbeidet med å legge til rette for samlokalisering.

Utvalget støtter Justis- og beredskapsdepartementets forslag om å opprette et nytt nasjonalt senter for å forebygge og etterforske kompleks og grenseoverskridende IKT-kriminalitet. Utvalget støtter videre, i tråd med Politidirektoratet, at politidistriktenes fagmiljøer blir betraktelig styrket. Utvalget har ikke gjort egne beregninger, men er kjent med at Justis- og beredskapsdepartementet arbeider med løsninger og kostnadsestimater for å opprette et senter og styrke politidistriktenes fagmiljøer.

Utvalget er av den oppfatning at IKT-situasjonen i politiet er kritisk, og at Justis- og beredskapsdepartementet bør iverksette tiltak for å sikre politiet et teknologiløft. Utvalget har ikke vurdert om et teknologiløft skal gjennomføres ved omdisponering av ressurser, eller om det bør gis ekstra midler til dette.

Utvalget ser behov for en styrket nasjonal evne til å detektere hendelser i det digitale rom. Dette vil kreve både engangsinvesteringer og midler til videreutvikling, blant annet for å videreutvikle et sektortilpasset varslingssystem for digital infrastruktur (VDI). Utvalget har ikke gjort egne beregninger, men er kjent med at NSM arbeider med kostnadsestimater for videreutvikling av VDI som en oppfølging av forslaget i *Sikkerhetsfaglig råd*.

Enkelte av utvalgets anbefalinger krever nærmere utredning og konsekvensvurderinger. Eksempler på dette er behovet for å utrede en nasjonal cyberreserve for digital hendelseshåndtering og å utvikle felles sikringstiltak mot sofistikerte angripere.

Utvalget er bedt om å komme med minst ett forslag basert på uendret ressursbruk. Utvalget anbefaler en rekke tiltak for å redusere den digitale sårbarheten og være bedre rustet til å møte den antatte teknologiske utviklingen fremover. Mange av tiltakene som foreslås, handler om økt samarbeid på tvers av ansvars- og kompetanseområder, både myndigheter imellom og mellom myndigheter og eiere av kritisk infrastruktur og kritiske samfunnsfunksjoner. Etter utvalgets vurdering krever ikke disse tiltakene ekstra bevilgninger. Utover dette mener utvalget at det må gjøres en vurdering av hvert enkelt tiltak for å fastslå om de i noen grad kan gjennomføres med uendret ressursbruk. Et tiltak som definitivt vil ha store økonomiske konsekvenser, er det å redusere kritikaliteten til kjernenettet.

Del VI
Vedlegg

Kapittel 25
Vedlegg

25.1 Datagrunnlag

Oversikt over hvem som har gitt skriftlig innspill

Barne-, likestillings- og inkluderingsdepartementet
Forsvarsdepartementet
Helse- og omsorgsdepartementet
Kommunal- og moderniseringsdepartementet
Justis- og beredskapsdepartementet
Kulturdepartementet
Kunnskapsdepartementet
Landbruks- og matdepartementet
Nærings- og fiskeridepartementet
Olje- og energidepartementet
Samferdselsdepartementet
Utenriksdepartementet
Simula
Forsvarets forskningsinstitutt
Forskningsrådet
NUPI
SINTEF
Fylkesmannen i Buskerud
Fylkesmannen i Finnmark
Fylkesmannen i Sogn og Fjordane
Fylkesmannen i Telemark
Fylkesmannen i Vest Agder
Fylkesmannen i Sør-Trøndelag
Altibox/Lyse
DNB
Direktoratet for nødkommunikasjon
Departementenes servicesenter
EVRY
Hafslund
ICE
Nets
Norsk helsenett
Norsk romsenter
Space Norway AS
Statkraft
Statnett
Tampnet
TDC
Tele 2
Telenor
TeliaSonera
Accenture
EY
KPMG
PWC
Steria
mnemonic
BDO
Capgemini
Gartner Consulting
NC-spectrum
DNV GL
Watchcom
KINS
Energi Norge
Finans Norge
FSK
IKT Norge
Norsk olje og gass
Næringslivets sikkerhetsorganisasjon
Spekter
Standard Norge
Statoil
Virke
Brønnøysundregistrene
Helseregistrene i FHI
Kartverket
Norges geologiske undersøkelse
Skattedirektoratet
Datatilsynet
Direktoratet for forvaltning og IKT
Direktoratet for samfunnssikkerhet og beredskap
Finanstilsynet
Garantiinstituttet for eksportkreditt
Helsedirektoratet
Hovedredningssentralene i Sør-Norge og Nord-Norge
Justervesenet
Kystverket
Mattilsynet
Nasjonal sikkerhetsmyndighet
Norges vassdrags- og energidirektorat
Oljedirektoratet

Politidirektoratet
Nasjonal kommunikasjonsmyndighet
Petroleumstilsynet
Sjøfartsdirektoratet
Statens jernbanetilsyn
Forsvarets etteretningshøgskole
Høgskolen i Gjøvik
Høgskolen i Østfold
Universitetet i Agder
Universitetet i Bergen
Universitetet i Oslo
Norges teknisk-naturvitenskapelige universitet
Westerdals
Helse Midt Norge
Helse Nord IKT
Helse Sør-Øst
Helse Vest
Hemit
Kripos
NorSIS
NSB
Statens Vegvesen

Møteliste

Nasjonal sikkerhetsmyndighet
E-tjenesten
Direktoratet for samfunnssikkerhet og beredskap
Forsvarsdepartementet
Cyberforsvaret
Forsvarets logistikkorganisasjon
Forsvarsstaben
Forsvarets sikkerhetsavdeling
Finanstilsynet
Utenriksdepartementet
Samferdselsdepartementet
Kommunal- og moderniseringsdepartementet
Olje- og energidepartementet
Norges vassdrags- og energidirektorat
Statnett
Statkraft
Nasjonal kommunikasjonsmyndighet
Kripos
Petroleumstilsynet
Politiets sikkerhetstjeneste
Datatilsynet
FinansCERT
Telenor
TeliaSonera
ICE
Statsministerens kontor
Direktoratet for forvaltning og IKT
Forsvarets forskningsinstitutt
Norsk romsenter
Space Norway
Justervesenet
Norsk helsenett
Finanstilsynet
Finansdepartementet
E-tjenesten
Direktoratet for nødkommunikasjon
Huawei
Justis og beredskapsdepartementet (flere underavdelinger)
NorSIS
POD strategigruppe for å bekjempe datakriminalitet
Broadnet
Vegdirektoratet
Avinor
Avinor flysikring AS
Luftfartstilsynet
Politiets IKT-tjeneste
Kartverket
NSB
Flytoget
Ruter
Oslo politidistrikt
Arbeids- og sosialdepartementet
Brønnøysundregistret
Skatteetaten
Jernbaneverket
Jernbanetilsynet
Politidirektoratet
Forbrukerrådet
Forbrukerombudet

Workshop helse

SINTEF
Helse Nord
Sykehuspartner
Helse Sør-Øst
Helse Midt-Norge RHF
Helse Vest IKT
Ikomm AS
Legeforeningen/Akershus Universitetssykehus
Sykehuspartner
Helse- og omsorgsdepartementet
Norsk Helsenett
Pensjonist med tidligere tilknytning til sektoren
Helse Stavanger HF
Bærum kommune, PLO helseinformatikk
Helsedirektoratet
Helse Bergen
Teknologirådet
Norsk Helsenett

Workshop maritim

Kystverket
Sjøfartsdirektoratet
Colorline
Wilhelmsen Holding
Sjøfartsdirektoratet
Farstad Shipping
Rederiforbundet
Den Norske Krigsforsikring for Skib
Norsk Havneforening
Kongsberg Maritime

Workshop olje og gass

Lundin
Statoil
Gassco
Norsk olje og gass
Tampnet
Petroleumstilsynet
Norske Shell

Workshop finans

Finansdepartementet
Finanstilsynet
Norges Bank
NBIM
DNB
Oslo Børs
VPS
EIKA-gruppen
Evry
Nets
Finans Norge
Sparebank1
Nordea
BSK
BSK/BankID
FinansCERT
Bank Axept AS
B-IT Invest AS

Utvalget var involvert ved NorSIS Sikkerhetstoppmøte april 2015, med følgende deltakere:

Næringslivets Sikkerhetsråd
Abelia
IKT-Norge
Arbeidsgiverforeningen Spekter
Innovasjon Norge
Standard Norge
KINS
NorSIS
Justis- og beredskapsdepartementet
Microsoft
SPK
Det norske oljeselskap AS
Bergen kommune
Eigersund kommune
mnemonic as
Cyberforsvaret CKT
Bodø kommune
Telenor Norge
KS
NARF Ekstra AS
PwC
REMA i Norge AS
NVE
RGU Consulting
Politihøgskolen
KLP
UNINETT AS
Oslo politidistrikt
NorSIS
NISlab
Arbeidstilsynet
Austevoll Kraftlag SA – LYSGLIMT
FLO IKT
Helsedirektoratet
Senter for IKT i utdanningen
CCIS
NAV
COWI AS
Statkraft AS
Fujitsu
Difi
DNB
Bouvet ASA
PwC
Vann- og avløpsetaten, Oslo kommune
Riksantikvaren
Nasjonal sikkerhetsmyndighet
Lyse konsern
VNG Norge
NSB Fellestjenester IT

Eksterne rapporter utvalget har bestilt

- mnemonic (2015): *Avdekke, håndtere og etterforske digitale angrep*. Utarbeidet for Lysneutvalget. Benyttet i kapittel 21.
- DNV GL (2015): *Digitale sårbarheter Olje & gass*. Utarbeidet for Lysneutvalget. Benyttet i kapittel 14.
- DNV GL (2015): *Digitale sårbarheter Maritim Sektor*. Utarbeidet for Lysneutvalget. Benyttet i kapittel 18.

- SINTEF (2015): *Digitale sårbarheter i helsesektoren – En oppsummering av funn fra workshop holdt i mai 2015 i regi av Lysneutvalget.* Utarbeidet for Lysneutvalget. Benyttet i kapittel 17.
- BDO (2015): *Andre lands arbeid med digitale sårbarheter.* Utarbeidet for Lysneutvalget. Benyttet i kapittel 9.
- Utenriksdepartementet (2015): *Folkerettslige rammer for grenseoverskridende informasjonsinnhenting.* Utarbeidet for Lysneutvalget. Benyttet i kapittel 10 «Folkerett og internasjonalt samarbeid».
- Oslo Economics (2015): *Konsekvensutredning – Alternativer for styrket robusthet i landsdekkende kjernenett.* Utarbeidet for Lysneutvalget. Benyttet i kapittel 11.
- Oslo Economics (2015): *Konsekvensutredning – Tydeliggjøring av myndighetsansvar for norsk romvirksomhet.* Utarbeidet for Lysneutvalget. Benyttet i kapittel 12.

I tillegg har vi fått innspill og bistand fra følgende:

- Teknologirådet, bistand med tekst i kapittel 6 «Trender som påvirker sårbarhetsbildet».
- Seniorrådgiver Frank Robert Berg (B-IT Invest AS), benyttet i kapittel 16 «Finansielle tjenester».
- Seniorrådgiver Hans Petter Aarseth, benyttet i kapittel 17 «Helse og omsorg».
- Seniorrådgiver Jacob Kringen (DSB), benyttet i punkt 23.4 «Tilpasse tilsynsvirksomhet til å omfatte IKT-sikkerhet».
- Director & Senior Partner (ILPI) Njål Høstmælingen, bistand med tekst i kapittel 3 «Rettstatsprinsipper og grunnleggende samfunnsverdier».
- Seniorforsker Jon Røstum (SINTEF), benyttet i kap 15 «Vannforsyning».
- Seniorrådgiver Rune Erlend Fløisbonn og Alexandra Agersborg har bidratt i sekretariatet.

25.2 Ansvarsfordeling mellom departementene for samfunnssikkerhetsarbeidet[1]

[1] Prop. 1 S (2015–2016) Justis- og beredskapsdepartementet. Det pågår et arbeid for å avklare noen ansvarsområder. Tabellen vil bli justert ved behov.

Områder	Overordnet ansvarlig, samordnende departement	Utøvende virksomheter/forvaltningsnivåer med vesentlig ansvar	Øvrige departementer med ansvar
Elektronisk kommunikasjonsnett og -tjenester	SD	Nasjonal kommunikasjonsmyndighet (Nkom), Direktoratet for nødkommunikasjon (DNK), Forsvaret	JD, FD
IKT-sikkerhet i sivil sektor	JD	Nasjonal Sikkerhetsmyndighet (NSM), Direktoratet for samfunnssikkerhet og beredskap (DSB)	Alle
Satellittbasert kommunikasjon og navigasjon	SD	Norsk romsenter, Kystverket, Nkom, Statens kartverk	JD, NFD, KMD
Kraftforsyning	OED	Norges vassdrags- og energidirektorat, Kraftforsyningens beredskapsorganisasjon	JD
Vannforsyning	HOD	Vannverkseiere (offentlige og private), kommunene, Mattilsynet, Helsedirektoratet (Hdir), Statens helsetilsyn, Nasjonalt folkehelseinstitutt, Statens strålevern, fylkesmennene	KLD, LMD
Olje og gass	ASD	Petroleumstilsynet, olje- og gassnæringene	OED
Drivstofforsyning	OED	Drivstoffnæringene	SD, NFD

Områder	Overordnet ansvarlig, samordnende departement	Utøvende virksomheter/forvaltningsnivåer med vesentlig ansvar	Øvrige departementer med ansvar
Transport	SD	Statens vegvesen, fylkeskommunene, kommunene, Luftfartstilsynet, Statens jernbanetilsyn, Jernbaneverket, NSB AS, Avinor AS, Sjøfartsdirektoratet, Norges rederiforbund, Kystverket	NFD, OED
Avløpshåndtering	KLD	Miljødirektoratet, kommunene	
Meteorologiske tjenester	KD	Meteorologisk institutt	NFD
Finansiell stabilitet	FIN	Norges Bank, Finanstilsynet	
Matforsyning	NFD	Landbruksdirektoratet, Fiskeridirektoratet, matvarenæringene	LMD
Kulturminner og symboler	KLD	Riksantikvaren, Arkivverket, fylkeskommunene, kommunene, Kystverket, Statsbygg	KUD, SD, KMD
Liv og helse	HOD	Statens helsetilsyn, Hdir, Arbeids- og velferdsdirektoratet, DSB, Sivilforsvaret, Mattilsynet, Nasjonalt institutt for ernærings- og sjømatforskning, Veterinærinstituttet, Nasjonalt folkehelseinstitutt, Statens strålevern, Vitenskapskomiteen for mattrygghet, Statens legemiddelverkene, de regionale helseforetakene, helseforetakene, Norsk Helsenett SF, kommunene, fylkesmennene, Forsvaret	ASD, LMD, NFD, JD, FD
Lov og orden	JD	Politidirektoratet (POD), Politiet, DSB, Politiets sikkerhetstjeneste (PST), Datatilsynet, Sivilrettsforvaltningen, Riksadvokaten, Kriminalomsorgsdirektoratet, Utlendingsdirektoratet	KMD
Nød- og redningstjeneste	JD	Hovedredningssentralen, Hdir, de regionale helseforetakene, helseforetakene, Forsvaret, POD, politiet, DSB, Næringslivets sikkerhetsorganisasjon, DNK, Avinor, Luftambulansetjenesten, kommunene (brann), frivillige organisasjoner	FD, HOD, SD, KMD med flere
Sentral styring og kriseledelse	JD	POD, Politiet, Forsvaret, DSB, NSM, fylkesmennene, kommunene, NRK, Hdir, Statens strålevern	UD, FD, HOD, SMK, alle departementer
Forsvar	FD	Forsvaret, Forsvarets forskningsinstitutt (FFI), NSM, Forsvarsbygg	JD, SD, OED, NFD, HOD, UD
Nasjonal sikkerhet (sivil)	JD	POD, PST, NSM, Statens kartverk, DSB, Forsvaret, fylkesmennene	UD, HOD, KMD, SMK, FD

Områder	Overordnet ansvarlig, samordnende departement	Utøvende virksomheter/forvaltningsnivåer med vesentlig ansvar	Øvrige departementer med ansvar
Natur og miljø	KLD	Fiskeridirektoratet, Kystverket, Miljødirektoratet, Norsk Polarinstitutt, Statens strålevern, Forsvaret, Landbruksdirektoratet, Norsk institutt for bioøkonomi, Nasjonalt institutt for ernærings- og sjømat-forskning, Havforskningsinstituttet, Mattilsynet, Veterinærinstituttet, Norges vassdrags- og energidirektorat, fylkesmennene, kommunene	NFD, SD, KD, FD, HOD, LMD, OED

25.3 Oppsummering av sentrale utvalg

Datateknikk og samfunnets sårbarhet (Seip-utvalget)

I 1986 kom Sårbarhetsutvalget ledet av Helge Seip med rapporten *Datateknikk og samfunnets sårbarhet.* Allerede i denne rapporten ble det slått fast at samfunnet var helt avhengig av IKT – eller elektronisk databehandling (EDB) – og dermed også svært sårbart for brudd eller forstyrrelser i EDB. Seip avgrenset sårbarhetsbildet til å gjelde de sårbarhetene som får konsekvenser for samfunnsviktige funksjoner, og ikke ulemper og tap for enkeltindivider. Utvalget var bevisst på EDB-systemenes avhengighet av ekom, og var av den oppfatning at sårbarhet i datateknikk måtte ses i nær sammenheng med tilgjengelighet av ekom.

Seip-utvalget påpekte at de fleste samfunnsfunksjoner allerede var avhengige av IKT-systemer, og at denne avhengigheten var kommet skritt for skritt, uten at det var gjort noen strategiske og bevisste vurderinger av det totale sårbarhetsbildet. Dette mente de hadde ført til komplekse verdikjeder og svært liten oversikt over strukturer og avhengighetsforhold, både for næringsliv og for offentlig forvaltning.

Utvalget konkluderte med at det var en svært lav sikkerhetsbevissthet i samfunnet, og at det i liten grad var gjennomført sikkerhetstiltak, noe utvalget fremhevet som alvorlig. Dette mente de kunne føre til at de samfunnsmessige konsekvensene av svikt i EDB-systemene kunne eskalere i fremtiden om det ikke ble satt i verk omfattende tiltak. Seip-utvalget trakk særlig frem den indirekte avhengigheten som alvorlig

> «tatt i betraktning de uheldige kjedereaksjoner som kan følge av andres driftsavbrudd. Utvalget vil videre peke på behovet for informasjon om metoder og teknikker for risiko- og sårbarhetsanalyser, og anbefaler at det særlig blir arbeidet på dette felt.»

Utvalget var videre opptatt av samfunnets avhengighet av kraft og ekom. Ekom var da ensbetydende med det statseide Televerket, og utvalget fastslo:

> «Televerkets ansvar og plikter må gå langt utover beskyttelse mot konsekvenser for Televerkets egen organisasjon, fordi den enkelte telebruker er helt avhengig av Televerket og av beredskapsmessige grunner selv er avskåret fra innsyn i Televerkets beredskapsplanen. Den risikoforplantning som kan skjule seg her, må bli gjenstand for offentlig overvåking.»

Videre så utvalget på hvordan det kunne bygges sikkerhet fra begynnelsen av, og foreslo programmeringstekniske tiltak. Det mest konkrete forslaget var at det burde etableres adgang til å foreta kvalitetskontroll av viktige programmer hos den enkelte bedrift/institusjon som utførte samfunnsviktig databehandling. Utvalget foreslo også økte kompetansetiltak som veiledning og utdanning og økt tilsyn/revisjon fra myndighetssiden.

Et sårbart samfunn – utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet (Sårbarhetsutvalget)

I 2000 kom Sårbarhetsutvalget ledet av Kåre Willoch med sin rapport *Et sårbart samfunn – utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet.* Mandatet til dette sårbarhetsutvalget var omfattende og fokuserte på risikoen for ekstraordinære påkjenninger for samfunnet, inkludert sikkerhetspolitiske kriser og krig, og hvordan samfunnet som helhet var forberedt på å møte store og omfattende krisescenarioer. Utvalget så også på sårbarheter i samfunnskritiske virksomheter

og kritisk infrastruktur – som første gang ble definert her. Et av underutvalgene utvalget opprettet, hadde som oppgave å «analysere samfunnets sårbarhet for brudd i informasjons- og kommunikasjonsteknologi».

Utvalget la i rapporten mer vekt på resultatene fra BAS2-prosjektet[2] som så på avhengigheter og fysiske sårbarheter, enn IKT-underutvalget som fokuserte på den logiske trusselen. Norsk senter for informasjonssikring ble opprettet for å kartlegge trusselen mot informasjonssikkerhet i norske virksomheter. Dette senteret, samt etableringen av en nasjonal strategi for informasjonssikkerhet, var sentrale tiltak på IKT-sikkerhetsområdet fra Sårbarhetsutvalget.

Av konkrete anbefalinger knyttet til IKT-sikkerhet og kraft var de viktigste:

- å fastsette klare sikkerhetskrav til etablering og drift av kritiske IKT-systemer
- å etablere et senter for informasjonssikring, organisert som en ikke-kommersiell stiftelse, som skulle ha som oppgave å koordinere oppgaver innen hendelsesrapportering, varsling, analyse og erfaringsutveksling med tanke på trusler mot IKT-systemer
- å bygge opp kapasitet og kompetanse til å føre effektivt tilsyn med IKT-sikkerheten innenfor all samfunnskritisk virksomhet
- å oppdatere retningslinjene for sikring av kraftforsyningen

I tillegg foreslo Sårbarhetsutvalget en rekke tiltak på mange områder, blant annet innenfor terror og sabotasje, transportsikkerhet, forsyningsberedskap, olje- og gassvirksomhet, mat og vann, radioaktivitet, smittevern og kjemiske og biologiske stridsmidler og informasjonsberedskap før, under og etter en krise. Innenfor disse er det ikke nevnt tiltak direkte knyttet til digital sikkerhet.

Utvalget kom videre med anbefalinger knyttet til organisatoriske tiltak. De mest relevante var

- samling av arbeid for samfunnssikkerhet og beredskap i ett departement som får dette som hovedoppgave
- opprettelse av et koordineringsorgan for EOS-tjenestene
- en samlet strategi og vurdering av å slå sammen organer for tilsyn med sikkerhet på ulike områder
- en gjennomgang av landets operative redningsog beredskapsressurser
- en felles granskingskommisjon for store ulykker og kriser

Av juridiske anbefalinger ble følgende foreslått:

- Lovgivningen burde tilpasses for å fremme samfunnets sikkerhet og beredskap. Blant annet foreslo utvalget å pålegge kommunene arbeid med kriseplanlegging.
- Ansvarsområdet til Politiets overvåkingstjeneste burde lovfestes, inkludert lovbestemmelser som ga Politiets overvåkingstjeneste mulighet til offensiv forebyggende virksomhet, herunder kommunikasjonskontroll i forebyggende øyemed.
- Det burde foretas en nærmere vurdering av behovet for endringer i lover og regler og behovet for incentiver, for å redusere samfunnets IKT-sårbarhet og styrke robusthetsnivået i kritisk infrastruktur.
- Den øvre strafferammen for datainnbrudd burde revurderes.

Sårbarhetsutvalget rettet også stor oppmerksomhet mot behovet for forskning og utdanning, og fastslo at det trengtes en ny giv for norsk sikkerhetsforskning for å holde tritt med teknologi- og samfunnsutviklingen. Utvalget mente at ett departement burde ta et hovedansvar for å sette i gang, vedlikeholde og videreutvikle sikkerhetsforskningen, og at det burde søkes løsninger som gjorde at sektordepartementer med stort ansvar for sikkerhet og beredskap gikk sammen med næringslivet i et forpliktende partnerskap for et sektorovergripende forskningsprogram. Sikkerhet burde i større grad integreres i IKT-utdanningen på alle nivåer fra videregående skole til universitet. I tillegg så utvalget behov for spesialkompetanse og for at IKT-sikkerhet ble etablert som eget fag ved enkelte universiteter og høyskoler.

Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner (Infrastrukturutvalget)

I 2006 kom Infrastrukturutvalget med rapporten *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner.* Hovedhensikten med oppnevnelsen av utvalget var å kartlegge landets kritiske infrastruktur og kritiske samfunnsfunksjoner og vurdere hvilke virkemidler som måtte til for å opprettholde funksjonalitet og ivareta rikets sikkerhet og vitale nasjonale interesser.

I Infrastrukturutvalgets rapport er fokuset flyttet fra etablering av et helhetlig apparat rundt

[2] *Beskyttelse av samfunnet* (BAS), forskningsserie ved Forvarets forsvarsinstitutt.

informasjonssikkerhet til organisering av myndighetenes arbeid, herunder ansvarsavklaring på departementsnivå – dette på bakgrunn av arbeidet med *Nasjonal strategi for informasjonssikkerhet*. Arbeidet med denne strategien førte blant annet til den permanente opprettelsen av NorSIS og NSM NorCERT. Utvalgets rapport foreslår i hovedsak organisatoriske tiltak i offentlig sektor for å bedre oppfølgingen av tiltak. En annen utvikling som har funnet sted fra det første sårbarhetsutvalget la frem sin rapport, er at Infrastrukturutvalget gjennom enkelte tiltak har fokusert også på privatpersoner.

Infrastrukturutvalget mente at Justis- og politidepartementet, sammen med opprettelsen av DSB, i stor grad var innrettet som det innenriksdepartementet Sårbarhetsutvalget foreslo. Det ble likevel pekt på at Justis- og politidepartementets koordinerende rolle måtte tydeliggjøres gjennom å

- være rådgivende myndighet i spørsmål knyttet til kritisk infrastruktur og kritiske samfunnsfunksjoner
- være pådriver og tilrettelegger for samarbeid og informasjonsdeling, samt bidra til koordinering av arenaer for dette
- etablere og videreutvikle en oversikt over kritisk infrastruktur og kritiske samfunnsfunksjoner gjennom en felles metode og system for å definere disse
- systematisere og koordinere trussel-, risiko- og sårbarhetsinformasjon knyttet til kritisk infrastruktur og kritiske samfunnsfunksjoner – herunder å etablere et system for innhenting og formidling av denne informasjonen
- være et nasjonalt kontaktpunkt ved internasjonalt samarbeid på området
- ta initiativ til avklaring av eventuelle uklare ansvarsforhold
- utarbeide felles målsettinger og strategier knyttet til kritisk infrastruktur og kritiske samfunnsfunksjoner i samarbeid med relevante aktører
- koordinere igangsettingen og oppfølgingen av tverrsektoriell FoU på området, herunder BAS og SAMRISK[3]

I tillegg pekte Infrastrukturutvalget på at det burde tydeliggjøres nasjonale mål og/eller akseptnivåer gjennom å innarbeide dette som premiss i aktørenes risiko- og sårbarhetsanalyser. Justis- og politidepartementet burde videre gi konkrete retningslinjer for gjennomføring av risiko- og sårbarhetsanalyser, og det burde utvikles et program for «regelmessige ROS-analyser tilknyttet kritisk infrastruktur og kritiske samfunnsfunksjoner, som grunnlag for tverrsektorielle avveininger, risikobaserte prioriteringer, helhetlig analyse og politikk for det sivile og militære sikkerhetsarbeid». Utvalget foreslo også å utrede en lovregulering for å sikre kritisk infrastruktur og kritiske samfunnsfunksjoner.

Videre mente Infrastrukturutvalget at tilsynsvirksomheten på området kritisk infrastruktur og kritiske samfunnsfunksjoner burde styrkes, og at en i den sammenheng burde vurdere en samordning av tilsynsvirksomheten og en prinsipiell drøfting av forholdet mellom tilsyn som ivaretar overordnede interesser, og tilsyn som ivaretar sektorinteresser (horisontale versus vertikale tilsyn).

Utvalget foreslo en statlig tilskuddsordning for å sikre at tverrsektorielle tiltak uten en hovedeier ble fulgt opp. De mente at dette ville bidra til å finansiere den statlige delen i en risikofordeling mellom offentlige og private interesser, finansiere nødvendige sektorovergripende tiltak, følge opp sektorovergripende infrastrukturer, samt ivareta et helhetlig perspektiv og følge opp tiltak ut fra hensynet til sikkerhet mot utilsiktede og tilsiktede hendelser.

For å sikre at krav til sikkerhet ble ivaretatt, foreslo utvalget at det ved offentlige innkjøp skulle vurderes sikkerhets- og beredskapsmessige konsekvenser ved bortfall av de varene og tjenestene som ble levert. Videre burde det etableres en liste over kontrollpunkter som skulle benyttes i forbindelse med omreguleringer og omorganiseringer, for å ivareta sikkerhetsmessige problemstillinger ved omstillinger. Utvalget mente at kjøp av tjenester og tilskudd til spesielle oppgaver for sikring av kritisk infrastruktur ville være et nødvendig virkemiddel sammen med regulatoriske bestemmelser.

Utvalget var også svært opptatt av offentlig eierskap som virkemiddel, og mente at dette måtte vurderes konkret hos aktører som var eiere av kritiske samfunnsfunksjoner og kritisk infrastruktur. I avveiinger mellom offentlig og privat eierskap burde hensynet til samfunnssikkerhet og beredskap veie tungt. Videre burde eierskap til ekominfrastruktur være under kontroll av norske eiere. I kraftsektoren foreslo utvalget at sentralnettet skulle beholdes i offentlig eierskap, mens distribusjonsnettet ikke i samme grad burde være i offentlig eierskap.

Videre hadde utvalget blant annet følgende forslag til kraft og ekom: at det skulle etableres

[3] Forskningsrådets program for samfunnssikkerhetsforskning.

nødvendige lovhjemler som sikret reserveløsninger i ekomnett og -tjenester, at muligheter for strømrasjonering ble utredet, og at det ble stilt krav til nødstrøm for kritiske samfunnsfunksjoner. Vedlikeholdsetterslepet i kraftsektoren burde vies oppmerksomhet, og det burde vurderes om KILE-ordningen[4] kunne bidra til å sikre vedlikehold.

Av organisasjonsmessige tiltak foreslo Infrastrukturutvalget en reduksjon i antall fagdepartementer med ansvar for IT-sikkerhetsarbeid og en samordning mellom Samferdselsdepartementet og Forbruker- og administrasjonsdepartementet. Videre burde JD legge til rette for større faglige synergieffekter ved blant annet å opprette et organ for informasjonsdeling mellom PST, NSM og DSB. Utvalget satte også spørsmålstegn ved hvorvidt det er hensiktsmessig/mulig å skille mellom etatsstyringsansvar og fagansvar for NSM. Fylkesmannens ansvar burde tydeliggjøres, blant annet når det gjaldt rekvirering av ressurser for å prioritere mellom ulike brukere ved avbrudd i kritisk infrastruktur, og kommunene burde få en generell beredskapsplikt.

Infrastrukturutvalget foreslo også tiltak knyttet til forskning og utvikling, blant annet: FFIs mandat burde utvides til også å gjelde sivil sektor, SAMRISK burde iverksettes, forskning knyttet til beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner burde prioriteres hos Forskningsrådet, Terrorkonsortiet burde videreføres, og det burde startes et forskningsprosjekt for å se på gjensidige avhengigheter i kritisk infrastruktur.

[4] KILE (kvalitetsjusterte inntektsrammer ved ikke levert energi) er en ordning med insentivregulering som skal gi nettselskapene økonomisk motivasjon til riktig ressursallokering innenfor de rammer og vilkår som ellers er gitt av myndighetene.

Referanser

Ablon, Lillian, Martin C. Libicki and Andrea A. Golay (2014): *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. Santa Monica, CA: RAND Corporation.

ACM/IEEE-CS Joint Task Force on Computing Curricula (2013): *Computer Science Curricula 2013 – Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*.

Agenda Kaupang (2014): *Evaluering av Difi*.

Almklov (2011): *Offentlige etaters rolle i å sikre robusthet i komplekst organiserte og tett koblede infrastruktursektorer*.

Antony Deceglie (2012): T*aliban Using Facebook to Lure Aussie Soldier*, The Sunday Telegraph, September 09.2012, In: Harley, J.: Information Operations Newsletter, Vol. 13, no. 01.

BDO (2015): *Andre lands arbeid med digitale sårbarheter*.

Biener, Christian; Martin, Eling and Jan Hendrik Wirfs: *Insurability of Cyber Risk: An Empirical Analysis*. The Geneva Papers on Risk and Insurance-Issues and Practice 40.1 (2015): 131–158.

Bing, J.: *Building cyberspace: a brief history of Internet. In: Internet Governance, Infrastructure and Institutions*. Eds: Bygrave, L.A. and Bing. J., Oxford University Press: 8–47.

Carr, Nicholas (2014): *The Glass Cage: Automation and Us*.

CISCO (2015): *Annual security report*.

CISCO (2011): *The Internet of Things – How the Next Evolution of the Internet Is Changing Everything*.

Council of Europe (2001): *Treaty No.185 Convention on Cybercrime*.

Council of Europe (2001): *Convention on Cybercrime, Additional Protocol*, Budapest, 23.XI.2001. ETS No 185.

CWE-259 (2014): *Use of Hard-coded Password, Gartner survey of EHR suppliers and systems in the Norwegian market.*

DAMVAD og Samfunnsøkonomisk analyse (2014): *Dimensjonering av avansert IKT-kompetanse*.

Datatilsynet (2013): *Big Data – personvernprinsipper under press*.

Deceglie, Antony (2012): *Taliban Using Facebook to Lure Aussie Soldier*, The Sunday Telegraph, September 09.2012, In: Harley, J.: Information Operations Newsletter, Vol. 13, no. 01 (September–October 2012).

Detica, Cabinet Office (2011): *The cost of cyber crime*.

Direktoratet for forvaltning og IKT (2010): *Risikovurdering – en veiledning til Rammeverket for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor*.

Direktoratet for forvaltning og IKT (2010): *Nasjonale felleskomponenter i offentlig sektor – Forslag til hvordan nasjonale felleskomponenter bør styres, forvaltes, finansieres og utvikles*.

Direktoratet for nødkommunikasjon (2014): *Robusthet i transmisjon. Reservestrøm i transmisjonslinjer i Nødnett*.

Direktoratet for samfunnssikkerhet og beredskap (2015): *Sammenstilling av relevante funn fra hendelser og øvelser siste fem år*, delutredning til Lysneutvalget.

Direktoratet for samfunnssikkerhet og beredskap (2015): *Risikoanalyse av cyberangrep mot ekominfrastruktur*. Delrapport til Nasjonalt risikobilde 2014.

Direktoratet for samfunnssikkerhet og beredskap (2015): *Støtte til Forsvarssjefens operative planverk*. Oppdragsbrev fra Justis- og beredskapsdepartementet.

Direktoratet for samfunnssikkerhet og beredskap (2015): *Nasjonalt risikobilde 2014*.

Direktoratet for samfunnssikkerhet og beredskap (2014): *Kommuneundersøkelsen 2014. Status for samfunnssikkerhets- og beredskapsarbeidet i kommunene*.

Direktoratet for samfunnssikkerhet og beredskap (2012): *Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring (KIKS)*.

Direktoratet for samfunnssikkerhet og beredskap (2012): *Samfunnets sårbarhet som følge av bortfall av elektronisk kommunikasjon*.

Direktoratet for samfunnssikkerhet og beredskap (2012): *Nasjonalt risikobilde 2012 med fordyp-*

ningsdel. Kommunenes beredskap mot bortfall av elektrisk kraft.

DNV GL (2015): *Digitale Sårbarheter Maritim Sektor, Lysneutvalget.*

DNV GL (2015): *Digitale sårbarheter Olje & gass, Lysneutvalget.*

ECON (2014): *The partnership between the Norwegian Oil & Gas Industry and the EU countries.*

Éireann P. Leverett (2011): *Quantitatively Assessing and Visualising Industrial System Attack Surfaces, University of Cambridge, Dissertation.*

The Electric Infrastructure Security Council (2014): *E-PRO Handbook, EPRO Electric Grid*, First Edition.

EMC (2014): *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things.*

Energi Norge og Telenor (2013): *Sikkerhet og beredskap mot ekstremvær i telesektoren.*

ENISA (2014): *Threat landscape.*

ENISA (2012): *National Cyber Security Strategies – Setting the course for national efforts to strengthen security in cyberspace.*

ENISA (2012): *Smart Grid Security – Annex I General Concepts and Dependencies with ICT.*

ENISA (2012): *Incentives and barriers for the cyber insurance market in Europe.*

Etterretningstjenesten (2015): *Etterretningstjenestens vurdering, FOKUS.*

EU (2010): Article 29 *Data Protection Working Party.* 00070/2010/EN WP 176.

EU (2011): *Commission implementing regulation* (EU) No 1035/2011.

Europol (2014): *The internet organized crime threat assessment (IOCTA).*

Finansdepartementet (2013): Meld. St. 21 (2013–2014) *Finansmarknadsmeldinga 2013.*

Finanstilsynet (2015): *Endelige retningslinjer for sikkerhet i internettbetalinger.*

Finanstilsynet (2015): *Risiko- og sårbarhetsanalyse (ROS) 2014.* Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT).

Finanstilsynet og Norges Bank (2011): *Betalingssystemloven – samarbeid og ansvarsdeling mellom Finanstilsynet og Norges Bank.*

Forbrukerrådet (2014): *Du selger deg billig – En rapport om betalingsløsninger og personvern.*

Fornyings-, administrasjons- og kirkedepartementet (2013): Meld. St. 23 (2012–2013) *Digital agenda for Norge – IKT for vekst og verdiskaping.*

Fornyings- og administrasjonsdepartementet, Samferdselsdepartementet, Justis- og beredskapsdepartementet og Forsvarsdepartementet (2012): *Nasjonal strategi for informasjonssikkerhet.*

Fornyings- og administrasjonsdepartementet (2009): *Statens kommunikasjonspolitikk.*

Forskningsrådet (2015): *Årsrapport 2014.*

Forskningsrådet (2015): *IKTPLUSS – Plan for satsingen.*

Forskningsrådet (2015): *Research in Information and Communication Technology in Norway. An evaluation.*

Forsvarsdepartementet (2015): *Et felles løft.* Ekspertgruppen for forsvaret av Norge.

Forsvarsdepartementet (2011): *Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven).*

Forsvarsdepartementet, Justis- og beredskapsdepartementet (2015): *Støtte og samarbeid. En beskrivelse av totalforsvaret i dag.*

Forsvarets forskningsinstitutt (2015): FFI-rapport 2015/00923 *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger.*

Forsvarets forskningsinstitutt (2014): FFI-Rapport 2014/00948. *Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet.*

Forsvarets forskningsinstitutt (2014): *Krisehåndtering i et sårbart cybersamfunn.*

Forsvarets forskningsinstitutt (2004): TEK14: *Militærteknologiske trender – Oversiktsrapport.*

FOX IT (2015): *Cyber security: 60 percent of oil and gas companies do not have an Incident Response Plan in place.*

Gottschalk, Petter (2013): *Flytting av arbeidsoppgaver til utlandet. En oversikt over forskning om mål og resultat når virksomheter setter ut til andre å utføre tjenester.* BI. Til Finansforbundet.

Granskningsgruppe (2013): *Angrepet mot In Amenas – Rapport fra granskningen av terrorangrepet mot In Amenas.* Utarbeidet for styret i Statoil ASA.

Greveler U., Justus B., and Loehr, D. (2012): *Multimedia content identification through smart meter power usage profiles.*

Hagen, J (2009): *How do employees comply with security policy? A comparative case study of four organizations under the security act. In: The human factor behind the Security Perimeter, Evaluating the effectiveness of organizational information security measures and employees' contribution to security.* Universitetet i Oslo.

Helsedirektoratet (2015): *Styrket gjennomføringsevne for IKT-utvikling i helse- og omsorgstjenesten.*

Helsedirektoratet (2014): *Utredning av «Én innbygger – én journal». Komparativ analyse av de regionale helseforetakene på IKT-området.*

Helse- og omsorgsdepartementet (2014): *Nasjonal helseberedskapsplan*. Versjon 2.0.

Helse- og omsorgsdepartementet (2002): *Forskrift om vannforsyning og drikkevann (Drikkevannsforskriften)*.

Helse- og omsorgsdepartementet, Klima- og miljødepartementet, Arbeids- og sosialdepartementet (2011): *Forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg (styringsforskriften)*.

Helse- og omsorgsdepartementet, Klima- og miljødepartementet, Arbeids- og sosialdepartementet (2011): *Forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg (styringsforskriften)*.

Helsetilsynet (2015): *Med tilsynsblikk på alvorlige og uventede hendelser i spesialisthelsetjenesten. Status og erfaringer 2014*. Fra Undersøkelsesenheten i Statens helsetilsyn.

Hubbard, Z.P. (2007): *Information Operations in the Global Ear on terror: Lessons Learned From Operations in Afghanistan and Iraq. In Information Warfare. Separating hype from reality*, L. Armistead, ed., Dulles, Virginia: Potomac Books Inc.

Idaho National Laboratory (2011): *Vulnerability Analysis of Energy Delivery Control Systems*.

IEEE Volume 7, Issue: 4 (2009): *Human Relationships: A Never-Ending Security Education Challenge? Security & Privacy*.

International Monetary Fund (IMF) (2015): *Financial System Stability Assessment for Norway*.

ISC2 (2015): *Cybersecurity principles and learning outcomes for computer science and IT-related degrees. A resource for course designers and accreditors*. Versjon 1.1.

Johnsen, Stig Ole (2012): *An Investigation of Resilience in Complex Socio-Technical Systems to Improve Safety and Continuity in Integrated Operations*. NTNU.

Justis- og beredskapsdepartementet (2015): Prop. 1 S (2015–2016).

Justis- og beredskapsdepartementet (2015): *FoU-strategi for samfunnssikkerhet 2015–2019*.

Justis- og beredskapsdepartementet (2015): *Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet*.

Justis- og beredskapsdepartementet (2014): *Modell for håndtering av IKT-sikkerhetshendelser – anbefalinger og retningslinjer*, brev til departementene.

Justis- og beredskapsdepartementet (2012): Kgl.res. 15.6.2012: *Instruks for departementenes arbeid med samfunnssikkerhet og beredskap, Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering*.

Justis- og beredskapsdepartementet (2011): *Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret*.

Justis- og beredskapsdepartementet (2010): *Lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven)*.

Justis- og beredskapsdepartementet (2007): *Avtale om samarbeid om lokalradiostasjonens virksomhet under kriser og katastrofer av 22.01.2007*. Inngått mellom Justis- og beredskapsdepartementet, Norsk rikskringkasting, Telenor Norge AS og Norsk lokalradioforbund.

Justis- og beredskapsdepartementet (2005): *Lov om straff (straffeloven)*.

Justis- og beredskapsdepartementet (1999): *Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven)*.

Kommunal- og moderniseringsdepartementet (2015): *Kartlegging av hindringer i regelverk for bruk av skytjenester*. Interdepartemental arbeidsgruppe.

Kommunal- og moderniseringsdepartementet (2015): *Handlingsplan for informasjonssikkerhet i statsforvaltningen (2015–2017)*.

Kommunal- og moderniseringsdepartementet (2013): *Nasjonal strategi – IKT-forsking og – utvikling. Strategi 2013–2022*.

Kripos (2014): *Trendrapport 2015 – den organiserte kriminaliteten i Norge*.

Krutskikh, A.V. (2012): *Developments in the Field of Information and telecommunications in the Context of International Security*. Study Series 33, Part 1: A/65/201, United Nations, New York.

KS, FoU (2015): *Utredning av juridiske forhold ved bruk av nettsky i kommunal sektor – en mulighetsstudie*. Utarbeidet av Advokatfirmaet Føyen Torkildsen.

Lagner, Ralph (2014): *To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve*.

Langbråten, Nina (2012): *Nye betalingsmåter*. Norges Bank.

Langill, Joel, Zambon, Emmanuele and Trivellato, Daniel (2014): *Cyberespionage campaign hits energy companies, SilentDefense helps detecting and mitigating the threat*.

Line, Maria Bartnes (2015): *Understanding Information Security Incident Management Practices – A case study in the electric power industry*. NTNU.

Kjølle, G.H., Gjerde, O., Hofmann, M. (2013): *Vulnerability and security in a changing power system*. SINTEF.

Mattilsynet (2006): *Økt sikkerhet og beredskap i vannforsyningen. Veiledning*.

Meld. St. 7 (2010–2011) *Kampen mot organisert kriminalitet – en felles innsats*.

Meld. St. 8 (2010–2011) *Digitalisering av radiomediet*.

Meld. St. 29 (2011–2012) *Samfunnssikkerhet*.

Meld. St. 9 (2012–2013) *Én innbygger – én journal*.

Meld. St. 26 (2012–2013) *Nasjonal transportplan 2014–2023*.

Meld. St. 39 (2012–2013) *Mangfold av vinnere*

Meld. St. 37 (2014–2015) *Globale sikkerhetsutfordringer i utenrikspolitikken – Terrorisme, organisert kriminalitet, piratvirksomhet og sikkerhetsutfordringer i det digitale rom*.

Metier (2014): Rapport til Kommunal- og moderniseringsdepartementet og Finansdepartementet. *KS2 (kvalitetssikring fase 2) av Ny IKT-løsning for departementene*.

Ministry of Defence UK (2014): *Global Strategic Trends – Out to 2045*.

mnemonic (2015): *Avdekke, håndtere og etterforske digitale angrep*.

Moe, Marie (2015): *Informasjonssikkerhet og personvern: Hva må vi tenke på ved tilgjengeliggjøring av data?* SINTEF IKT, Systemutvikling og sikkerhet.

Moen-Hagalisletto, Anders og Fritsch, Lothar (2011): *Mobilnett-kollapsen: Vi må leve med risikoen*. Kronikk i forskning.no 21.06.2011.

Myndigheten för samhäldsskydd och beredskap (2015): *Informationssäkerhet – trender 2015*.

Myndigheten för samhäldsskydd och beredskap (2012): *Reflections on civil protection and emergency preparedness during major IT incidents*.

Myndigheten för samhäldsskydd och beredskap (2010): *Kartläggning av SCADA-säkerhet inom svensk dricksvattenförsörjning*.

Nasjonal kommunikasjonsmyndighet (2015): *Vurdering av om dekningsvilkår for avvikling av FM er oppfylt*. Dekningsvurderinger for NRKs DAB-nett, de kommersielle DAB-nettene og NRK P1s stereodekning i FM-nettet.

Nasjonal kommunikasjonsmyndighet (2014): *Robusthet i elektronisk kommunikasjon – veiledning og råd til kommuner*.

Nasjonal kommunikasjonsmyndighet (2013): *Forskrift om klassifisering og sikring av anlegg i elektroniske kommunikasjonsnett (klassifiseringsforskriften)*.

Nasjonal sikkerhetsmyndighet (2015): *Helhetlig IKT-risikobilde 2015*.

Nasjonal sikkerhetsmyndighet (2015): *Sikkerhetsfaglig råd*.

Nasjonal sikkerhetsmyndighet (2014): *Fire effektive tiltak mot dataangrep*.

Nasjonal sikkerhetsmyndighet (2015): *Risiko 2015*.

Nasjonal sikkerhetsmyndighet (2009): *Veiledning i verdivurdering*.

National Intelligence Council (2012): *Global Trends 2030: Alternative Worlds*.

Nexia International (2015): *Kartlegging og analyse av landskapet for offentlige datasentre i Norge 2015 – Utarbeidet for Kommunal- og moderniseringsdepartementet*.

Nexia/Styrmand (2012): *Kost/nyttevurdering av tiltak for styrking av norsk sambands- og IP-infrastruktur*. For Post- og teletilsynet.

NorSIS (2015): *Trusler og trender*.

Norges Bank (2014): *Finansiell infrastruktur 2014*.

Norges Bank (2015): *Finansiell infrastruktur 2015*.

Norges vassdrags- og energidirektorat (2015): *Smarte målere (AMS). Status og planer for installasjon og oppstart per 1. kvartal 2015*.

Norges vassdrags- og energidirektorat (2015): *Kraft fra land til Johan Sverdrup-feltet*.

Norsk elektroteknisk norm (2014): NEK 399-1 *Tilknytningspunkt for el- og ekomnett. Normen omhandler etablering og utforming av felles grensesnitt (skap) for blant annet elnett, elmåler og ekomnett*.

Norsk romsenter (2013): *Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur*.

Norsk vann (2014): *Vann- og avløpsteknikk*.

Norsk vann (2014): *Fra driftsassistanser til regionale vannassistanser*. Rapport 203/2014.

Norsk vann (2013): Rapport 195/2013: *Sikkerhet og sårbarhet i driftskontrollsystemer for VA-anlegg*.

NOU 2015: 1 *Produktivitet – grunnlag for vekst og velferd*.

NOU 2013: 9 *Ett politi – rustet til å møte fremtidens utfordringer – Politianalysen*.

NOU 2013: 2 *Hindre for digital verdiskaping*.

NOU 2012: 14 *Rapport fra 22. juli-kommisjonen*.

NOU 2014: 14 *Fagskolen – ett attraktivt utdanningsvalg*.

NOU 2012: 2 *Utenfor og innenfor Norges avtaler med EU*.

NOU 2009: 15 *Skjult informasjon – åpen kontroll – Metodekontrollutvalgets evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker.*

NOU 2009: 1 *Individ og integritet – Personvern i det digitale samfunnet.*

NOU 2015: 8 *Fremtidens skole – Fornyelse av fag og kompetanser.*

NOU 2007: 2 *Lovtiltak mot datakriminalitet – Delutredning II.*

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

NOU 2003: 27 *Lovtiltak mot datakriminalitet – Delutredning I om Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi.*

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

NOU 1999: 27: *«Ytringsfrihed bør finde Sted» – Forslag til ny Grunnlov § 100.*

NOU 1986: 12 *Datateknikk og samfunnets sårbarhet.*

Nærings- og fiskeridepartementet (2001): *Lov om elektronisk signatur (esignaturloven).*

Næringslivets sikkerhetsråd (2014): *Mørketallsundersøkelsen 2014 – Informasjonssikkerhet, personvern og datakriminalitet.*

OECD (2002): *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.*

Office of Electricity Delievery and Energy Reliability (2011): *Vulnerability analysis of energy delivery control systems.*

Office of Electricity Delievery and Energy Reliability (2011): *Vulnerability analysis of energy delivery control systems.*

Oljeindustriens landsforening (nå Norsk olje og gass) (2007): *HMS- og Integrerte operasjoner: Forbedringsmuligheter og nødvendige tiltak.*

Olje- og energidepartementet (2003): *Kronprinsregentens resolusjon om det nye Oljedirektoratets ansvar og oppgaver etter utskillelsen av Petroleumstilsynet.*

Olje- og energidepartementet (2014): *Et bedre organisert strømnett.*

Olje- og energidepartementet (2003): *Kronprinsregentens resolusjon om det nye Oljedirektoratets ansvar og oppgaver etter utskillelsen av Petroleumstilsynet.*

Oljeindustriens landsforening (nå Norsk olje og gass) (2007): *HMS- og Integrerte operasjoner: Forbedringsmuligheter og nødvendige tiltak.*

Oslo Economics (2015): *Konsekvensutredning – Alternativer for styrket robusthet i landsdekkende kjernenett.* Utarbeidet for Lysneutvalget.

Oslo Economics (2015): *Konsekvensutredning – Tydeliggjøring av myndighetsansvar for norsk romvirksomhet.* Utarbeidet for Lysneutvalget.

Ot.prp. nr. 92 (1998–99) *Om lov om behandling av personopplysninger (personopplysningsloven).*

Perrow, Charles (1984): *Normal Accidents: Living with High Risk Technologies.* Basic Books.

Petroleumstilsynet (2011): *Deepwater Horizon-ulykken – Vurderinger og anbefalinger for norsk petroleumsvirksomhet.*

Politidirektoratet (2012): *Organisering av øko-teamene.*

Politidirektoratet (2012): *Politiet i det digitale samfunnet – En arbeidsgrupperapport om: elektroniske spor, IKT-kriminalitet og politiarbeid på Internett.*

Politidirektoratet (2010–2012): *Tendenser i kriminaliteten.*

Politiets sikkerhetstjeneste (2015): *Åpen trusselvurdering 2015.*

Post- og teletilsynet (2014): *Ekomtjenester, -nett og -utstyr. Utvikling og betydning for PT.*

Post- og teletilsynet (2013): *Ekomlovens krav vedrørende kommunikasjonsvern, integritet og tilgjengelighet – logiske angrep.* Presiseringsnotat fra Post- og teletilsynet til ekomtilbydere.

Post- og teletilsynet (2012): *Foreløpige erfaringer og forslag til tiltak etter ekstremværet Dagmar.*

Post- og teletilsynet (2012): *Sårbarhetsanalyse av mobilnettene i Norge.*

Proactima og Energi Norge (2015), *Overordnet risiko- og sårbarhetsanalyse for innføring av AMS.*

Prop. 112 L (2010–2011): *Endringer i energiloven og i enkelte andre lover.*

Prop. 73 S (2011–2012) *Et forsvar for vår tid.*

Prop. 53 L (2012–2013) *Endringer i straffeloven 1902 mv. (offentlig sted, offentlig handling m.m.).*

Rambøll (2013): *Utfordringer og muligheter i kommunalteknisk sektor.* FOU-prosjekt nr. 134038 for KS.

Regjeringen (2013): *Tiltredelseserklæring fra regjeringen Solberg 18. oktober 2013*, Sundvoldenplattformen.

Report of the joint Informatics Europe & ACM Europe Working Group on Informatics Education (2013): *Informatics education – Europe cannot afford to miss the boat.*

Riksadvokaten (2015): *Rundskriv nr. 1/2015 Mål og prioriteringer for straffesaksbehandlingen i 2015 – Politiet og statsadvokatene.*

Riksrevisjonen (2014): *Riksrevisjonens kontroll med forvaltningen av statlige selskaper for 2013*, Dokument 3:2 (2014–2015).

Riksrevisjonen (2014): *Riksrevisjonens undersøkelse om elektronisk meldingsutveksling i helse- og omsorgssektoren*. Dokument 3:6 (2013–2014).

Riksrevisjonen (2013): *Riksrevisjonens rapport om den årlige revisjon og kontroll for budsjettåret 2013,* Dokument 1 (2014–2015).

Riksrevisjonen (2008): Riksrevisjonens undersøkelse om IKT i sykehus og elektronisk samhandling i helsetjenesten, Dokument nr. 3:7 (2007–2008).

Samferdselsdepartementet (2015): *Lov om elektronisk kommunikasjon (ekomloven)*.

Samferdselsdepartementet (2010): *Krisescenarioer i samferdselssektoren – KRISIS*.

Samferdselsdepartementet (1999): *Forskrift om etablering, drift og bruk av jordstasjon for satellitt*.

Sampigethaya et al. (2011): *Future E-Enabled Aircraft Communications and Security: The Next 20 Years and Beyond, Proceedings of the IEEE* Vol. 99. No.11.

Senter for IKT i utdanningen (2012): *Monitor 2011 – Skolens digitale tilstand*.

SINTEF (2015): *Digitale sårbarheter i helsesektoren – En oppsummering av funn fra workshop holdt i mai 2015 i regi av Lysneutvalget*. Utarbeidet for Lysneutvalget.

Slay, J and Miller, M (2007): *Lessons Learned from the Maroochy Water Breach in Critical Infrastructure Protection*, vol. 253, E. Goetz and S. Shenoi, Eds., ed: Springer Boston, 2007, pp. 73–82.

SOU 2015:23 *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten*.

Statens Vegvesen, Vegdirektoratet (2014): *Bransjenorm for personvern og informasjonssikkerhet i elektronisk billettering*.

Standard Norge (2014): NS 5832:2014 *Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse*.

Standard Norge (2012): NS-ISO 22300:2012 *Samfunnssikkerhet – Terminologi*.

Standard Norge (2008): NS 5814:2008 *Krav til risikovurderinger*.

Statsministerens kontor (2013): *Overføring av samordningsansvaret for forebyggende IKT-sikkerhet fra Fornyings-, administrasjons- og kirkedepartementet til Justis- og beredskapsdepartementet*. Kgl. res. 22.03.2013.

St.meld. nr. 22 (2007–2008) *Samfunnssikkerhet – samvirke og samordning*.

St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet*.

Symantec (2015): *Internet Security Threat Report*.

Sæle, H., Sagosen, Ø., Bjørndalen, J. (2014): *Norsk driftssentralstruktur Funksjon, kostnadsforhold og fremtidig utvikling*. SINTEF Energi.

Teknologirådet (2014): *På nett med publikum. Hvordan smarttelefonen og sosiale medier gir nye muligheter for norsk politi*.

The Bank for International Settlements (BIS) (2014): *Cyber resilience in financial market institutions*.

Tøndel et al. (2013): *Towards Improved Understanding and Holistic Management of the Cyber Security Challenges in Power Transmission Systems*, SINTEF.

United States Government Accountability Office (2015): *Air Traffic Control. FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen*.

UNODC (2013): *Comprehensive Studyon Cybercrime (Draft)*.

Utdanningsdirektoratet (2012): *Rammeverk for grunnleggende ferdigheter – Til bruk for læreplangrupper oppnevnt av Utdanningsdirektoratet*.

Utenriksdepartementet (2015): *Folkerettslige rammer for grenseoverskridende informasjonsinnhenting*.

Vinnem, J.E., Utne, I.B., Skogdalen, J.E. (2011): *Looking Back and Forward: Could Safety Indicators Have Given Early Warnings about the Deepwater Horizon Accident?* Deepwater Horizon Study Group.

Walton, Mark (2015): *Google's quirky self-driving bubble car hits public roads this summer*.

Weiss, Joseph (2010), *Protecting Industrial Control Systems from Electronic Threats. Momentum Press*. New York.

White House (2014): *Big data: Seizing opportunities, preserving values*.

World Economic Forum (2015): *Partnering for Cyber Resilience, Towards the Quantification of Cyber Threats*.

World Economic Forum (2012): *Risk and responsibility in a Hyperconnected world – pathways to global cyber resilience*.

Øvstedal, L., Lervåg, L.E. og T. Foss (2010): *Personvern og trafikk: Personvernet i intelligente transportsystemer*. SINTEF.

Norges offentlige utredninger 2014 og 2015

Statsministeren:

Arbeids- og sosialdepartementet:
NOU 2014: 3 Grunnlaget for inntektsoppgjørene 2014
NOU 2014: 17 Pensjonsordning for arbeidstakere til sjøs
NOU 2015: 6 Grunnlaget for inntektsoppgjørene 2015
NOU 2015: x Arbeidstidsutvalget

Barne-, likestillings- og inkluderingsdepartementet:
NOU 2014: 8 Tolking i offentlig sektor
NOU 2014: 9 Ny adopsjonslov
NOU 2015: 4 Tap av norsk statsborgerskap

Finansdepartementet:
NOU 2014: 13 Kapitalbeskatning i en internasjonal økonomi
NOU 2015: 1 Produktivitet – grunnlag for vekst og velferd
NOU 2015: 5 Pensjonslovene og folketrygdreformen IV
NOU 2015: 9 Finanspolitikk i en oljeøkonomi
NOU 2015: 10 Lov om regnskapsplikt
NOU 2015: 12 Ny lovgivning om tiltak mot hvitvasking og terrorfinansiering

Forsvarsdepartementet:

Helse- og omsorgsdepartementet:
NOU 2014: 12 Åpent og rettferdig – prioriteringer i helsetjenesten
NOU 2015: 11 Med åpne kort

Justis- og beredskapsdepartementet:
NOU 2014: 1 Ny arvelov
NOU 2014: 10 Skyldevne, sakkyndighet og samfunnsvern
NOU 2015: 3 Advokaten i samfunnet
NOU 2015: 13 Digital sårbarhet – sikkert samfunn

Klima- og miljødepartementet:

Kommunal- og moderniseringsdepartementet:
NOU 2014: 6 Revisjon av eierseksjonsloven
NOU 2015: 7 Assimilering og motstand

Kulturdepartementet:
NOU 2014: 2 Lik og likskap

Kunnskapsdepartementet:
NOU 2014: 5 MOOC til Norge
NOU 2014: 7 Elevenes læring i fremtidens skole
NOU 2014: 14 Fagskolen – et attraktivt utdanningsvalg
NOU 2015: 2 Å høre til
NOU 2015: 8 Fremtidens skole

Landbruks- og matdepartementet:
NOU 2014: 15 Norsk pelsdyrhold – bærekraftig utvikling eller styrt avvikling?

Nærings- og fiskeridepartementet:
NOU 2014: 4 Enklere regler – bedre anskaffelser
NOU 2014: 11 Konkurranseklagenemda
NOU 2014: 16 Sjømatindustrien

Olje- og energidepartementet:

Samferdselsdepartementet:

Utenriksdepartementet:

Bestilling av publikasjoner

Offentlige institusjoner:
Departementenes sikkerhets- og serviceorganisasjon
Internett: www.publikasjoner.dep.no
E-post: publikasjonsbestilling@dss.dep.no
Telefon: 22 24 00 00

Privat sektor:
Internett: www.fagbokforlaget.no/offpub
E-post: offpub@fagbokforlaget.no
Telefon: 55 38 66 00

Publikasjonene er også tilgjengelige på
www.regjeringen.no

Trykk: 07 Aurskog AS – 11/2015

MILJØMERKET
241 Trykksak 379