NTNU
Det skapende universitet

Nasjonal satsing på informasjonssikkerhet

Geir Espen Narum Paulsberg

Master i kommunikasjonsteknologi
Oppgaven levert: Juni 2007
Hovedveileder: Jan Arild Audestad, ITEM
Biveileder(e): Tore Larsen Orderløkken, NorSIS

Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

Oppgavetekst

Norge er i dag svært avhengig av IKT innen mange sektorer. I takt med den stadige utbredelsen av IKT som arbeidsverktøy, er det interessant å betrakte hva myndighetene har gjort for å sørge for at informasjonssikkerheten er ivaretatt på nasjonalt nivå. Det er et stort sprik i hvordan norske virksomheter jobber med informasjonssikkerhet, og det eksisterer derfor et behov for en nasjonal koordinering på området. Kandidaten skal lage en oversikt over regjeringens satsing på informasjonssikkerhet.
Bakgrunnsmateriale som for eksempel bør benyttes er Riksrevisjonens rapport, stortingsmeldinger samt forslag fra andre råd og utvalg. Det skal utifra disse kildene lages en historisk oversikt over det arbeid som har vært utført innen informasjonssikkerhet i Norge. Blant faktorer som skal vurderes inngår implementerte tiltak og effekten av disse. Offentlige og private organisasjoner og miljøer med tilknytning til informasjonssikkerhet skal kartlegges sammen med deres prosjekter. Retningslinjer for hvordan disse organisasjonene bedre kan dra nytte av hverandre skal deretter utarbeides. Kandidaten skal også, i et begrenset omfang, undersøke hva andre land gjør innen informasjonssikring og hvor mye ressurser de bruker på det. Finnes det helhetlige satsinger på informasjonssikkerhet - og virker de?

Oppgaven gitt: 17. januar 2007
Hovedveileder: Jan Arild Audestad, ITEM

NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET
FAKULTET FOR INFORMASJONSTEKNOLOGI, MATEMATIKK OG ELEKTROTEKNIKK

MASTEROPPGAVE

Studentens navn: Espen Paulsberg

Tittel: Nasjonal satsing på informasjonssikkerhet

Oppgavetekst: Norge er i dag svært avhengig av IKT innen mange sektorer. I takt med den stadige utbredelsen av IKT som arbeidsverktøy, er det interessant å betrakte hva myndighetene har gjort for å sørge for at informasjonssikkerheten er ivaretatt på nasjonalt nivå. Det er et stort sprik i hvordan norske virksomheter jobber med informasjonssikkerhet, og det eksisterer derfor et behov for en nasjonal koordinering på området.

Kandidaten skal lage en oversikt over regjeringens satsing på informasjonssikkerhet. Bakgrunnsmateriale som for eksempel bør benyttes er Riksrevisjonens rapport, stortingsmeldinger samt forslag fra andre råd og utvalg. Det skal utifra disse kildene lages en historisk oversikt over det arbeid som har vært utført innen informasjonssikkerhet i Norge. Blant faktorer som skal vurderes inngår implementerte tiltak og effekten av disse.

Offentlige og private organisasjoner og miljøer med tilknytning til informasjonssikkerhet skal kartlegges sammen med deres prosjekter. Retningslinjer for hvordan disse organisasjonene bedre kan dra nytte av hverandre skal deretter utarbeides.

Kandidaten skal også, i et begrenset omfang, undersøke hva andre land gjør innen informasjonssikring og hvor mye ressurser de bruker på det. Finnes det helhetlige satsinger på informasjonssikkerhet — og virker de?

Innleveringsfrist: 14.06.2007

Innlevert: 14.06.2007

Institutt: ITEM: Institutt for telematikk

Hovedveileder: Jan Arild Audestad

Biveileder: Tore Larsen Orderløkken

Trondheim, 14. juni 2007

Jan Arild Audestad

Forord

Denne masteroppgaven ble skrevet våren 2007 som en avsluttende obligatorisk oppgave i det femårige sivilingeniør-/masterprogrammet i kommunikasjonsteknologi ved Norges teknisk-naturvitenskapelige universitet (NTNU). Den ble utført ved Institutt for telematikk (ITEM) og Norsk senter for informasjonssikring (NorSIS) på oppdrag av sistnevnte.

Jeg vil herved rette en takk til min veileder Tore Orderløkken ved NorSIS og hovedveileder Jan Audestad ved Institutt for telematikk ved NTNU for veiledning og innspill til oppgaven. Videre vil jeg benytte anledningen til å takke alle informanter i ulike departementer og organisasjoner som har bidratt med opplysninger, herunder:

Cort Archer Dreyer / FAD
Peter Wallström / Sitic
Christophe Birkeland / NSM
Morten Ween og Eirik Normann / NFR
Håvar Fridheim og Jan Erik Torp / FFI
Erik Hjelmås / NISlab
Jan Erik Østvang / KInS
Arne Røed Simonsen / NSR

Trondheim, juni 2007

Espen Paulsberg

Sammendrag

Samfunnets avhengighet til IKT har de siste årene økt dramatisk. Kritisk infrastruktur og kritiske samfunnsfunksjoner er blitt fullstendige avhengige av IKT. Myndighetene har i sammenheng med den økte avhengigheten utredet samfunnets sårbarhet som følge av IKT-avhengighet og iverksatt tiltak for å styrke informasjonssikkerheten.

Denne oppgaven har vurdert nasjonal satsing på informasjonssikkerhet gjennom å foreta: 1) en evaluering av sentrale utvalg nedsatt av regjeringen og oppfølgingen av disse, 2) en kartlegging av sentrale offentlige og private virksomheters arbeid og 3) en sammenligning av informasjonssikkerhetarbeid i utlandet opp mot Norge. Innledningsvis var det tenkt å sammenligne norske myndigheters innsats opp mot Sverige, Danmark og Nederland. På grunn av manglende respons fra NorSIS sine kontaktpersoner i dansk og nederlandsk CERT ble det kun foretatt en sammenligning med Sverige.

Det er i hovedsak brukt kilder i form av offentlig tilgjengelige dokumenter fra myndighetene og forvaltningen samt kontaktpersoner i relevante organisasjoner og andre institusjoner.

Denne rapporten tar for seg resultater fra fem sentrale arbeider i sammenheng med myndighetenes satsing på informasjonssikkerhet: Sårbarhetsutvalget, Infrastrukturutvalget, Datakrimutvalget, Nasjonal strategi for informasjonssikkerhet og Riksrevisjonens undersøkelse.

Sårbarhetsutvalget var det første utvalget som oppnådde nasjonal oppmerksomhet rundt informasjonssikkerhet i 1999. Utvalget vektla i sin rapport resultatene fra BAS2 prosjektet mer enn IKT-underutvalget som fokuserte på den logiske trusselen. På tross av et noe feil fokus ble det likevel opprettet et Senter for informasjonssikring for å kartlegge informasjonssikkerhetstrusselen i norske virksomheter. Dette senteret samt etableringen av en nasjonal strategi for informasjonssikkerhet er den viktigste arven fra Sårbarhetsutvalget. De fleste tiltakene som Sårbarhetsutvalget foreslo er i etterkant blitt implementert. Denne gode uttellingen må delvis tilskrives at også andre prosesser og aktiviteter pågikk samtidig med utvalgets utredning, og ikke minst at det nå har gått hele sju år siden rapporten ble avlevert.

Infrastrukturutvalget fulgte opp Sårbarhetsutvalgets arbeid og avla sin rapport i 2006, seks år etter sistnevnte utvalg. I Infrastrukturutvalgets rapport er fokus flyttet fra etablering av et helhetlige apparat rundt informasjonssikkerhet til organiseringen av myndighetenes arbeid, herunder ansvarsavklaring på departementnivå. At utvalget har kunnet tillate seg å skifte fokus fra etablering til organisering skyldes arbeidet som har foregått med Nasjonal strategi for informasjonssikkerhet. Arbeidet med denne strategien har blant annet ført til den permanente opprettelsen av NorSIS og NorCERT. Utvalgets rapport foreslår i hovedsak organisatoriske tiltak i offentlig sektor for å bedre oppfølgingen av tiltak, og man har delvis benyttet Riksrevisjonens undersøkelse som informasjonsgrunnlag for forslag til forbedringer. En annen utvikling som har funnet sted fra Sårbarhetsutvalget til Infrastrukturutvalget er at sistnevnte gjennom enkelte tiltak har rettet fokus også mot privatpersoner. Det er for tidlig å si hvilke konsekvenser Infrastrukturutvalgets anbefalinger har medført for myndighetenes arbeid med informasjonssikkerhet.

Sårbarhetsutvalget var inne på problemstillingen med en rask utvikling innen informasjonssikkerhetstusselen og et utdatert lovverk. Denne problemstillingen ble tatt opp av Datakrimutvalgets delutredning I og II i forbindelse med henholdsvis ratifisering av Europarådets datakrimkonvensjon og en særregulering for nasjonale straffebestemmelser om datakriminalitet. Norge måtte utføre få endringer i lovverket som følge av ratifiseringen av datakrimkonvensjonen. Konvensjonen ble ratifisert av Norge i 2006 og gir deltagerlandene felles definisjoner, straffebestemmelser, straffeprosessuelle bestemmelser og regler for internasjonalt samarbeid vedrørende datakriminalitet. Konvensjonen ble kritisert for å bruke meget vide og omfattende definisjoner som gir rom for at unødvendig mange handlinger og typer utstyr kriminaliseres. Videre ble konvensjonen kritisert av menneskerettighetsorganisasjoner og dataindustrien for ikke å ta nok hensyn til personvern. Internettilbyderne mente det var bekymringsverdig at konvensjonen åpnet for å pålegge tilbyderne å utføre overvåkning og ikke bare bistå politiet med teknisk kompetanse under slik overvåkning.

Datakrimutvalgets delutredning II og forslag til straffebestemmelser går på flere områder lenger enn det datakrimkonvensjonen krever. Utredningen presenterer mange positive forslag, herunder kriminalisering av spam. Likevel gir alle forslagene i sum et inntrykk av en lovgivning som vil være i overkant restriktiv. Grunnen til dette skyldes at utvalget har foreslått å kriminalisere en rekke forberedelseshandlinger, herunder elektronisk kartlegging og all befatning med skadelige dataprogrammer. Et meget kontroversielt mindretallsforslag vedrørende filtrering av Internett i henhold til Straffeloven er også inkludert i utvalgets rapport. Dersom alle utvalgets anbefalinger godkjennes av Stortinget, inkludert mindretallsforslaget om filtrering, vil dette føre til at Norge får en av de strengeste, om ikke den strengeste, internettlovgningingene i Vesten. En slik lovgivning er overhodet ikke hensiktsmessig.

Nasjonal strategi for informasjonssikkerhet har vært helt sentral i myndighetenes arbeid med å styrke samfunnets informasjonssikkerhet. Strategien lister tolv tiltak eller tiltaksområder myndighetene skal konsentrere sin satsing rundt. Tiltakene er fornuftige, men gjennom Riksrevisjonens undersøkelse har det kommet frem at oppfølgingen av strategien har lidd på grunn av mangelfull ansvarsavklaring blant annet på departementnivå. Mange av tiltakene er av tverrsektorielt omfang, og FAD har vært ansvarlig for disse. En tydeligere ansvarsfordeling presenteres i St.meld. nr. 17 (2006–2007) – "Eit informasjonssamfunn for alle" der det fremheves at ansvarsprinsippet og ansvarslinjene er de samme for arbeidet med informasjonssikkerhet som for annet sikkerhet- og beredskapsarbeid. Videre avklares det at FAD skal ha ansvaret for *forebyggende*, tverrsektorielle tiltak i motsetning til alle tverrsektorielle tiltak slik ansvarsfordelingen har vært antydet før. Den nasjonale strategien inneholder mange løpende tiltak, og det er blant annet disse som myndighetene ikke har fulgt godt nok opp. Det nevnes forøvrig at Riksrevisjonen gjennomgående var svært kritisk og lite positiv til innsatsen som ble gjort i oppfølgingen av tiltakene, hvilket inkluderer sikring av kritisk IKT-infrastruktur og organiseringen av myndighetenes arbeid generelt. En revidert strategi, eller "retningslinjer for informasjonssikkerhet" som sannsynligvis blir navnet, ventes offentliggjort i september 2007. Det medfører at nåværende strategi har vart i over ett år lenger enn det tidsperspektivet på 2–3 år som ble anbefalt. Det har vært vanskelig å evaluere graden av måloppnåelse i strategien siden tiltak ikke er knyttet opp mot måloppnåelse. Dette må utbedres.

Det finnes en rekke offentlige institusjoner som er involvert i myndighetenes arbeid med å styrke nasjonal informasjonssikkerhet. Organisasjonene NorCERT/VDI, NorSIS, KIS, FFI, PT og FFI er helt sentrale i dette arbeidet. De tre førstnevnte organisasjonene kom til på bakgrunn av eller ble innlemmet i Nasjonal strategi for informasjonssikkerhet.

NorCERT/VDI er ansvarlig for analyse av trusselbildet og hendelseshåndtering for virksomheter som er en del av kritiske infrastrukturer eller samfunnsfunksjoner. VDI hadde 10–15 tilkoblede virksomheter ved oppstart, og det kan stilles spørsmål ved hvorvidt et slikt begrenset utvalg kan være representativt for landets kritiske virksomheter.

NorSIS har siden kritikken fra Riksrevisjonen fått et endret mandat. Senteret har en stor jobb foran seg med å bringe blant annet kommunesektoren og mindre bedrifter opp på et tilfredsstillende nivå. Den svake informasjonssikringen som er i mindre virksomheter innen offentlig og privat sektor bekreftes av Mørketallsundersøkelsen 2003/2006 utført av Næringslivets sikkerhetsråd.

KIS har som koordinerende organ for informasjonssikkerhetsarbeidet ingen myndighet til å fatte vedtak. Likevel kan utvalget legge premisser for en bedre oppfølging av informasjonssikkerhetsarbeidet gjennom sine anbefalinger og i kraft av å være en en møteplass for sentrale aktører.

PT har et særskilt ansvar overfor infrastrukturer i telesektoren. Tilsynet har den siste tiden arbeidet med å sikre eksisterende samtraffikpunkter samt etablere nye regionale punkter mellom internettilbyderne. Det er på høy tid dette arbeidet blir gjennomført da disse punktene lenge har vært en kritisk del av IKT-infrastrukturen. PT har i oppgave å kontinuerlig kartlegge infrastruktur innen egen sektor samt utføre ROS-analyser i samarbeid med private aktører med ansvar for denne infrastrukturen. Det bemerkes at metodikken fra BAS5 prosjektet kan være nyttig for tilsynet i denne sammenheng, og at det derfor bør undersøkes i hvilket omfang metodikken kan nyttiggjøres. PT har forøvrig opprettet nettstedet nettvett.no, et informasjonstiltak rettet mot privatpersoner

samt mindre og mellomstore bedrifter.

FFI har vært en viktig aktør som har kommet med bidrag om samfunnets sårbarhet gjennom sine BAS prosjekter. BAS2 og BAS5 har fokusert på telesektoren og kritiske IKT-infrastrukturer. NSM og DSB hadde vanskeligheter med å samle inn nok midler for å starte BAS5 prosjektet som har hatt en tverrsektoriell profil. FFI sitt mandat bør slik som Infrastrukturutvalget anbefaler utvides til å omfatte sivil sektor. En utvidelse av mandatet vil sikre bedre kontinuitet i forskningsinnsatsen, forhindre tap av kompetanse samt gi en mer forutsigbar finansieringsmodell for fremtidige prosjekter.

Sverige har vært gjenstand for en raskere avmonopolisering enn Norge og de fleste andre europeiske land. Dette har gitt seg utslag i at Sverige har ligget noe foran Norge i å utrede samfunnets sårbarhet og IKT. Den raskere avmonopoliseringen som foregikk i Sverige rettferdiggjør ikke den ulike utviklingen landene hadde på 1990-tallet. Sverige økte jevnlig den økonomiske støtten til investeringer i nye sikringstiltak innen telesektoren under denne perioden. I Norge var utviklingen motsatt, og det ble i samme periode investert stadig mindre i nye tiltak. Idag har begge landene etablert et helhetlig apparat rundt informasjonssikkerhet med blant annet nasjonale CERTer, sertifiseringsordninger og tiltak innen bevisstgjøring. Til tross for at etableringen av dette apparatet har funnet sted så har landenes respektive riksrevisjoner påpekt en rekke mangler ved oppfølgingen av arbeidet med å styrke samfunnenes informasjonssikkerhet.

Infrastrukturutvalget har vært en helt sentral oppfølging av Sårbarhetsutvalgets arbeid, og begge utvalgene har forsøkt å gjøre en samlet vurdering av sårbarheten for alle samfunnssektorer. I Sverige hadde man i perioden 2005–2007 en egen utredning innen informasjonssikkerhet som bestod av fire ulike delutredninger. Informasjonssikkerhet er en tverrsektoriell problemstilling, og kraft- og telesektoren (herunder IKT-infrastrukturer) er de eneste sektorene som alle andre sektorer er kritisk avhengige av. Det er derfor synd at Norge ikke har fulgt Sveriges eksempel og nedsatt et utvalg med fokus utelukkende på informasjonssikkerhet.

Når et utvalg har et begrenset antall utvalgsmedlemmer, er det vanskelig å oppnå en bred og samtidig høy faglig kompetanse som sikrer at alle samfunnssektorer får bidratt med egen ekspertise på området. I Sårbarhetsutvalget hadde ingen av utvalgsmedlemmene IKT-bakgrunn. I Infrastrukturvalget var det et par personer med IKT-bakgrunn, hvorav én innen sikkerhet. I Datakrimutvalgets arbeid med delutredning II var det kun ett utvalgsmedlem som hadde bakgrunn innen IKT og informasjonssikkerhet. Resterende utvalgsmedlemmer var jurister. Sammensetningen av disse utvalgene avdekker en mangel på kompetanse i informasjonssikkerhet. Riktignok opprettet for eksempel Sårbarhetsutvalget et IKT-underutvalg for å oppnå et bedre beslutningsgrunnlag, men synspunktene fra dette underutvalget ble ikke vektlagt tilstrekkelig i sluttrapporten. All teknisk kompetanse er ikke like enkel å formidle til personer som ikke har den nødvendige bakgrunn innen fagområdet, og det er derfor viktig at kompetansen og de synspunkter som kommer til uttrykk gjennom den ivaretas på høyeste nivå, det vil si i utvalget selv. Hvis ikke risikerer man å tegne et bilde av tilstanden som ikke er korrekt, noe som igjen kan lede til at man utarbeider en lite hensiktsmessig eller feilaktig strategi på området.

Myndighetenes satsing gir inntrykk av at det vært iverksatt mange ulike tiltak, men at gjennomføringen og oppfølgingen av tiltakene har vært varierende. Mangelfull ansvarsavklaring og en utydelig arbeidsfordeling i den offentlige organisasjonsstrukturen har vært en medvirkende årsak til dette. Det understrekes at det også har skjedd mye positivt på området, og at mange tiltak har blitt gjennomført for å styrke informasjonssikkerheten. Det er likevel viktig at myndighetene arbeider for en mer effektiv oppfølging av tiltakene, og at man i denne oppfølgingen tar hensyn til at problemstillingene innen informasjonssikkerhet raskt endrer seg.

Innhold

Figurer

Tabeller

Forkortelser

AAD
: Arbeids- og administrasjonsdepartementet

AS
: Autonomt System

BAS
: Beskyttelse av samfunnet. Prosjektserie i regi av FFI.

CCRA
: Common Criteria Recognition Arrangement

DNS
: Domain Name System

DSB
: Direktoratet for samfunnssikkerhet og beredskap

ENISA
: European Network and Information Security Agency

EOS
: Etteretnings- og sikkerhetstjenesten

ETSI
: European Telecommunications Standards Institute

FAD
: Fornyings- og administrasjonsdepartementet

FD
: Forsvarsdepartementet

FFI
: Forsvarets forskningsinstitutt

FRA
: Försvarets radioanstalt

HiG
: Høgskolen i Gjøvik

IKT
: Informasjons- og kommunikasjonsteknologi

IKT SoS
: IKT sikkerhet og sårbarhet. Forskningsprogram for informasjonssikkerhet i regi av NFR.

IP
: Internet Protocol

ISP
: Internet Service Provider

ITU
: International Telecommunication Union

IX(P)
: Internet eXchange (Point) – Samtrafikkpunkt mellom Internettleverandører

JD
: Justis- og politidepartementet

KBM
: Krisberedskapsmyndigheten

NFR
: Norges forskningsråd

NHO
: Næringslivets Hovedorganisasjon

NISlab
: The Norwegian Information Security laboratory

NIX
: Norwegian Internet eXchange – Nasjonalt samtrafikkpunkt mellom Internettleverandører

NorCERT
: Norwegian Computer Emergency Response Team

NorSIS
: Norsk Senter for Informasjonssikring (tidligere SIS)

NOU
: Norges offentlige utredninger

NSM
: Nasjonal sikkerhetsmyndighet

NSR
: Næringslivets sikkerhetsråd

NTNU
: Norges teknisk-naturvitenskapelige universitet

NVE
: Norges vassdrags- og energidirektorat

ÖCB
: Överstyrelsen för civil beredskap

OECD

Organisation for Economic Co-operation and Development

PDS
Politiets datakrimsenter

PKI
Public Key Infrastructure

PST
Politiets sikkerhetstjeneste

PT
Post- og teletilsynet

PTS
Post- och telestyrelsen

ROS
Risiko- og sårbarhet

SD
Samferdselsdepartementet

SIS
Senter for informasjonssikring

SITIC
Sveriges IT-incident centrum

UD
Utenriksdepartementet

UiO
Universitet i Oslo

USIT
Universitetets senter for informasjonsteknologi (ved UiO)

VDI
Varslingssystem for Digital Infrastruktur

VoIP
Voice over IP

Kapittel 1

Innledning

1.1 Bakgrunn

IKT får en stadig viktigere og sentral rolle i samfunnet, og har samlet sett gått fra å være et nyttig verktøy for samhandling til å bli en av de mest kritiske komponentene i infrastrukturen vår. I dag ser vi at alle industrialiserte land er kritisk avhengige av den infrastrukturen som IKT kan realisere. Uten IKT stopper *hele* samfunnet i løpet av meget kort tid [1,2].

Historien om Internett begynte raskt å endre seg da World Wide Web (WWW) ble kommersielt tilgjengelig i 1993. Mot slutten av 1990 tallet hadde Internett allerede blitt en betydelig samfunnsfaktor. I den samme perioden bygde dot-com eventyret seg opp. I 2000 nådde eventyret toppen og boblen sprakk. I mars 2000 begynte aksjemarkedet å stupe, og nedgangen sluttet ikke før i 2002 [3]. Før boblen sprakk hadde IKT allerede gjort sitt inntog overalt i samfunnet, og fra ca. 2000 var all infrastruktur kritisk avhengig av IKT [2]. Trenden med samfunnets stadig økende avhengighet til IKT fortsetter den dag i dag.

En utvikling hvor stadig flere tjenester realiseres gjennom IKT innebærer mange fordeler. Problemene oppstår når tjenestenes IKT-infrastruktur er sårbar og/eller tjenestene selv ikke sikres godt nok. Sikkerhetsbrudd på en enkelt tjeneste vil som regel ha konsekvenser i et nokså begrenset omfang. Dette kan være svært alvorlig for den som rammes, men som oftest vil skaden være lokal. Rettes angrepet derimot mot kritisk IKT-infrastruktur kan dette få fatale konsekvenser for hele samfunnet.

Eksempler på kritiske IKT-infrastrukturer inkluderer søkemotorer og DNS (Domain Name System) tjenere. Det finnes et begrenset antall søkemotorer og DNS tjenere på Internett. Disse to komponentene, søk og DNS oppslag, er kritiske for at World Wide Web skal fungere. Angrep rettet mot disse tjenestene vil derfor kunne få svært dramatiske konsekvenser. Uten søkemotorer finnes ikke lenger noen helhetlig oversikt over alle nettsidene som er på Internett, og uten DNS tjenere vil ingen finne veien til de samme sidene selv om de har hele domenenavnet.

Fysiske og logiske IKT-infrastrukturer er sårbare av natur, og må derfor sikres fra tilsiktede og utilsiktede hendelser som kan gjøre skade. Ved å implementere effektive tiltak som beskytter mot logiske og fysiske angrep kan man oppnå en høy grad av informasjonssikring, noe som igjen vil øke robustheten.

Det er først de siste 7–8 [1] årene det har blitt satt et fokus på informasjonssikring fra regjeringens side. Dette fokuset er tvingende nødvendig for å forbedre og vedlikeholde informasjonssikkerheten i samfunnet. Sikkerhetsarbeid er en kontinuerlig prosess og ikke et produkt av en engangsinvestering [4].

Manglende eller svake informasjonssikkerhetstiltak av kritisk IKT-infrastruktur kan få katastrofale følger for befolkningen. Eksempler på konsekvenser kan være omfattende eller total svikt i funksjoner innen bankvesenet eller kraftforsyningen. I 2006 stoppet myndighetene en bankstreik ved tvungen lønnsnemnd [1]. Terskelen er høy for å ty til slike midler. Det at myndighetene griper inn for å stoppe en bankstreik, indikerer hvor kritisk bankvesenet er som infrastruktur i samfunnet. Truslene mot samfunnet kommer både innenfra og utenfra, og et angrep utenfra på kritisk IKT-infrastruktur for bankvesenet kunne fått like store, om ikke større konsekvenser for samfunnet enn en bankstreik.

Samtidig som IKT-tjenester funksjonelt sett må virke som forventet, er det viktig at de ivaretar sikkerheten. Systemer og tjenester må gjøres robuste gjennom informasjonssikring slik at brukerne kan ha tillit til de. Slutten på sikre IKT-tjenester vil bety slutten på brukergruppene av de samme tjenestene.

1.2 Problemstilling

Siden slutten av 1990 tallet og frem til idag har det vært nedsatt mange ulike utvalg, råd og komiteer som har drøftet nasjonal satsing på informasjonssikkerhet. Dette arbeidet har skjedd på bakgrunn av en forståelse om at samfunnet har blitt svært sårbart grunnet avhengighet til IKT. De mange arbeidene som har drøftet aspekter ved IKT og samfunnets sårbarhet, har resultert i et antall rapporter og andre dokumenter med anbefalinger om tiltak for å redusere denne sårbarheten.

Det finnes ingen helhetlig oversikt over disse arbeidene og hva som konkret har kommet ut av de. På bakgrunn av dette, er det ønskelig å fremstille en overordnet oversikt over sentrale arbeider og virksomheter i tilknytning til samfunnets sårbarhet som følge av IKT-avhengighet. Denne oppgaven skal derfor kartlegge og vurdere regjeringens nasjonale satsing på informasjonssikkerhet samt kartlegge andre virksomheter og miljøer som jobber med dette.

To spørsmål står sentralt i sammenheng med regjeringens nasjonale satsing. Det første og mest sentrale spørsmålet for oppgaven er: *"Hva gjør regjeringen for å bedre informasjonssikkerheten i samfunnet?"* For å svare på dette skal oppgaven svare på følgende spørsmål:

- Hvilke tiltak er foreslått i forskjellige utvalg nedsatt av regjeringen?
- Hvilke av de foreslåtte tiltakene er blitt implementert?
- Hva har graden av fremgang vært mellom de ulike utvalgene?
- Hva gjør offentlig sektor for å styrke informasjonssikkerheten i samfunnet?
- Hva gjør privat sektor for å styrke informasjonssikkerheten i samfunnet?

[1] Sårbarhetsutvalget ble nedsatt i 1999 og var det første utvalget som oppnådde nasjonal oppmerksomhet rundt informasjonssikkerhet i Norge.

Det andre spørsmålet som skal besvares i sammenheng med regjeringens nasjonale satsing er: *"Hva gjør Norge i forhold til Sverige for å satse på informasjonssikkerhet?"*. For å besvare dette spørsmålet skal oppgaven finne svar på følgende:

- Hvilke tiltak er foreslått og implementert i Sverige for å bedre informasjonssikkerheten?
- Hvordan skiller arbeidet med informasjonssikkerhet seg i Sverige fra det som skjer i Norge?

Oppgaven skulle opprinnelig sammenligne Norges satsing med flere andre land, men på grunn av fraværende respons har dette ikke vært mulig.

1.3 Avgrensninger

Denne oppgaven vurderer myndighetenes nasjonale satsing på informasjonssikkerhet. Oppgaveteksten er relativt omfattende og det har derfor blitt foretatt enkelte avgrensninger.

Myndighetenes satsing på informasjonssikkerhet evalueres blant annet gjennom å vurdere nedsatte utvalg og deres rapporter. Oppgaven har fokusert på sentrale utvalg i nyere tid og antall utvalg ble begrenset til tre stykker for å kunne gjennomføre en grundig evaluering av disse. I tillegg til disse tre utvalgene er Nasjonal strategi for informasjonssikkerhet og Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur også evaluert.

Det eksisterer et relativt stort antall offentlige og private organisasjoner i Norge som på ulike måter er involvert i arbeidet med å styrke nasjonal informasjonssikkerhet. Oppgaven kartlegger og omtaler de mest sentrale av disse med størst fokus på organisasjoner i offentlig sektor siden oppgaven primært omhandler myndighetenes og offentlig sektors satsing. Utarbeidelse av retningslinjer for hvordan organisasjonene bedre kan dra nytte av hverandre er utelatt fra oppgaven for å vie mer tid til evaluering av nedsatte utvalg og kartlegging av organisasjoner og deres arbeider.

I oppgaveteksten heter det at kandidaten i et begrenset omfang skal undersøke andre lands satsing innen informasjonssikkerhet. Å kartlegge hva flere andre land gjør ned til samme detalj som gjøres for Norge har naturligvis ikke vært mulig med tiden som har vært til disposisjon. Hensikten har derfor vært å foreta en mer overfladisk vurdering av satsingen på informasjonssikkerhet i et utvalg av andre land. Kandidaten har sendt forespørsler til tre av NorSIS sine kontaktpersoner i nasjonale CERTer i henholdsvis Sverige, Danmark og Nederland. På grunn av fraværende respons fra Danmark og Nederland har det ikke vært mulig å kartlegge disse landenes arbeid med å styrke nasjonal informasjonssikkerhet. Kontakten med den nasjonale CERTen i Sverige (Sitic) har derimot vært meget god.

1.4 Metode

En metode kan karakteriseres som en strukturert måte å nå et mål på. Metodene som brukes i denne oppgaven faller inn under kategoriene innsamling, vurdering og sammenligning av informasjon. I tillegg blir også intervju brukt som metode. Litteraturanalyse og intervju er sentrale kjennetegn på kvalitative tilnærminger [5].

Målet med metodene som blir brukt i oppgaven er å formidle en *forståelse* av hva som er blitt gjort for å satse på informasjonssikkerhet. Metodene vil bruke relativt få informanter eller kilder, men vurdere materiale med mange opplysninger i dybden.

Oppgavens første mål er å foreta en dybdeundersøkelse av nasjonal satsing på informasjonssikkerhet. For å kartlegge hva som er gjort fra regjeringens side vil det benyttes rapporter fra utvalg, stortingsmeldinger samt forslag fra andre råd og utvalg. Offentlig informasjon publisert av andre land vil også bli brukt. Internett og personer i relevante fagmiljøer vil i hovedsak utgjøre kildene til oppgaven.

Det andre målet i oppgaven er å foreta en sammenligning av satsing på informasjonssikkerhet i Norge opp mot andre land. Denne sammenligningen vil kun skje opp mot ett land. Målet er her ikke å gå i bredden og trekke konklusjoner på et statistisk grunnlag, men å diskutere enkelte tiltak som utføres i utlandet opp mot våre egne.

Sett i lys av karakteristikkene til metodene som vil bli brukt, karakteriseres den overordnede tilnærmelsen til denne oppgaven som kvalitativ.

1.5 Oppbygging

Resten av denne rapporten er organisert som følger: kapittel 2 definerer begrepet informasjonssikkerhet, gir eksempler på kritiske infrastrukturer i Internett og gjennomgår trusselbildet og de endringer som har skjedd i tilknytning til dette.

Kapittel 3 beskriver innholdet og oppfølgingen av tiltakene i rapportene fra Sårbarhetsutvalget, Infrastrukturutvalget og Datakrimutvalget. I kapittel 4 beskrives Nasjonal strategi for informasjonssikkerhet og Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur. Fordi diskusjonene og konklusjonene rundt disse utvalgene og de andre sentrale arbeidene er relativt omfattende, gjengis de i de respektive kapitlene istedenfor i den endelige diskusjonen og konklusjonen bakerst i rapporten.

Offentlige og private institusjoner som er en del av arbeidet med å styrke nasjonal informasjonssikkerhet, kartlegges i henholdsvis kapittel 5 og 6. Ansvarsområde og arbeider utført av den enkelte institusjon omtales også i disse kapitlene.

Kapittel 7 omhandler Sveriges satsing på informasjonssikkerhet. Kapittelet gir en oppsummering av foreslåtte tiltak i sentrale utredninger vedrørende informasjonssikkerhet på myndighetsnivå. Det indikeres også hvilke av tiltakene som er implementert.

I kapittel 8 diskuteres de innledenede forskningsspørsmålene før det konkluderes i kapittel 9.

Kapittel 2

Informasjonssikkerhetstrusselen

Dette kapittelet beskriver IKT-trusselbildet og de endringer som har foregått i tilknytning til dette bildet de siste årene. Innledningsvis defineres begrepet "informasjonssikkerhet" og det blir gitt eksempler på kritiske IKT-infrastrukturer i Internett. Det gis deretter en introduksjon til utviklingen som har foregått med å modellere Internett ved hjelp av grafteori og betydningen av dette for kartlegging av kritisk IKT-infrastruktur. Videre følger en oppsummering av NorCERT/VDI sine ugraderte trusselvurderinger for nyere tid, før trusselen vedrørende botnett blir viet særskilt oppmerksomhet på slutten av kapittelet.

Definisjoner

Før informasjonssikkerhetstrusselen kan drøftes, må begrepet informasjonssikkerhet defineres. Tradisjonelt har begrepet vært knyttet til akronymet CIA, hvilket er en forkortelse for confidentiality, integrity og availibility. På norsk blir dette henholdsvis konfidensialitet, integritet og tilgjengelighet. Disse tre egenskapene hindrer henholdsvis innsyn fra uvedkommende i data, modifisering av data utført av uvedkomne og angrep eller feil som resulterer i at et system blir utilgjengelig (Denial of Service).

Nasjonal strategi for informasjonssikkerhet fremhever at tilgjengelighet og integritet som regel er de viktigste egenskapene i myndighetenes arbeid med å beskytte kritisk IKT-infrastruktur.

Det kan argumenteres for at også andre begreper bør knyttes til definisjonen av informasjonssikkerhet. Autentisering, autorisasjon og ikke-benekting er eksempler på slike begreper.

I denne rapporten brukes begrepene IT-sikkerhet og IKT-sikkerhet med tilsvarende mening som informasjonssikkerhet. Begrepene IT-infrastruktur og IKT-infrastruktur brukes synonymt.

Om kritisk infrastruktur i Internett

Begrepet kritisk IKT-infrastruktur brukes hyppig i denne oppgaven, og det nevnes derfor her noen eksempler på hva slik infrastruktur konkret kan være.

Eksempler på kritisk IKT-infrastruktur i Internett inkluderer rutere, transportnett, aksessnett, IXPer (Internet eXchange Point), DNS (Domain Name System) tjenere og søkemotorer.

Et transportnett kobler sammen aksessnett med ulik geografisk beliggenhet, mens aksessnettene knytter brukerne opp mot transportnettet slik at data kan sendes over større avstander.

IXP er en infrastruktur som som tillater ISPer å sende data direkte mellom hverandres autonome systemer (AS). Meningen med dette er å unngå at ISPene må sende trafikk via nettverk tilhørende en tredjepart. Hvis to ISPer må sende data til hverandre via en tredjepart, vil dette føre til økte kostnader og høyere forsinkelser for trafikken. I Norge heter den primære IXPen Norwegian Internet eXchange (NIX) og befinner seg i Oslo.

DNS tjenere gjør oppslag i registre for å avdekke IP adressen bak et domenenavn. Slike tjenere kan også oppgi epost tjenere som er ansvarlige for å motta epost for et visst domene. Både domenenavnene og DNS tjenerne er organisert i hierarkier. For hvert nivå i domenehierarkiet finnes det et sett med DNS tjenere som er ansvarlige for dette domenet.

Søkemotorer indekserer nettsider på Internett ved hjelp av søkeroboter. Robotene leter rundt på Internett etter nye nettsider og legger de til i søkemotorens database.

Informasjonssikkerhetstrusselen

Informasjonssikkerhetstrusselen slik den fremstår i dag er en relativt ny problemstilling. For 10–15 år siden var samfunnet slett ikke kritisk avhengig av IKT i infrastrukturen [2]. I dag er derimot situasjonen en helt annen.

IKT er sammen med elektrisitet blitt den faktoren som er aller viktigst for at alle andre sektorer skal kunne løse sine oppgaver [2]. Dette betyr at samfunnsfunksjonene nå er kritisk avhengige av to komponenter istedenfor én, slik det var tidligere. IKT og kraftforsyningen er i tillegg gjensidig avhengige av hverandre, noe som ytterligere øker samfunnets sårbarhet. Dette er prisen som samfunnet betaler for forenkling, effektivisering og modernisering.

I takt med Internetts utbredelse har informasjonssikkerhetstrusselen gått fra å være primært fysisk til å bli primært logisk. I dag representerer den logiske trusselen langt mer realistiske og farlige angrep enn rent fysiske angrep. Et logisk angrep kan komme fra hvor som helst, hvem som helst og når som helst. Den ansvarlige for angrepet kan være et enkeltindivid, en gruppe/organisasjon eller en stat. IKT åpner for en type krigføring som er teknologibasert asymmetrisk. I disse begrepene ligger det at angriperen kan være et enkeltindivid eller en organisasjon, befinne seg langt vekk fra målet, være i stand til å kamuflere seg selv (bruke andres datamaskiner som plattform for angrepet) og at han kan nekte skyld (hevde at andre brukte hans datamaskin til å utføre angripet). Mengden personer som i dag kan utgjøre en logisk trussel mot IKT installasjoner er langt større enn antallet personer som kan utgjøre en fysisk trussel for de samme installasjonene. I tillegg vokser den førstnevnte gruppen av datakyndige mennesker svært raskt.

I tillegg til fysiske og logiske angrep er social engineering eller sosiale angrep en tredje kategori av angrep. Denne typen angrep går ut på å få personer til å avsløre konfidensiell informasjon eller utføre visse handlinger. Phishing er en type angrep som faller innunder denne kategorien.

Det er ikke alltid mulig å spore et logisk dataangrep. Dette er for eksempel tilfellet hvis det ikke føres logger eller loggene slettes etter kun kort tid på de maskinene som angriperen måtte nyttegjøre seg av for å nå målet. Det er heller ikke alltid mulig å finne et klart motiv for angrepet. Angriperen kan ha ett bestemt mål, men kan også ramme blindt. Et eksempel på angrep som rammer blindt er ormer og såkalte “script kiddies”. Slike personer benytter

ofte programmer som er fritt tilgjengelig på Internett for å bryte seg inn på maskiner med spesifikke sikkerhetshull.

Effekten av et dataangrep varierer ettersom hva målet er. IKT kan brukes som et verktøy for å angripe alle IKT-avhengige sektorer. Avhengigheter mellom sektorer kan lede til en dominoeffekt ved bortfall av kritiske funksjoner i én enkelt sektor.

Internett har lenge hatt rykte for å være robust mot angrep og feil. Dette er riktig hvis det er snakk om angrep som rammer tilfeldige noder eller linker i nettverket. Det finnes intet såkalt "single point of failure" i Internett, og en mer eller mindre tilfeldig vekstutvikling har gitt god redundans i nettet på mange steder.

De siste sju årene har det blitt gjort forsøk på å modellere Internett ved hjelp av grafteori [2]. Man har kommet fram til en modell som godt tilnærmer Internetts struktur, såkalte skalafrie nettverk. Navnet kommer av at disse nettverkene ikke har én enkelt kantfordeling (eller skala) for alle nodene, men at kantfordelingen varierer sterkt mellom nodene i nettverket. Skalafrie nettverk forekommer ofte i naturen og kjennetegnes ved at endel noder i nettverket opptrer som nav (engelsk: hub) med svært høy konnektivitetsgrad, mens de fleste nodene har lav konnektivitetsgrad. Egenskapene til skalafrie nettverk er de samme uavhengig av antall noder i nettverket. Den viktigste egenskapen er at kantfordelingen kan tilnærmes ved følgende negativ eksponensial fordeling $P(k) \sim k^{-\gamma}$, hvor γ som regel befinner seg i intervallet $(2, 3)$ [6]. En annen viktig egenskap er at klyngekoeffisienten minsker når kantfordelingen øker [6]. Denne fordelingen er også en negativ eksponensial fordeling. Egenskapen gjør at noder med få kanter blir funnet i tette delgrafer og at disse delgrafene er koblet sammen med hverandre gjennom nav [6].

Det som gjør skalafrie nettverk ekstra sårbare er ikke tilfeldige angrep (eller fjerning) av noder, men rettede angrep. Angrep kan rettes mot den *strukturelle sårbarheten* i nettverket, nemlig navene. Kjenner man til nettverksstrukturen er det enkelt å angripe navene slik at et stort antall nettverkskoblinger faller ut og nettverket fragmenteres.

En annen svakhet med skalafrie nettverk er at smitte sprer seg svært raskt i de. Den hurtige spredningen skyldes at navene viderefører smitten til sine mange tilknyttede noder. Strukturen i slike nettverk gjør at tiden det tar å infisere hele nettverket ikke er så mye lenger enn tiden det tar å infisere det første navet [2]. Den raske spredningen gjør at man ikke har tid til å utvikle tiltak etter infeksjonen er oppdaget. Istedenfor er man nødt til å sette lit til proaktive tiltak. I IKT sammenheng kan et proaktivt tiltak være et antivirus program basert på signaturskanning samt heuristiske metoder for deteksjon av nye virus/ormer.

Det at Internett er et skalafritt nettverk har betydning for hvordan kritisk IKT-infrastruktur bør sikres. Mange av samfunnsfunksjonene bruker Internett som infrastruktur eller har en egen infrastruktur som er koblet opp mot Internett. I begge tilfeller kan infrastrukturen som nyttes betegnes som en del av Internett. I lys av de fremskrittene som er gjort vedrørende grafteori og Internett de siste årene, er det viktig at den strukturelle sårbarheten i den delen av nettet som fysisk er innen landegrensene utredes. En slik utredning bør ha som mål å kartlegge og kategorisere all kritisk IKT-infrastruktur, samt foreslå tiltak for å gjøre den kritiske infrastrukturen tilstrekkelig robust.

Ugraderte trusselvurderinger fra NorCERT/VDI

NorCERT/VDI [1] utgir månedlige ugraderte trusselvurderinger basert på egne vurderinger av intern informasjon fra VDI og andre eksterne kilder. I rapporten inkluderer NorCERT en pulsindikator på trusselbildet fra 1 til 5. I 2006 var denne denne pulsen stort sett på én, med unntak av visse perioder der man avdekket at sikkerhetshull aktivt ble utnyttet i Norge. I slike perioder ble trusselnivået rangert til to.

I 2007 nådde pulsindikatoren nivå tre i slutten av mars og i april som følge av to kritiske sikkerhetshull i Microsoft Windows. Samme måned ble også Estland utsatt for det som fremstår som et politisk motivert og massivt tjenestenektangrep mot de fleste departementene, parlamentet og politiet [7].

NorCERT presenterer visse trender i trusselbildet for 2006 i [8]. Det blir sagt at økonomisk motiverte dataangrep er et område som er øker stort i antall. Ofte brukes botnett for å samle inn store mengder sensitiv informasjon fra et kommandosenter. Eksempler på sensitiv informasjon som ofte stjeles er innloggingspassord til nettbanker, auksjonssider og andre nettsteder der det foretas transaksjoner.

Det påpekes at angrepsmetodene har blitt stadig mer avanserte, og at det er blitt vanskeligere å oppdage om det er installert ondsinnet programvare på datamaskinene på grunn av kamuflasjeteknikker.

Tjenestenektsangrep er et annet område som også brukes mer i økonomisk motiverte sammenhenger. Motivet er gjerne å tjene penger ved hjelp av elektronisk utpressing: ofrene får valget mellom å betale eller få gjentatte tjenestenektsangrep rettet mot seg. Når virksomheten er avhengig av IKT i den daglige driften, blir det vanskelig for nettstedene å nekte og betale siden systemene deres vil gå ned, hvilket resulterer i tapt omsetning og tapte penger for å gjenopprette normal drift. Også ved tjenestenektsangrep brukes botnett av angriperen. Med et stort nettverk av infiserte maskiner til sin disposisjon, oppnår angriperen en enorm samlet båndbredde som kan brukes til masseutsendelse av data mot målet.

Phishing er et annet område som også har opplevd en stor økning i aktivitet. Phishing er en form for svindel som gjennomføres ved at man etablerer nettsteder som tilsynelatende er like nettsidene til legitime institusjoner slik som banker. Ofte starter svindelen med at man mottar epost som tilsynelatende er fra en legitim institusjon. I eposten blir man henvist til en nettside for å bekrefte personopplysninger og annen sensitiv informasjon slik som nummer på VISA-kort. Ofte blir det skrevet at brukeren må bekrefte opplysningene på grunn av at nettstedet har endret sikkerhetsrutiner eller har lidd tap av data som følge av feil. Over 90% av alle forsøk på phishing er rettet mot finansielle institusjoner [8].

Om botnett

Som det kommer frem av NorCERT sin trusselvurdering er botnett en sterkt økende trussel. NorSIS [2] er enig i denne oppfatningen [9]. Botnett har fått en markant økning i tilknytning til økonomisk motivert kriminalitet den siste tiden. Kriminelle kan bruke botnett for å drive utpressing og true med tjenestenektsangrep dersom pengene ikke utbetales. De kan også bruke botnett for å samle inn sensitive opplysninger fra enorme nettverk av infiserte

[1] Norwegian Computer Emergency Response Team og Varslingssystem for Digital Infrastruktur.
[2] Norsk senter for informasjonssikring.

maskiner eller drive masseutsendelse av spam. McAfee har sagt at de største botnettene til og med kan true den nasjonale infrastrukturen i de fleste land [10, kap. 1]. På grunn av botnettenes skadelige potensiale vies de her særskilt oppmerksomhet.

Programvaren som gjør det mulig å realisere et botnett er ofte modulbasert og kan bestå av moduler med ulike formål [10, kap. 1]. Det at botnett er modulbaserte og adaptive gjør utfordringen med å bekjempe de enda større. Én type modul kan avdekke sårbarheter og ta kontroll over maskinen. Deretter kan denne laste ned en annen type modul som kan stoppe antivirus og ta ned brannmurer før en tredje modul lastes ned som søker etter andre sårbare maskiner [3]. På toppen av botnettverket sitter et kommandosenter med én eller noen få personer som har kontroll over alle de infiserte maskinene. Maskinene i bottnettverket laster ned en IRC bot [4] når de blir infisert. IRC boten som automatisk oppretter kommunikasjon med kommandosentralen. På denne måten mottar maskinene i botnettet sine ordre fra kommandosentralen.

Botnett har vokst i det skjulte og blitt en stor trussel mot samfunnet. De er blitt de kriminelles nye våpen i informasjonsalderen. Den første ormen som benyttet IRC for å kontrollere andre maskiner ble oppdaget i 1999 [10, kap. 1]. Etter denne har det vært et mange nye utviklinger, deriblant SpyBot som er en avansert form for spyware som kan utføre logging av tastaturtrykk, data mining etter epost adresser og andre oppgaver.

Da botnett ble et utbredt problem prøvde man å bekjempe de ved å lokalisere og ta ned kommandosentrene. Etter en tid er det nå blitt tatt i bruk bruk peer-to-peer teknologi og DDNS (Dynamic DNS) for å unngå svakheten med et sentralisert kommandosenter. En distribuert arkitektur gjør det vanskelig å spore opprinnelsen til botnettverket, og DDNS tillater kommandosentralen(e) å endre IP adresse(r) slik at botnettet alltid kan finne tilbake til sin eier og en ny kommandosentral selv om den primære sentralen blir tatt ned.

I september 2006 ga Symantec ut en trusselvurdering vedrørende Internett. Under perioden januar til juni i 2006 ble det observert nesten 58,000 aktive maskiner i bottnettverk fra dag til dag. Totalt ble rundt 4,5 millioner unike maskiner observert aktive i bottnettverk i den samme perioden [10, kap. 1]. Det kan være vanskelig å oppdage aktive maskiner som deltar i bottnettverk, og ofte oppdages ikke disse før kommandosentralen beslutter at de har utspilt sin rolle. De blir da utelatt fra botnettet, og først på dette tidspunktet kommer restene av den ondsinnede programvaren lett til syne. Dette gjør det sannsynlig at antall infiserte maskiner på internett langt overstiger 4,5 millioner [10, kap. 1].

Bottnettverk kan anta enorme dimensjoner, noe følgende eksempler fra virkeligheten illustrerer.

- I 2004 oppdaget Telenor et botnett med 10,000 maskiner og fikk lokalisert og stoppet kommandosentralen.
- I 2006 ble det oppdaget et botnett med 70,000 maskiner under kontroll av russere. Nettverket ble brukt til masseutsendelse av spam og til såkalt "pump and dump" av aksjer slik at aksjeprisene ble drevet opp før aksjebeholdningen ble solgt [10, kap. 1].

[3] AgoBot fra 2002 er basert denne inndelingen av moduler.

[4] IRC (ro)bot eller bare bot er et program som kan automatisere en rekke oppgaver på vegne av brukeren når den er tilknyttet et IRC nettverk.

➢ I 2005 ble det oppdaget et enormt botnett bestående av hele 1,5 millioner maskiner under kontroll av nederlendere. Tre personer ble tiltalt i saken. De tiltalte hadde tidligere konstruert et botnett på oppdrag fra den litauiske mafiaen [10, kap. 1].

Det at botnettene kan bli store nok til å true nasjonal infrastruktur eller deler av sådan er en skremmende tanke, og det må derfor arbeides med å stoppe oppbyggingen av slike nettverk. Det virker som om mange av maskinene i botnett kjører eldre versjoner av operativsystemer som ikke jevnlig oppdateres med sikkerhetsoppgraderinger.

Selv personer som er meget bevisste på informasjonssikkerhet kan oppleve at ondsinnede bryter seg inn i systemene deres. Sikkerhetshull i operativsystemer og annen programvare er noe man sannsynligvis må leve med langt inn i framtiden også. Et mottiltak mot botnett er å drive bevisstgjøring, slik at ihvertfall majoriteten garderer seg ved å installere sikkerhetsoppdateringer og annen sikkerhetsprogramvare.

Dessverre er den ondsinnede programvaren som bygger opp botnettene ofte avansert nok til å infisere kjerne i operativsystemet. Med en gang kjernen er kompromittert, er det ikke lenger mulig å stole på at man er i stand til å detektere og fjerne den ondsinnede programvaren. Dette er én faktor som tilsier at tiltak bør iverksettes andre steder.

Mange Internettilbydere og aktører i telesektoren med ansvar for IKT-infrastruktur merker en stor økning av trafikk fra botnett. Telenor så et eksempel på dette i 2004 da de avdekket et botnett på 10,000 maskiner. I 2006 fikk et nasjonalt teleselskap i Sentral-Amerika også erfare konsekvensene av å bli dominert av botnett. Selskapet opplevde flere brudd i nettverket, hvorav noen varte i opptil seks timer. I tillegg mistet minibanker forbindelsen i lengre perioder. På grunn av disse problemene fikk mange bedrifter alvorlige driftsforstyrrelser og -avbrudd, og selskapet mottok tusenvis av kundeklager og ble også truet med søksmål [11].

McAfee utvikler antivirus og innbruddsforebyggende løsninger og fikk i oppdrag å stoppe trafikken fra disse botnettene. Dette ble gjort ved å installere et Network Intrusion Prevention System (NIPS). Systemet viste seg å være effektivt og man fikk blokkert og stoppet nesten all trafikk fra botnettene.

Flere aktører benytter seg av slike systemer for å hindre at nettverkene deres overbelastes av botnett. I kampen mot botnettene er det viktig at privatpersoner og bedrifter sikrer seg så godt de kan på egenhånd. Samtidig er det minst like viktig at Internettilbydere og andre aktører i telesektoren selv iverksetter tiltak, og da særlig de med et ansvar for nasjonal kritisk IKT-infrastruktur.

Det er sannsynlig at Telenor har en eller annen form for Network Intrusion Prevention System, selv om det ikke har vært mulig å få bekreftet dette.

Kapittel 3

Regjeringsnedsatte utvalg om informasjonssikkerhet

3.1 Introduksjon

Dette kapittelet tar for seg de mest sentrale utvalg nedsatt av regjeringen med relevans for satsing på nasjonal informasjonssikkerhet. Det har vært gjort et bevisst valg med å primært fokusere på utredninger fra utvalg istedenfor stortings-/odelstingsmeldinger og -innstillinger. Dette valget er gjort fordi rapportene fra slike utredninger beskriver den aktuelle problemstillingen både i bredde og dybde. Oppfølgingen som kommer i form av stortings-/odelstingsmeldinger og -innstillinger kan ofte karakteriseres som mindre sammendrag av utredningene og mister noe av dybden i materialet.

For å oppnå en best mulig innsikt i den aktuelle problemstillingen er det naturlig å gå nærmest mulig den opprinnelige kilden. Under arbeidet med å foreta utredninger er utvalgsmedlemmene ofte i direkte konktakt med virksomheter, ledere og andre relevante kilder. Det er følgelig naturlig å hevde at utvalgene utarbeider sine anbefalinger på et mer omfattende og presist beslutningsgrunnlag enn eksempelvis stortingsrepresentanter som primært nyttiggjør seg av stortingsmeldinger for å fatte vedtak. Etter en utredning er foretatt av et utvalg, blir det utarbeidet en stortings-/odelstingsmelding av det ansvarlige departementet på bakgrunn av utredningens anbefalinger. Departementet vekter mange ulike hensyn opp mot hverandre slik som for eksempel organisatoriske eller økonomiske forhold i den sektoren departementet er ansvarlig for. En slik vekting av ulike hensyn vil i praksis si å legge begrensninger eller restriksjoner på utvalgets anbefalinger. På bakgrunn av denne tankegangen er regjeringsnedsatte utvalg valgt som den primære informasjonskilden i første del av denne oppgaven.

Utvalgene som drøftes i oppgaven har tatt for seg informasjonssikkerhet, sårbarhet og beredskap. Rapportene fra disse utvalgene dekker ulike typer tiltak av fysisk, logisk og juridisk karakter og illustrerer således nødvendigheten av å bedre informasjonssikkerheten på flere ulike arenaer.

For hvert utvalg er det gjort en sammenfatning av de mest sentrale tiltakene som ble foreslått av de enkelte utvalgene. Naturligvis er det kun tiltak som har relevans for denne oppgaven som inkluderes. Etter sammenfatningen av de enkelte utvalgenes forslag

til tiltak, følger en diskusjon rundt oppfølgingen av tiltakene. Konklusjonen oppsummerer de foreslåtte tiltakene og hvilke som er blitt implementert. Utvalgene som diskuteres i denne rapporten er gjengitt i tabell 3.1.

Utvalg	Periode	Oppdragsgiver
Sårbarhetsutvalget	September 1999 – juli 2000	JD
Infrastrukturutvalget	Oktober 2004 – april 2006	JD
Datakrimutvalget (delutredning I)	Januar 2002 – november 2003	JD
Datakrimutvalget (delutredning II)	September 2005 – februar 2007	JD

Tabell 3.1: *Liste over regjeringsnedsatte utvalg som drøftes i denne rapporten. Alle utvalgene har hatt Justis- og politidepartementet som oppdragsgiver.*

Å kartlegge hvordan de enkelte tiltakene fra en utredning har blitt fulgt opp er en vanskelig prosess. Etter et utvalg har foretatt sin utredning, utarbeider det ansvarlige departementet en stortings-/odelstingsmelding som sendes til henholdsvis Stortinget/Odelstinget. På Stortinget/Odelstinget blir det formet en komité som har i oppgave å utarbeide en innstilling. Når denne innstillingen er ferdig, blir det foretatt en avstemning på Stortinget/Odelstinget. Saksgangen er illustrert i figur 3.1.

Prosessen handler om å konsentrere stoffet som blir presentert i utredningen til en innstilling med forslag som Stortinget kan stemme over. Disse forslagene kan være svært konkrete, men også av en generell karakter. Det at endel foreslåtte tiltak er av generell karakter, og også av tverrsektorielt omfang, gjør det spesielt vanskelig å vurdere effekten av de. Videre kan det ofte gå svært lang tid før tiltak i stortingsmeldinger eller -innstillinger realiseres. Et eksempel på dette beskrives i sluttrapporten til prosjektet "Beskyttelse av samfunnet 5" (BAS5) i regi av Forsvarets forskningsinstitutt. Et tidligere prosjekt fra FFI i samme serie, BAS2, fikk en svært lite effektiv oppfølging. En av hovedgrunnene til dette var dårlig forvaltningsskikk [13, kap. 3.3].

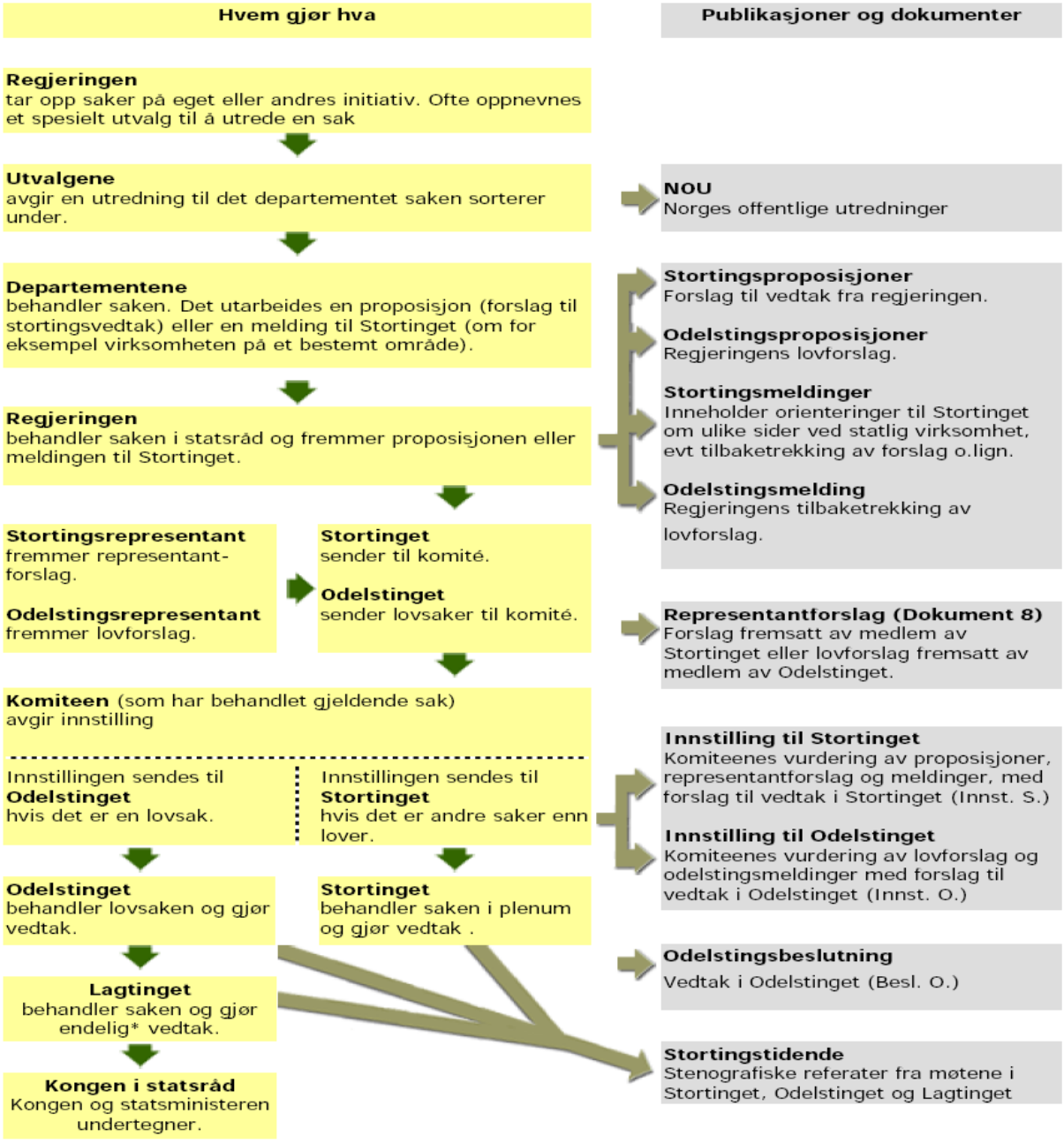
Når en innstilling eller proposisjon godkjennes i Stortinget, er det opp til Riksrevisjonen å vurdere arbeidet som har skjedd i etterkant av innstillingens godkjennelse. Riksrevisjonen er Stortingets kontrollorgan og har et uavhengig forhold til forvaltningen. Sammensetningen av Riksrevisjonen er tverrfaglig, og organisasjonen opererer med tre revisjonstyper: regnskapsrevisjon, forvaltningsrevisjon og selskapskontroll.

3.2 Sårbarhetsutvalget

3.2.1 Bakgrunn

Sårbarhetsutvalget ble nedsatt 3. september 1999 av regjeringen Bondevik I. Utvalgets utredning var ferdigstilt og ble avgitt til Justis- og politidepartementet 4. juli 2000. Utredningen ble kjent som NOU 2000: 24 og hadde tittelen "Et sårbart samfunn: Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet".

Målet med utredningen var å utrede sårbarheten og beredskapen i det norske samfunn. På bakgrunn av denne utredningen skulle utvalget foreslå tiltak for å redusere sårbarheten og forbedre beredskapen slik at samfunnet kunne ha en akseptabel sikkerhet mot uforutsette og negative hendelser. Utvalget ble bedt om å "gi en helhetlig beskrivelse av risikoen for



Figur 3.1: *Saksgangen mellom regjeringen og Stortinget [12].*

ekstraordinære påkjenninger mot det sivile samfunnet i fred, sikkerhetspolitiske kriser og krig" [14]. Et viktig punkt var å finne ut hvordan den sivile beredskapen burde organiseres i fremtiden.

Sårbarhetsutvalget benyttet tidligere forskning og analyser på områder der slikt fantes. På andre områder måtte utvalget selv gjennomføre egne analyser. Blant annet ble et eget underutvalg opprettet for å analysere sårbarheten for brudd i kritisk IKT-infrastruktur. En underveis rapport fra et underutvalg i NHD (Samfunnets sårbarhet som følge av avhengighet til IT) ble også avlevert til Sårbarhetsutvalget. Denne spilte en viktig rolle i Sårbarhetsutvalgets analyse av IKT-sårbarhet. En bredt sammensatt referansegruppe støttet utvalget under sitt arbeid. Utvalget besøkte flere organisasjoner i USA, Sverige, Storbritannia, Tyskland og Sveits for å hente inspirasjon utenfra.

Kåre Willoch ledet Sårbarhetsutvalget som var satt sammen av personer med svært forskjellige yrkesbakgrunner i den hensikt å oppnå stor faglig bredde [14].

I rapporten er det ett kapittel som konkret omhandler IKT og sikkerhet, nemlig [14, kap. 6, Beskyttelse av IKT og kraftforsyning]. I tillegg omhandler rapporten generelle tiltak for all kritisk infrastruktur.

3.2.2 Oppsummering av foreslåtte tiltak

På bakgrunn av utvalgets kartlegging om IKT sårbarhet i samfunnet, ble det overordnede målet for å redusere IKT-sårbarhet definert som følger:

> *"Å øke robusthetsnivå i IKT-infrastruktur til et nivå som gjør det helt usannsynlig at viktige samfunnsfunksjoner stanses i en normalsituasjon. I en krisesituasjon skal robustheten være tilstrekkelig til å opprettholde kritiske funksjoner."* [14, kap. 6.6.2]

I dette kapittelet vil tiltakene som ble foreslått av Sårbarhetsutvalget bli presentert. Det er tatt utgangspunkt i listen som er presentert i [14, kap. 6.6.4]. Det er noen forskjeller fra listen i den nevnte kilden og den som presenteres her. Tiltak nummer 8 på Sårbarhetsutvalgets liste er utelatt fra denne listen da det anses som mindre relevant for denne oppgaven. Tiltaket lød som følger: "For Post- og teletilsynet bør det vurderes å ha en egen utskilt avdeling for sikkerhetstilsyn som blir styrt av og rapporterer til et annet departement enn sektordepartementet." [14, kap. 6.6.4]. Alle lovrelaterte tiltak på utvalgets liste (nr. 9–15) diskuteres under avsnittet "Lovendringer". Den siste forskjellen mellom listen som presenteres her og Sårbarhetsutvalgets liste er at tiltakene 16–18 på utvalgets liste er slått sammen. De diskuteres i avsnittet "Annen sikring".

Nasjonal strategi for IKT sårbarhet

Dette var det første punktet på listen over foreslåtte tiltak. En strategi er langsiktig og virkemidlene for å nå strategien må derfor tilpasses etter situasjonen, selv om det overordnede målet alltid vil være det samme. For Sårbarhetsutvalget var målet å redusere samfunnets IKT-sårbarhet. På daværende tidspunkt besluttet utvalget at følgende tiltak burde gjennomføres for å realisere strategien [14, kap. 6.6.4]:

- ➢ Etablering av Senter for informasjonssikring

- Økt innsats på forskning og utvikling
- Styrket utdanning og kompetanse
- Risiko- og sårbarhetsanalyser
- Gjennomgang av behov for lover, regler og incentiver
- Etablere IKT-tilsyn og styrke sertifiseringsarbeidet

Alle tiltakene bortsett fra "Risiko- og sårbarhetsanalyser" blir beskrevet i dette kapittelet. Utvalget foreslo at Risiko- og sårbarhetsanalyser ble gjort med jevne mellomrom i hver enkelt virksomhet som befinner seg i en samfunnskritisk sektor. Utvalget begrunnet en jevn oppdatering av analysene med at både teknologien og trusselbildet endret seg raskt. Dette tiltaket er ikke nevnt under utvalgets endelige liste over anbefalte tiltak. Dette skyldes sannsynligvis at et slikt tiltak må tilpasses til hver enkelt virksomhet og derfor er vanskelig å konkretisere til noe som er generelt anvendbart.

Senter for informasjonssikring (SIS)

SIS var et av hovedtiltakene for å realisere strategien for IKT sårbarhet, og det ikke-kommersielle senteret skulle jobbe på tvers av offentlige og private aktører. Intensjonen med senteret var mangfoldig. For det første skulle SIS være den koordinerende enheten ved sikkerhetsbrudd i offentlig og privat sektor. Videre skulle senteret jobbe for å bygge nettverk og tillit mellom aktørene. Denne tilliten skulle være basis for en utveksling av gjensidig nyttig og sensitiv informasjon om sikkerhetsarbeid og sikkerhetsbrudd. SIS skulle også benytte seg av denne informasjonen for å lage nasjonale statistikker om sikkerhetsbrudd, i tillegg til å analysere endringer i trusselbildet innenfor informasjonssikkerhet.

En annen oppgave SIS skulle ha var å spre informasjon om preventive sikkerhetstiltak til private og offentlige aktører. Denne informasjonen skulle blant annet komme i form av de anonymt utarbeidede statistikkene fra aktørene selv. Hensikten med informasjonsspredningen var å øke bevisstheten om sikkerhetstiltak. Utvalget kommenterte at slike tiltak kunne være tekniske og for eksempel rettet mot driftsansvarlige, men at de også kunne komme i form av generelle retningslinjer som kunne følges av alle ansatte.

SIS skulle skape økt fokus omkring informasjonssikkerhet ved å føre dialog med utdannings- og forskningsmiljøer [14, kap. 6.6.4]. Senteret var også tiltenkt oppgaven med å være et kontaktpunkt mot organisasjoner i utlandet med lignende mandat. På denne måten skulle Norge kunne samarbeide med andre land om sikkerhetshendelser på tvers av landegrenser.

Varslingssenter mot IKT-trusler

Sårbarhetsutvalget foreslo å etablere et "varslingssenter for trusler mot IKT-tjenester i offentlig virksomhet" [14, kap. 6.6.3]. Begrunnelsen for dette var at Internett ble brukt i alle deler av det norske samfunnet og at samfunnet derfor var gjenstand for internasjonal eksponering. Utvalget konkluderte med at det var et behov for "å bedre rutinene for overvåking, varsling og håndtering av sikkerhetshendelser mellom virksomheter" [14, kap. 6.6.3].

Strategisk forskningsprogram for IKT-sårbarhet

Utvalget ville etablere et program for å forske på IKT-sårbarhet og sikkerhet. Dette mente utvalget var nødvendig fordi det hadde vært lite forskning gjort i tilknytning til sivil sektor [14, kap. 6.6.4]. Den økte bruken av IKT verktøy i samfunnet hadde medført et nytt risikobilde for virksomheter på grunn av nasjonal og internasjonal eksponering.

Forskningen skulle skje i forening mellom staten og det private næringslivet. Målet med programmet var å få økt fokus på sikkerhet i virksomheter samt realisere bedre sikkerhetstiltak som ville redusere både sårbarheten og ressursbruken i samfunnet. Programmet skulle produsere tiltak for å redusere sårbarheten i det nye trusselbildet. Det ble foreslått at Nasjonal sikkerhetsmyndighet og Næringslivets sikkerhetsorganisasjon samt flere burde ta ansvar for at et slikt koordinert og langsiktig program ble startet [14, kap. 6.6.4].

Integrasjon av sikkerhet i IKT-utdanning

Som et av leddene i å øke kompetansen på informasjonssikkerhet foreslo utvalget å integrere sikkerhet i IKT-utdanning. Utvalget fant denne endringen nødvendig på grunn av manglende bevissthet og kompetanse blant personell i mange virksomheter. Målet ved tiltaket var å gi studenter kunnskap om informasjonssikkerhet som de ville være til nytte i arbeidslivet. Det ble anbefalt at informasjonssikkerhet burde bli integrert i all IKT-undervisning fra videregående skole til universitetet. Dette skulle gi basiskunnskap til et bredt spekter av studenter på skoler og universiteter. Videre ble det også påpekt at det var et behov for spesialkompetanse, og at informasjonssikkerhet derfor burde opprettes som eget fag ved noen universiteter og høyskoler.

Utvikling av sertifiseringsordninger for kritiske IKT-komponenter

Utvalget ville ha en organisasjon med utvikling av sertifiseringsordninger som ansvarsområde. På grunn av et økende behov for sertifisering av sikkerhetskrav på nye områder innen IKT, ble en slik organisasjon ansett som nødvendig [14, kap. 6.6.4]. Målet med dette tiltaket var å sørge for at kritiske komponenter kunne klassifiseres i henhold til et gitt sikkerhetsnivå. En sertifisering av produkter ville kunne gi "salgsmuligheter i nye/internasjonale markeder, bedre konkurransedyktighet og høyere grad av tillit og omdømme" [15]. I Norge ville en sertifiseringsordning forenklet anskaffelse av komponenter med sikkerhetskrav både for privat og offentlig sektor. Det ville være enkelt å sørge for at et system bare kunne inneholde komponenter i henhold til et gitt sikkerhetsnivå. En internasjonal klassifisering ville i tillegg forenklet handel av komponenter med sikkerhetskrav med andre land.

Tilsyn av sertifiseringsordninger for kritiske IKT-komponenter

I tillegg til utviklingen av sertifiseringsordninger anbefalte utvalget at Staten burde ha ansvar med tilsyn av informasjonssikkerheten i all samfunnskritisk virksomhet [14, kap. 6.6.4]. Dette burde gjøres for å vurdere sikkerheten samt styrke den i samfunnskritisk virksomhet. Utvalget mente at NSM og Post- og teletilsynet burde ha sentrale roller i dette arbeidet, og at samtlige sektortilsyn burde være ansvarlige for å styrke informasjonssikkerheten i deres respektive sektorer.

Lovendringer

Utvalget foreslo flere endringer og vurderinger som burde gjøres med lovverket for å holde tritt med teknologiutviklingen. Lovforberedelse er en grundig og langsom prosess, og det er naturlig at den kan komme på etterskudd i forhold til den raske utviklingen som har pågått og fortsatt pågår innen IKT. Det ble derfor anbefalt at man muliggjorde en raskere lovforberedelse på lovgivning innen IKT.

Den øvre strafferammen på 6 måneder for datainnbrudd ble ansett som lav av utvalget. Ved straffeskjerpende omstendigheter åpnet straffeloven (jf. § 145, tredje ledd) for fengsel inntil 2 år [14, kap. 6.6.4] for datainnbrudd. Til sammenligning hadde et ordinært innbrudd øvre strafferamme på 2 år, og inntil 4 år ved straffeskjerpende omstendigheter (jf. § 147). Datainnbrudd kan få konsekvenser av stort omfang, og utvalget anså det derfor som naturlig å heve strafferammen av allmennpreventive hensyn.

For å lette samt effektivisere politiets arbeid i bekjempelse av datakriminalitet, foreslo utvalget å påby tjenestetilbyderne å føre logger en bestemt tidsperiode. Det ble også foreslått at politiet skulle ha anledning til å beordre denne perioden utvidet for enkeltindivider ved behov. Norske myndigheter ble oppfordret til å sørge for at slike logger effektivt kunne innhentes og utveksles mellom politi i forskjellige land [14, kap. 6.6.4]. Et slikt samarbeid kunne bidratt til oppklaring av datainnbrudd på tvers av landegrensene. Det ville gjort etterforskningen enklere og muliggjort straffeforfølgelse i langt flere tilfeller enn der hvor ett land må løse en slik sak på egenhånd. Utvalget påpekte forøvrig at det burde vurderes hvorvidt norske tjenestetilbydere burde pålegges meldeplikt ved kjennskap til misbruk av deres tjenester. Et eksempel på slikt misbruk er hvitvasking av penger.

Annen sikring

Utvalget foreslo å sikre kritiske IKT-installasjoner ved å bruke fysisk sikring andre steder enn på selve installasjonene. Kraftforsyningen og IKT er gjensidig avhengig hverandre: IKT brukes for å regulere driften av kraftverkene, og kraft er en fundamental forutsetning for at IKT-komponenter kan fungere. På grunn av den store avhengigheten til kraftforsyningen anbefalte utvalget at retningslinjer for sikring av kraftforsyningen måtte gjennomgås og oppdateres [14, kap. 6.6.4].

Uønskede og uforutsette hendelser slik som flom og dambrudd kan også påvirke driften av IKT systemer dersom de rammer kraftforsyningen til systemene eller systemene selv. Utvalget påpekte derfor at kartlegging av risiko for slike hendelser måtte fortsettes.

Utvalget drøftet fysisk sikring av IKT-installasjoner i mindre omfang. Istedenfor sluttet utvalget seg til til konklusjonene fra FFI sitt prosjekt TIFKOM (Teleberedskap i fritt konkurransemarked). En anbefaling utvalget kom med angående fysisk sikring var å beskytte kritiske IKT-installasjoner fra mikrobølgevåpen. Utvalget beskrev slike våpen som en reell og farlig trussel, blant annet fordi rekkevidden er på flere kilometer.

Organisatoriske tiltak

Utvalget sammenfattet de organisatoriske forslagene under 5 hovedpunkter i [14, kap. 1.3.2]:

1. Samling av arbeid for samfunnssikkerhet og beredskap i ett departement som får dette som hovedoppgave.

2. Opprettelse av et koordineringsorgan for EOS-tjenestene.
3. Samlet strategi og vurdering av å slå sammen organer for tilsyn med sikkerhet på ulike områder.
4. Gjennomgang av landets operative rednings- og beredskapsressurser.
5. Felles granskningskommisjon for store ulykker og kriser.

Det virker rimelig å anta at punktet om samling av sikkerhetsarbeid under et eget departement er det punktet som er mest relevant i forhold til IKT. Tiltak som er mer generelt anvendbare på mange områder og ikke spesifikt myntet på informasjonssikkerhet blir i denne oppgaven ansett som mindre relevante og blir derfor ikke vektlagt. Kun tiltaket om et felles departement for krisehåndtering vil bli nevnt her. For mer utfyllende informasjon dette tiltaket, se [14, kap. 23].

Samfunnssikkerhet og beredskap under eget departement
Utvalget anbefalte å opprette et eget departement med sikkerhets- og beredskapsarbeid som hovedansvarsområde. Et slikt departement ville satt et permanent fokus på sikkerhetsarbeid i samfunnet. Tettere samarbeid mellom instanser og tverrsektoriell nytteverdi av resultater ville også kunne bedret ressursutnyttelsen i beredskapsarbeidet. I tillegg ville man unngått typiske problemer som ansvarsfraskrivelse mellom instansene involvert i krisehåndteringen [14, kap. 23.1].

Departementet ville blant annet hatt "et overordnet ansvar for å ta initiativ, fungere som pådriver, være en koordinator og en kontrollør for samfunnssikkerheten i bredest mulig betydning" [14, kap. 23.2]. Sett i lys av informasjonssikkerhet ville et slikt departement kunne håndtere kriser i forbindelse med kritisk IKT-infrastruktur.

Blant oppgavene som var IKT relaterte og ble tiltenkt departementet var [14, kap. 23.2]:

- Utarbeidelse av nasjonale sårbarhets- og trusselvurderinger.
- Utarbeidelse av overordnede mål og krav for sikkerhet og beredskap.
- Utarbeidelse av koordinerte handlingsplaner for sikkerhet og beredskap.
- Samordning av statlige myndigheters beredskap og krisehåndtering ved komplekse krisesituasjoner
- Strategisk forskning og utvikling innen sikkerhet og beredskap

Nasjonal sikkerhetsmyndighet ville ifølge utvalget vært én av flere virksomheter som burde kommet inn under et slikt departement.

3.2.3 Diskusjon

Sårbarhetsutvalgets utredning ble fulgt opp i St.meld. nr. 17 (2001-2002) – "Samfunnssikkerhet: Veien til et mindre sårbart samfunn" og videre i Innst. S. nr. 9 (2002-2003) – "Innstilling fra forsvarskomiteen og justiskomiteen om samfunnssikkerhet - Veien til et mindre sårbart samfunn".

Endel kritikk mot utvalgets og referansegruppens sammensetning er berettiget. Ingen av medlemmene av utvalget hadde IKT-bakgrunn. Referansegruppen bestod av bortimot 50

personer, hvorav fire hadde bakgrunn innen IKT og erfaring fra informasjonssikkerhet [16]. Det var disse fire som sto for innspillene til IKT. Dette vil si at mindre enn 10% av de som bidro til arbeidet (ekskludert utvalgsmedlemmene) og som la grunnlag for rapporten hadde noen bakgrunn innen IKT og sikkerhet [17].

En av de fire datakyndige demonstrerte under et møte hvor enkelt det var å bryte seg inn i en av departementenes databaser [16]. Etter å ha brutt seg inn i databasen modifiserte vedkommende departementets budsjett og flyttet midler til en verdi av rundt hundre millioner kroner [16]. Denne demonstrasjonen og gjentatte gjentatte innlegg fra de tre andre datakyndige om viktigheten av logiske trusler og informasjonssikring førte til opprettelsen av et IKT-underutvalg [16]. Erkjennelsen om at den fysiske IKT-trusselen overgås av den logiske viste seg å sitte langt inne blant utvalgsmedlemmene [16]. Underutvalget ble ledet av Jan Hovden, professor i sikkerhetsledelse, og bestod forøvrig av de fire personene med IKT-bakgrunn, en person fra departementet som sekretær samt to andre.

I sluttrapporten til Sårbarhetsutvalget ble konklusjonene fra FFI prosjektet BAS2 vektlagt mer enn konklusjonene fra IKT-underutvalget [16]. Tiltakene foreslått i BAS2 handlet i hovedsak om fysiske sikringstiltak fremfor logiske, og satt således feil fokus på hva som var den viktigste trusselen. Et sentralt tiltak i prosjektrapporten til BAS2 var fysisk sikring av driftssentraler og annen infrastruktur ved å flytte de inn i fjellanlegg. Telenor kritiserte forøvrig sluttrapporten til BAS2 fordi de mente at den fokuserte for mye på fysisk sikring og ikke nok på informasjonssikring [16].

En oppfølging av Sårbarhetsutvalgets utredning kom i St.meld. nr. 17 (2001–2002). Denne Stortingsmeldingen var i likhet med Sårbarhetsutvalget såvidt inne på den logiske trusselen, men ingenting ble sagt om hvordan man skulle beskytte seg mot denne.

Det er vanskelig å påvise hvilke anbefalte tiltak som faktisk ble iverksatt på bakgrunn av Sårbarhetsutvalgets anbefalinger. Samtidig som utvalget holdt på med sin utredning, var det andre aktiviteter som foregikk parallelt (for eksempel prosjektet om IT-sårbarhet i regi av NHD). Disse aktivitetene samt andre aktiviteter som har foregått i ettertid har sannsynligvis også bidratt til at mange av tiltakene er blitt fulgt opp. Dette kapittelet fokuserer derfor ikke på hvilke tiltak som ble fulgt opp bare på grunnlag av utvalgets anbefalinger, men heller *om* de er blitt fulgt opp. Det tas utgangspunkt i *Oppfølgingen av sårbarhetsutvalgets forslag: Delrapport til Utvalg for sikring av landets kritiske infrastruktur* [18, vedlegg 7].

Nasjonal strategi for informasjonssikkerhet – opprettet

Nasjonal strategi for informasjonssikkerhet ble opprettet i 2003, og strategien videreføres i en revidert utgave som skal gjelde i perioden 2007–2010. Strategien fra 2003 består av totalt tolv tiltak og den har innlemmet flere av de tiltakene som Sårbarhetsutvalget anbefalte.

Følgende liste angir forholdet mellom Sårbarhetsutvalgets foreslåtte strategitiltak og de tiltak i Nasjonal strategi for informasjonssikkerhet fra 2003 som tar hensyn til disse forslagene:

Etablering av Senter for informasjonssikring Tiltak III: Nasjonal koordinering av IT-sikkerhet

Økt innsats på forskning og utvikling Tiltak X: Forskning, kompetanse og utdanning

Styrket utdanning og kompetanse Tiltak X: Forskning, kompetanse og utdanning

Risiko- og sårbarhetsanalyser Tiltak IV: Risiko og sårbarhetsanalyser

Gjennomgang av behov for lover, regler og incentiver Tiltak II: Regelverk for IT-sikkerhet

Etablere IKT-tilsyn og styrke sertifiseringsarbeidet Tiltak III: Nasjonal koordinering av IT-sikkerhet

Som det går frem av listen, er det stort sett tatt hensyn til anbefalingene fra Sårbarhetsutvalget i utformingen av Nasjonal strategi for informasjonssikkerhet.

Senter for informasjonssikring (SIS) – opprettet

Et av de viktigste tiltakene ifølge Sårbarhetsutvalget var etableringen av et senter for informasjonssikring. Nærings- og handelsdepartementet besluttet å etablere SIS som et prøveprosjekt i 2004, fire år etter utvalget avleverte rapport. Prøvetiden ble forlenget ut 2005 og senteret er idag fortsatt operativt under navnet NorSIS. Den offisielle opprettelsen av NorSIS fant sted 1. januar 2006. Den første perioden var senteret i Trondheim, men det ble etterhvert flyttet til Gjøvik Kunnskapspark.

Opprinnelig ble det foreslått at senteret skulle bemannes av fem personer med spisskompetanse innen fagområdet og fullfinansieres med sju, åtte millioner kroner årlig over statsbudsjettet [19]. I dag har senteret en bemanning på fire personer og er delfinansiert av FAD med fire millioner årlig. I tillegg mottar NorSIS to millioner kroner fra private aktører.

NorSIS har i dag en viktig oppgave med bevisstgjøring, rådgivning og veiledning av offentlige og private virksomheter såvel som privatpersoner. Senteret er en del av et nasjonalt og helhetlig apparat rundt informasjonssikkerhetstrusselen.

NorCERT/VDI – opprettet

Varslingssystem for digital infrastruktur (VDI) ble etablert i 2000 som et prøveprosjekt og eksisterte derfor før Sårbarhetsutvalget avleverte sin rapport. Prosjektet var et samarbeid mellom etterretningstjenestene og noen offentlige og private virksomheter med erfaring innen sikring av nettverk [19, kap. 3.1]. Fra januar 2003 ble VDI permanent etablert under NSM.

Erfaringene som ble gjort med VDI i begynnelsen avdekket et behov for et nasjonalt responssenter som kunne håndtere dataangrep mot kritisk infrastruktur. På grunnlag av dette ble prosjekt NorCERT etablert i februar 2004 [20]. Regjeringen besluttet å permanent legge NorCERT som en avdeling under NSM med virkning fra januar 2006. NorCERT ble formelt opprettet samtidig med NorSIS 1. januar 2006.

NorCERT/VDI har i dag en bemanning på 17 personer. I tillegg kommer et visst antall vernepliktige med datafaglig kompetanse.

Organisasjonen har en viktig oppgave med å detektere, avverge og gjenopprette systemer i kritisk IKT-infrastruktur dersom de blir angrepet. NorCERT/VDI er i likhet med NorSIS en del av et nasjonalt og helhetlig apparat rundt informasjonssikkerhetstrusselen.

Strategisk forskningsprogram for IKT sikkerhet – opprettet

Beskyttelse av samfunnet 5 (BAS5) ble opprettet i 2004 med det formål å gjøre en studie på kritisk IKT-infrastruktur. Programmet har hatt fokus på metodeutvikling og det er blant annet gjennomført en doktorgrad ved Høgskolen i Gjøvik. Metodene som har blitt utviklet gjaldt risiko- og sårbarhetsanalyse av samfunnsviktige IKT-systemer, rangering av sårbarhetsreduserende tiltak samt rangering av samfunnsviktige funksjoner og tilhørende IKT-systemer [21].

Programmet var et samarbeid mellom FFI, Universitetet i Stavanger, Høyskolen på Gjøvik og NTNU/Institutt for økonomi og teknologiledelse i Trondheim [21]. Finansieringen skjedde gjennom forskningsprogrammet IKT sikkerhet og sårbarhet (IKT SoS) som er underlagt Norges forskningsråd. Andre departementer og virksomheter bidro også til finansieringen av BAS5 prosjektet.

BAS5 sendte sluttrapporten på høring ca. 30. mars 2007. Per idag er det ikke planlagt noen arvtager til BAS5 prosjektet [22].

Prosjektet har vært en viktig forskningsinnsats for å gi informasjon om samfunnets sårbarhet som følge av avhengighet til IKT.

Integrasjon av sikkerhet i IKT-utdanning – oppnådd i liten grad

I etterkant av Sårbarhetsutvalgets rapport ble det etablert en mastergrad i informasjonssikkerhet på Høgskolen i Gjøvik. En tid etter opprettelsen av denne mastergraden ble også en bachelorgrad i informasjonssikkerhet opprettet ved HiG. Disse studiene kan dog ikke sies å ha kommet som et resultat av Sårbarhetsutvalgets arbeid, men er heller et resultat av mangel og etterspørsel etter kompetanse innen informasjonssikkerhet fra næringslivet sin side [9, 23].

På Universitetet i Tromsø er det opprettet en bachelorgrad i datasikkerhet, men heller ikke denne er kommet som et resultat av Sårbarhetsutvalgets anbefalinger [24].

På NTNU, Norges fremste tekniske universitet, er informasjonssikkerhet fortsatt ikke obligatorisk for alle informatikkstudentene. Den eneste studieretningen som har informasjonssikkerhet som obligatorisk fag er telematikk på kommunikasjonsteknologi. På linjen datateknikk er faget frivillig. Spesialiseringen i informasjonssikkerhet på NTNU eksisterte forøvrig lenge før Sårbarhetsutvalget ble nedsatt, og spesialiseringen ble ikke påvirket av utvalgets arbeid.

I Stavanger fantes det en mastergrad på fagområdet fysiske sikkerhetstrusler før Sårbarhetsutvalget ble etablert. Denne graden hadde betydning for opprettelsen av utvalget [16].

På videregående skole har det skjedd lite. SAFT (Medietilsynet) tilbyr en læringspakke som fokuserer informasjonssikkerhet rettet mot grunn- og videregående skoler, og utdanningsdirektoratet har utviklet en lignende pakke rettet mot lærere [25]. Det er uvisst i hvilken grad disse pakkene er blitt tatt i bruk. Visse videregående skoler har hatt fag som har omhandlet informasjonssikkerhet som en del av andre IKT-fag. Det virker likevel som det ikke er noen systematikk i at det undervises i informasjonssikkerhet som en integrert del av IKT-undervisningen. Riksrevisjonen kommenterte i sin undersøkelse at det ikke var tatt initiativ til å styrke undervisning i IT-sikkerhet, for eksempel gjennom endring av læreplanen [26, kap. 5.5.2].

IKT-underutvalget foreslo å etablere et introduksjonsfag på universitetsstudier som dekket IKT-sårbarhet, miljø og annet [16]. Et slikt fag kom ikke med på listen over konkrete tiltak i forbindelse med IKT og utdanning i Sårbarhetsutvalgets rapport. Det er naturligvis en vanskelig politisk oppgave å sørge for at informasjonssikkerhet blir integrert i all IKT-utdanning og at emnet blir introdusert på andre studieretninger hvor det kan være relevant. Politikerne må overbevises om nødvendigheten av endringen i fagplanene. Høyskolene og universitetene har allerede den kompetansen som trengs for å kunne gi en introduksjon til problemstillinger rundt informasjonssikkerhet. Alle disse institusjonene sitter nødvendigvis ikke på nok kompetanse til å integrere informasjonssikkerhet på en tilfredsstillende måte i bachelor- og mastergradsstudier.

Utvikling av sertifiseringsordninger for kritiske IKT-komponenter – opprettet

Utvalget så et behov for å definere sikkerhetskrav på en rekke områder innen IKT: telenettet, Internett, programvare og annen kritisk IKT-infrastruktur. TIFKOM prosjektet foreslo å etablere organisasjonen Nasjonal telesikkerhet og -beredskap. Utvalget sluttet seg til dette forslaget og mente at andre sektorer også burde ha en lignende løsning.

I utvalgets arbeidsperiode var to ordninger for sertifisering av IKT-sikkerhet på vei til å bli etablert. Disse ble altså ikke realisert som følge av utvalgets anbefalinger.

Den første sertifiseringsordningen var for organisasjoner som hadde Norsk Akkreditering[1] som operatør. Norsk Akkreditering ble startet i 1991 som følge av EØS avtalen [27].

Den andre sertifiseringsordningen gjaldt for produkter eller systemer i organisasjoner med Forsvarets sikkerhetstjeneste som operatør [14]. Forsvarets overkommando/Sikkerhetsstaben (FO/S) fikk gjennom St. prp. nr. 1 (1998–99) bevilget midler av NHD slik at SERTIT kunne opprettes [28]. FO/S ble senere omgjort til direktoratet NSM (underlagt Forsvarsdepartementet). Fra 2000 overtok Forsvarsdepartementet budsjettansvaret fra NHD for SERTIT [15]. SERTIT ble opprettet på bakgrunn av en anbefaling som kom fra Rådet for IT-sikkerhet i 1997 [28].

SERTIT fungerer i dag som offentlig sertifiseringsmyndighet for IT-sikkerhet. Sertifiseringen er basert på internasjonalt anerkjente, standardiserte krav (Common Criteria og Common Evaluation Methodology). SERTIT representerer Norge i "Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security" og er en internasjonalt anerkjent sertifikatutsteder under denne organisasjonen [15].

Tilsyn av sertifiseringsordninger for kritiske IKT-komponenter – opprettet

SERTIT ble underlagt en bredt sammensatt styringskomité som hadde som ansvar å føre tilsyn med driften av sertifiseringsmyndigheten (SERTIT) [28]. Komitéen består av representanter fra blant annet Forsvarsdepartementet, Justis- og politidepartementet, Datatilsynet og Nasjonal sikkerhetsmyndighet.

Lovendringer – delvis gjennomført

Datakrimutvalget ble opprettet i 2002. Utvalget avla delutredning I vedrørende tilpassing av norsk lovverk i forhold til EU sin datakrimkonvensjon i 2003. Utvalget fikk også i

[1] "Akkreditering er en offisiell anerkjennelse av en organisasjons kompetanse og evne til å utføre angitte oppgaver i samsvar med gitte krav." [27]

oppgave å vurdere behovet for ytterligere lovendringer, noe som førte til arbeidet med delutredning II.

I 2007 avla utvalget rapporten fra delutredning II som omhandlet et eget kapittel om straffebestemmelser for datakriminalitet. Kapittelet er ment å inkluderes i den nye Straffeloven. Utredningen hadde høringsfrist 25. mai 2007, og JD skal etter dette utarbeide et lovforslag som skal fremmes for Stortinget. Departementet har uttalt at det tar sikte på å fremme proposisjonen om straffelovens spesielle del (inklusive bestemmelser om datakriminalitet) i løpet av 2008 [29].

3.2.4 Konklusjon

Foreslåtte tiltak	**Gjennomføring**	**Kommentar**
Nasjonal strategi for informasjonssikkerhet	Opprettet	En ny, revidert strategi for perioden 2007–2010 vil avløse nåværende strategi fra 2003.
Senter for informasjonssikring (SIS)	Opprettet	
Varslingssystem for digital infrastruktur (VDI)	Opprettet	NorCERT ble opprettet senere på bakgrunn av erfaringene fra VDI.
Strategisk forskningsprogram for IKT sikkerhet	Opprettet	Programmet (BAS5 hos Forsvarets Forskningsinstitutt) er nå ferdigstilt. Ingen arvtager er planlagt for BAS5 [22].
Integrasjon av sikkerhet i IKT utdanning	Oppnådd i liten grad	
Utvikling av sertifiseringsordninger for kritiske IKT-komponenter	Opprettet	
Tilsyn av sertifiseringsordninger for kritiske IKT-komponenter	Opprettet	
Lovendringer vedrørende datakriminalitet	Delvis oppnådd	JD fremmer ikke proposisjonen som inkluderer Datakrimutvalgets delutredning II før i 2008.

Tabell 3.2: *Liste over tiltakene som ble foreslått av Sårbarhetsutvalget og hvilke som er blitt implementert.*

I ettertid er det vanskelig å si hvilke tiltak som ble implementert nettopp på grunn av Sårbarhetsutvalgets anbefalinger. Prosesser som foregikk parallelt med Sårbarhetsutvalget og andre kilder har også hatt innvirkning på arbeidet som skjedde i kjølvannet av utvalgets rapport [18, Vedlegg 7, kap. 2]. Det er viktigere å se på om de foreslåtte tiltakene er blitt implementert eller ikke. I den sammenheng må man kunne si at det har skjedd mye arbeid i ettertid med å bedre nasjonal informasjonssikkerhet. Mange av resultatene kan tillegges Sårbarhetsutvalgets arbeid, men mange andre aktører har også bidratt i prosessen. For eksempel er det klart at mastergraden i informasjonssikkerhet ved HiG og bachelorgraden i datasikkerhet ved UiT ikke har kommet på bakgrunn av anbefalingene i Sårbarhetsutvalget,

men heller som et behov for faglig kompetanse og utvikling ved institusjonene [24,23]. Det er verdt å merke seg at det tok hele fire år før SIS ble etablert og før det strategiske forskningsprogrammet [2] ble opprettet fra Sårbarhetsutvalgets rapport ble avlevert i 2000.

3.3 Infrastrukturutvalget

3.3.1 Bakgrunn

Utvalget for sikring av kritisk infrastruktur ble nedsatt av regjeringen Stoltenberg II den 29. oktober 2004. Utredningen var ferdigstilt og ble avlevert til Justis- og politidepartementet 5. april 2006. Utredningen ble kjent som NOU 2006: 6 og hadde tittelen "Når sikkerheten er viktigst: Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner".

Målet med utredningen var å utrede sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner i Norge. Det skulle spesielt fokuseres på privatiserte virksomheter (kraft, tele, vannforsyning m.m.). Utvalget fikk i oppdrag å "kartlegge og vurdere virkemidler for sikring av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner" [18, kap. 2.2]. Konsekvensene av de foreslåtte tiltakene skulle også utredes.

Utvalget tok utgangspunkt i Sårbarhetsutvalgets rapport NOU 2000: 24 og nyttiggjorde seg av materiale derfra. Det ble sendt brev til en rekke private og offentlige virksomheter med anmodning om innspill. Disse var en viktig del av informasjonsgrunnlaget til utvalget. Det ble avholdt ca. 200 møter med diverse offentlige og private virksomheter, organisasjoner og privatpersoner. Videre ble det foretatt en rekke besøk til organisasjoner i Sverige, Storbritannia Sveits, Tyskland, Nederland, Canada og USA. Viktige norske bidragsytere til utredningen inkluderte NSM, DSB, FFI, NHD og Post- og teletilsynet. Utvalget ble ledet av Sven Ullring som tidligere var konsernsjef i det norske Veritas.

Det er intet kapittel som alene omhandler IKT tiltak i denne rapporten slik som i Sårbarhetsutvalgets rapport. De fleste tiltakene i denne rapporten er ikke IKT spesifikke, men heller av generell karakter og med tverrsektoriell anvendelse. Utredningen har lite materiale som omfatter konkrete IKT tiltak sammenlignet med Sårbarhetsutvalgets rapport. Noen av de konkrete IKT tiltakene som finnes i rapporten er beskrevet i [18, kap. 1.2.6.1]. Rapporten beskriver mange generelle tiltak som også har anvendelse innen kritisk IKT-infrastruktur. Disse tiltakene er beskrevet i dybden i [18, kap. 5,6,7,8,9,13]. Et sammendrag av alle disse tiltakene presenteres i [18, kap. 1.2].

3.3.2 Oppsummering av foreslåtte tiltak

Tiltakene som presenteres her er hentet fra [18, kap. 1.2] og supplert med informasjon fra øvrige kapitler. Det er gjort et utvalg av de tiltak som er meningsfylte for IKT. De kapitlene i utvalgets rapport som beskriver tiltakene i utdypet form er gjengitt i tittelen for hvert enkelt avsnitt.

[2] Det strategiske forskningsprogrammet fikk navnet BAS5 – Beskyttelse av samfunn 5 og ble utført ved Forsvarets forskningsinstitutt.

Klar ansvarsfordeling for beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner, kapittel 5

Tydeliggjøring av Justis- og politidepartementets rolle

Ifølge utvalget hadde Justis- og politidepartementet allerede gode muligheter til å bli departementet med hovedansvar for samfunnssikkerhet og -beredskap. JDs rolle som overordnet koordinator for sikkerhet- og beredskapsarbeid burde derfor avklares formelt og tydeliggjøres. Videre mente utvalget at antall departementer med overordnet ansvar for IT-sikkerhet ideelt sett burde reduseres til ett, og at ansvarsfordelingen mellom SD, FAD, og JD måtte klargjøres. Det ble anbefalt en samordning av SD og FAD sitt ansvar innen IT-sikkerhet.

Utvalget mente at blant annet følgende oppgaver burde legges til JD [18, kap. 1.2.1]:

- Rådgivende myndighet i sikkerhet og beredskapsspørsmål
- Pådriver for samarbeid mellom virksomheter med ansvar for kritisk infrastruktur
- Etablere og videreutvikle oversikt over kritisk infrastruktur
- Nasjonalt kontaktpunkt for internasjonale operasjoner
- Koordinere forskningsarbeid innen sikkerhet og beredskap

Målet med dette tiltaket var å forankre det overordnede ansvaret og arbeidet med sikkerhet og beredskap i ett departement, slik Sårbarhetsutvalget foreslo i sin rapport.

Tydeliggjøre nasjonale mål/akseptnivå

Utvalget pekte på at endringen i risikobildet og sårbarheten innen kritisk infrastruktur foregikk raskt, og at det derfor burde tas høyde for dette i risiko- og sårbarhetsanalyser. JD burde gi retningslinjer til de forskjellige sektorene om hvordan risikoanalysen burde gjennomføres. Det ble nevnt at det også burde utvikles et program som ville forplikte sektorene til å gjennomføre risikoanalyse periodisk.

Koordinert samarbeid mellom NSM, PST og DSB

Utvalget mente at JD burde inneha rollen som koordinator for samarbeid mellom NSM, PST og DSB. Dette skulle gi en klarere ansvarsfordeling og bedre gjensidig utnyttelse av organisasjonenes ressurser.

Prinsipper for god sikkerhetskultur og informasjonshåndbok

Det ble utarbeidet en liste over prinsipper som burde følges i virksomheter med behov for god sikkerhetskultur. Disse prinsippene var:

- Godt lederskap og god kultur og høy status for sikkerhetsarbeid innen virksomheten
- Sikkerhet og beredskapsarbeid må være en integrert del av virksomhetens arbeid
- Sikkerhets- og beredskapstiltak må utarbeides med grunnlag i risikoanalyser
- Kompetansebygging på sikkerhet og beredskap gjennom kursing, trening og øvelser
- System for intern/ekstern deling av sikkerhetsrelatert informasjon

- ➢ Vedlikeholde lister over ansvarsroller i forbindelse med sikkerhet og beredskap innad i organisasjonen
- ➢ Planer for proaktive og reaktive tiltak for ulike trusler (reaktiv for å redusere konsekvensen av en pågående trussel), samt tiltak for gjenopprettelse til normal drift etter en trussel er blitt realisert i form av en uønsket hendelse

Utvalget anbefalte også at myndighetene publiserte en informasjonshåndbok. Håndboken skulle inneholde en oversikt over ulike myndighetsorganer og hva disse kan tilby av informasjon og veiledning for sikkerhet og beredskap.

Virkemidler for god sikring av kritisk infrastruktur, kapittel 6

Utvalget anbefalte å bruke følgende virkemidler for å ivareta en tilfredsstillende og god sikring av kritisk infrastruktur:

- ➢ Etablere en generell, sektorovergripende lov om beredskap for slik å sikre kritisk infrastruktur. Forslaget innebar krav til risiko- og sårbarhetsanalyser, drifts- og leveransesikkerhet, beredskapsplaner, informasjonsdeling og samarbeid, tilsyn og sanksjonsmuligheter.
- ➢ Utarbeide en klar ansvarsfordeling av sikkerhet og beredskap for kritisk infrastruktur. Dette innebærer en utredning for å klargjøre ansvarsfordelingen og tilsynsvirksomheten for kritisk infrastruktur. Utredningen er tenkt å gi en mer mål- og resultatorientert arbeidsmetode for sikkerhets- og beredskapsplanlegging. Videre ble det anbefalt å vurdere en eventuell samordning mellom tilsynsvirksomhetene. Utvalget foreslo også å undersøke om tilsynsvirksomheter er direkte underlagt den samme sektoren som tilsynet skal undersøke. En slik organisering er uheldig og bør isåfall omgjøres.
- ➢ Etablere en nasjonal strategi for tilsyn med sikring av kritisk infrastruktur som ansvarsområde.
- ➢ Etablering av en statlig tilskuddsordning for å forsikre at tiltak som faller utenfor en virksomhets eget ansvarsområde allikevel blir fulgt opp, dersom tiltakene er viktige for rikets sikkerhet. En slik ordning ville blant annet sørget for at tiltak på tvers av sektorer uten én klar hovedinteressent ble gjennomført og fulgt opp.
- ➢ Vurdere offentlige innkjøp slik at sikkerhets- og beredskapsmessige konsekvenser ved bortfall av tjenester og varer kan kartlegges. Krav til sikkerhet og beredskap burde også bli stilt til underleverandører av tjenester og varer.
- ➢ Økt informasjonsutveksling relatert til sikkerhet og beredskap mellom virksomheter (også mellom offentlig og privat sektor), og da spesielt mellom virksomheter med ansvar for kritisk infrastruktur.

Endringer i Sikkerhetsloven, kapittel 7

Utvalget anbefalte en gjennomgang av Sikkerhetsloven slik at nødvendige endringer relatert til objektsikkerhet kunne utføres. For å bestemme hvilke objekter som burde sikres, ble det foreslått å ta utgangspunkt i virksomhetens risiko- og sårbarhetsanalyser. I tillegg ble det anbefalt at virksomhetene førte dialog med myndighetene for å avgjøre om virksomhetens objekter fallt inn under Sikkerhetsloven.

Ivaretakelse av sikkerhets- og beredskapshensyn ved omreguleringer og omorganiseringer, kapittel 8

Utvalget mente at omstillingsprosesser lett kunne føre til at sikkerhet- og beredskapshensyn ikke ble ivaretatt. Det ble derfor utarbeidet en oversikt av utvalget over punkter som burde tas hensyn til ved omorganiseringer og omreguleringer i offentlige virksomheter (se kap 8). Listen inneholdt spørsmål om sikkerhets- og beredskapsarbeid i virksomheten og lød som følger [18, kap. 8.5.1]:

1. Hvordan ivaretas sikkerhet og beredskap i virksomheten?
2. Hvilke konsekvenser har endringen for ivaretakelse av sikkerhet og beredskap i virksomheten?
3. Påvirker endringen reguleringen av sikkerhet og beredskap i virksomheten?
4. Påvirker endringen ivaretakelsen av hensynet til rikets sikkerhet og vitale nasjonale interesser?
5. Hva er ressursinnsatsen til sikkerhet og beredskap i virksomheten før og etter endringen?
6. Hvilke underleverandører er virksomheten kritisk avhengig av for å opprettholde driftskontinuitet?
7. Leverer virksomheten samfunnskritiske varer og tjenester?
8. Hvordan skal spørsmål knyttet til sikkerhet og beredskap håndteres av virksomhetens ledelse og styrende organer?

Målet med listen var at punktene i den skulle følges ved en omregulering eller omorganisering, og på den måten garantere at virksomhetens sikkerhets- og beredskapsarbeid ble ivaretatt også etter omstillingsprosessen.

Det ble videre anbefalt å ikke gjennomføre endringer samtidig i tilsyn og i sentrale virksomheter innen sektoren som tilsynet har ansvar for. Samtidige omstillinger i begge to kan føre til at sektoren blir ekstra svekket hvis både tilsynet og virksomheten i sektoren som tilsynet overvåker er under omstrukturering.

Utvalget anbefalte også at virksomheter med ansvar for kritisk infrastruktur ikke "outsourcer" sikkerhets- og beredskapsarbeid tilknyttet infrastrukturen, men beholder den som en integrert del av virksomhetens arbeid.

Offentlig eierskap, kapittel 9

Utvalget mente at offentlig eierskap måtte vurderes innenfor hver enkelt sektor og tilhørende virksomheter med ansvar for kritisk infrastruktur. Det ble funnet tre ulike kjennetegn ved kritisk infrastruktur som talte for offentlig eierskap som middel for å oppfylle det offentlige ansvaret:

Kritisk avhengighet Infrastrukturen er nødvendig for å oppfylle grunnleggende behov.

Absolutt nødvendighet Det finnes ingen gode alternativer til infrastruktur som kan brukes som midlertidig erstatning.

Tett kobling Fungerer som en seriekobling mellom systemer eller innad i et system. Bortfall av én komponent medfører bortfall av alle.

Det ble påpekt at siden myndighetene uansett måtte tatt ansvar for å organisere reserveløsninger og gjenopprette normal drift i en krisesituasjon, ville det være naturlig at de også er ansvarlige for normal drift og vedlikehold av den kritiske infrastrukturen.

Kartlegging av kritisk infrastruktur og sektorvise anbefalinger, kapittel 10

Elektronisk kommunikasjon

Utvalget var av den oppfatning at infrastruktur som er kritisk for landet burde være under norsk eierskap. Om nødvendig måtte det offentlige sikre nok eierandeler i de aktuelle selskapene for å kunne utøve tilstrekkelig kontroll. Reserveløsninger som kunne sikre nasjonal autonomi[3] for elektroniske kommunikasjons- og nettjenester burde bli etablert, hvis ikke vil avhengigheten av utenlandske tjenester til telemarkedet fortsette å øke. Denne økte avhengigheten vil igjen føre til at det ville bli svært dyrt og vanskelig å etablere en god, nasjonal beredskap i telesektoren.

I utvalgets rapport var det tre forslag som omfattet regulering av brukere tilknyttet Internett. Det første forslaget var å pålegge alle Internettilbydere å levere sikkerhetsprogramvare til kundene deres. Det andre forslaget var å pålegge leverandører av trådløse nettverkskomponenter å levere disse med gode sikkerhetsinnstillinger og veiledninger på norsk. Det siste forslaget var tredelt og måtte utredes nærmere av Samferdselsdepartementet før det kunne blitt fulgt opp. Forslaget besto av å pålegge alle privatpersoner og virksomheter å bruke oppdatert sikkerhetsprogramvare ved oppkobling til Internett. Videre skulle Internettilbydere pålegges å kontrollere at deres brukere hadde oppdatert sikkerhetsprogramvare, og til slutt skulle det utarbeides en IKT-sikkerhetsstandard som alle virksomheter med tilknytning til Internett skulle bli pålagt å følge.

Utvalget henviste til og støttet Riksrevisjonens undersøkelse vedrørende anbefalingen om å konsentrere det overordnede ansvaret for sikkerhetsarbeid innen IKT til ett departement for bedre å avklare ansvarsfordelingen.

Det ble også foreslått et økonomisk tiltak av utvalget. Tiltaket gikk ut på å gi økonomiske tilskudd for visse oppgaver knyttet til sikring av kritisk infrastruktur. Dette brukes allerede i en viss grad per idag. For eksempel kjøper staten tjenester fra Telenor for at selskapet skal drifte kystradionettverket. Utvalget var enige i Samferdselsdepartementets konklusjon i St.meld. nr. 47 (2000-2001) om at slike tjenester prinsipielt sett kunne konkurranseutsettes så lenge sikkerheten ble ivaretatt og man hadde tillitt til aktøren.

Forskning og utredning, kapittel 13

På dette området kom utvalget fram til at mandatet til FFI burde utvides til å omfatte samfunnets sårbarhet også i sivil sektor. FFI har gjort forskning på samfunnssårbarhet i sivil sektor siden 1994, men prosjektene har vært organisert ad-hoc og vært et spleiselag

[3] "Nasjonal autonomi for elektroniske kommunikasjons- og nettjenester betyr at transport- og tjenestenett er lokalisert nasjonalt, at trafikk og signalering skjer innen landets grenser og at produksjon av ulike elektroniske kommunikasjonstjenester skjer nasjonalt. Det innebærer også at drift og styrefunksjoner skjer innen landets grenser. Nasjonal autonomi omhandler også nasjonal tilgjengelighet til reservedeler og kompetanse til å håndtere feil." [18, kap .10.1.4.2]

mellom forskjellige offentlige aktører. En utvidelse av mandatet ville sikret kontinuitet i prosjektaktiviteten og sørget for at kompetansen i FFI opprettholdes på permanent basis.

Et tiltak som utvalget støttet gjaldt etableringen et tverrsektorielt forskningsprogram for å kartlegge samfunnets sårbarhet. Dette tiltaket ble anbefalt av en utredning gjort under Norges forskningsråd i 2005. Samfunnssikkerhet og risikoforskning (SAMRISK) ble foreslått som navn på programmet. Målet med et slikt program var flerdelt. For det første skulle forskningen bidra til utformingen av politiske løsninger. Programmet skulle også fungere som en nettverksbygger både i offentlig og privat sektor. Det siste målet var at programmet skulle kvalifisere norske forskningsinstitusjoner for internasjonalt forskningssamarbeid [18, kap. 13.3.2].

Utvalget mente at Norsk Terror Konsortium, en organisasjon for forskning på terrorisme og internasjonal kriminalitet, hadde lyktes i å koble sammen forsknings- og brukermiljøer. Konsortiet består av Forsvarets forskningsinstitutt (FFI), Norsk Utenrikspolitisk Institutt (NUPI) og Politihøgskolen.

Brukerne av konsortiet bestilte oppdrag tilpasset til eget brukermiljø, og kunne bestille oppdragene fra en bred sammensetning av forskningsinstitusjoner istedenfor enkeltinstitusjoner. Brukergruppene støttet konsortiet ved å gi mindre beløp til grunnforskningen, samt betale for egne oppdrag. Ifølge utvalget burde finansieringen på lang sikt være mer forutsigbar enn den var på det tidspunktet. En usikker finansieringsmodell ville kunne lede til tap av kompetanse hvis strømmen av nye oppdrag ikke var stor nok.

Utvalget anbefalte å starte et forskningsprosjekt med det mål å redusere gjensidige avhengigheter i kritisk infrastruktur. Det var klart at det allerede fantes en del forskning på dette området, men at mye av forskningen hadde vært gjort ved å betrakte et begrenset antall objekter eller systemer. Hva som ville skje ved større sammenbrudd var fortsatt uklart og krevde en nøyere utredning. Det ble derfor anbefalt å starte et eget forskningsprogram under Justis- og politidepartementet for å kartlegge nettopp dette.

3.3.3 Diskusjon

Utredningen fra Infrastrukturutvalget ble fulgt opp i St.meld. nr. 17 (2006–2007) "Eit informasjonssamfunn for alle" og videre i Innst. S. nr. 158 (2006–2007). Infrastrukturutvalgets rapport skal forøvrig innarbeides i en Stortingsmelding som JD vil legge frem i løpet av 2008 [30].

Det er kun litt over ett år siden Infrastrukturutvalgets rapport ble avgitt til Justis- og politidepartementet (5. april 2006). St.meld. nr. 17 (2006–2007) fra FAD kom 15. desember 2006, og meldingen ble behandlet i Stortinget i 16. april 2007 [30]. Siden behandlingen av meldingen har skjedd såpass nylig, er det for tidlig å vurdere oppfølgingen av forslagene. Istedenfor å vurdere oppfølgingen av utredningen og de foreslåtte tiltakene, drøftes de foreslåtte tiltakene i dette kapittelet.

Det bemerkes at det i likhet med Sårbarhetsutvalget fantes lite kompetanse innen IKT og sikkerhet i utvalget. Av utvalgsmedlemmene var det kun to personer som hadde IKT bakgrunn: sikkerhetssjef Anne M. Reinsnes ved Telenor og direktør Willy Jensen i Post- og teletilsynet.

Klar ansvarsfordeling for beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner

Klar ansvarsfordeling og arbeidsfordeling er en forutsetning for god oppfølging av tiltak. Å legge overordnet ansvar for et antall relevante oppgaver til ett og samme departement er noe som kan bidra til en tydeligere ansvarsfordeling mellom departementene. En slik samling av overordnet ansvar for et relevant sett med oppgaver vil også gjøre det lettere for andre aktører å vite hvor de skal henvende seg. Det er derfor hensiktsmessig å samle det overordnede ansvaret for IT-sikkerhet til ett departement slik som utvalget foreslo. FAD ville sannsynligvis vært den mest passende kandidaten til et slikt overordnet ansvar. Departementet har allerede et overordnet ansvar for oppfølging av Nasjonal strategi for informasjonssikkerhet.

Utvalget mente at JD sin rolle som sikkerhet- og beredskapsdepartement burde styrkes. For å gjøre dette ble det foreslått å legge følgende oppgaver til departementet:

- Rådgivende myndighet i sikkerhet og beredskapsspørsmål
- Pådriver for samarbeid mellom virksomheter med ansvar for kritisk infrastruktur
- Etablere og videreutvikle oversikt over kritisk infrastruktur
- Nasjonalt kontaktpunkt for internasjonale operasjoner
- Koordinere forskningsarbeid innen sikkerhet og beredskap

JD har allerede en nøkkelrolle i sivilt sikkerhet- og beredskapsarbeid, og tillegges de nevnte oppgavene departementet vil denne rollen styrkes ytterligere. Dette er i overensstemmelse med Sårbarhetutvalgets forslag om å forankre det overordnede ansvaret for sikkerhet- og beredskapsarbeid i ett departement.

Infrastrukturutvalget anbefalte at JD burde gi retningslinjer for hvordan ROS-analysene burde gjennomføres i de ulike sektorene. På bakgrunn av de raske endringene i risikobildet for kritisk infrastruktur ønsket utvalget at sektorene gjennom et program forpliktet seg til å gjennomføre periodiske ROS-analyser. Det er fornuftig at ett departement har et overordnet ansvar for oppfølgingen av ROS-analyser i sektorene. Departementet har således mulighet til å påvirke alle sektorer til å bruke det samme formatet når de rapporterer tilbake, uavhengig av hvilken sektor ROS-analysen er foretatt i. Bruken av det samme rapporteringsformatet i alle sektorer er viktighet for å kunne understøtte tverrsektorielle prioriteringer. Dette faktum understrekes i BAS5 prosjektet [13, kap. 4.3]. En periodisk forpliktelse i sektorene til å gjennomføre ROS-analyser er også et godt tiltak. ROS-analyser burde være en selvfølge for svært mange virksomheter, og en forpliktelse på dette området burde derfor ikke spille noen rolle for de virksomheter som har en god sikkerhetskultur. Forpliktelsen vil derimot sørge for at de virksomheter som per idag ikke utfører periodiske ROS-analyser, vil måtte gjøre det. En periodisk forpliktelse til å utføre ROS-analyser i virksomhetene vil gi en mer nøyaktig kartlegging av kritisk infrastruktur idet man får et jevnlig oppdatert bilde fra alle aktørene, og ikke bare fra de med god sikkerhetskultur. Presis kartlegging av kritisk infrastruktur kan igjen hindre at det blir investert i tiltak for feil beskyttelsesmål.

Utvalget ønsket at JD skulle koordinere samarbeidet mellom NSM, PST og DSB for å oppnå bedre utnyttelse av ressursene. NSM er primært ansvarlig for forebyggende eller

proaktive tiltak for å styrke samfunnets sikkerhet, mens PST også fokuserer på reaktive tiltak ved uønskede eller kriminelle hendelser. Foruten denne overlappingen mellom NSM og PST er det sannsynligvis også en viss synergigevinst å vinne ved ytterligere koordinering av NSM og DSB, idet førstnevnte jobber med å realisere forebyggende tiltak mens sistnevnte har beredskapsplanlegging og gjennomføring av øvelser som fokus. Det kan virke noe uklart om det er mest hensiktsmessig å koordinere organisasjonene gjennom JD, eller om det er tilstrekkelig med en formell ansvarsavklaring og jevnlige møter mellom organisasjonene. I denne sammenheng kan det nevnes at NSM og DSB i 2006 gjennomførte en felles utredning for å vurdere grenselinjer mellom de to direktoratene [25].

Infrastrukturutvalget utarbeidet en liste over prinsipper som burde følges for å oppnå en god sikkerhetskultur. Det ble også anbefalt at myndighetene publiserte en informasjonshåndbok over ulike myndighetsorganer og hva disse kan tilby av informasjon og veiledning av for sikkerhet og beredskap.

En liste over gode sikkerhetsprinsipper er vel og bra, men det er nok ikke mangel på eksisterende informasjon om sikkerhet og prinsipper som gjør at virksomheter ikke følger opp. Det vanskeligste arbeidet er å kommunisere denne informasjonen ut til virksomhetene på en måte som får virksomhetene selv til å forstå viktigheten av å etterleve sikkerhetsprinsipper. De må forstå fullt ut de konsekvenser manglende sikkerhetsrutiner kan medføre, og vurdere akseptabel risiko opp mot økonomiske midler for sikkerhetstiltak. De virksomheter som omfattes av Sikkerhetsloven er pålagt å følge visse sikkerhetsrutiner. Da Riksrevisjonen gjennomførte sin undersøkelse var det derimot fortsatt ikke klart hva som skulle defineres som skjermingsverdige objekter i henhold til Sikkerhetsloven, og hva som skulle gjøres for å beskytte disse. Slike uklarheter gjør det vanskelig for de relevante virksomhetene å forholde seg til loven. Videre vanskeliggjør uklarhetene tilsynsarbeidet til Nasjonal sikkerhetsmyndighet som er ansvarlig forvalter av Sikkerhetsloven.

En informasjonshåndbok over ulike myndighetsorganer og hva de kan tilby er et tiltak næringslivet ville satt pris på. Bransjeorganisasjonene IKT-Norge, Abelia og NSR har i Riksrevisjonens rapport uttalt at en utydelig ansvarsfordeling gjør det vanskelig å forholde seg til de mange ulike aktørene i offentlig forvaltning. Abelia påpekte at det spesielt var vanskelig å finne ut hvilke organer som er rene informasjonstiltak, og hvilke som er tilsynsorganer som kan fatte vedtak og/eller håndheve lovverk [26, kap. 4.2.1]. Å lage innholdet i en slik håndbok kan bare anses å være første del av tiltaket. Hvis informasjonshåndboken skal lages, må også næringslivet opplyses om dens eksistens. Slikt opplysningsarbeid er helt nødvendig for at tiltaket skal ha noen som helst effekt. En god ansvarsavklaring i offentlig sektor vil bidra mye til å avhjelpe det uoversiktlige bildet over myndighetenes fagorganer og samtidig gjøre det lettere for næringslivet å finne frem til relevante fagorganer.

Virkemidler for god sikring av kritisk infrastruktur

Utvalget foreslo å etablere en sektorovergripende lov om beredskap for kritisk infrastruktur. Forslaget innebærer blant annet at virksomhetene må gjennomføre ROS-analyser og utarbeide beredskapsplaner. Krav til informasjonsdeling, samarbeid og drifts- og leveransesikkerhet er også innlemmet i forslaget. Tilsyn- og sanksjonsmuligheter er andre faktorer som nevnes. En slik lov ville hatt en positiv effekt på beredskapsarbeidet vedrørende kritisk IKT-infrastruktur. IKT-sikkerhet er en tverrsektoriell problemstilling, og et lovverk som

er sektorovergripende vil bidra til at kravene til den kritiske infrastrukturen og tilsynsmulighetene for å vurdere oppfølging av kravene er de samme på tvers av sektorene.

Det ble anbefalt en utredning for å klargjøre ansvarsfordelingen av sikkerhet og beredskap for kritisk infrastruktur. Meningen med en slik utredning ville være å gjøre arbeidsmetoden mer mål- og resultatorientert. En slik arbeidsmetode synes fornuftig. Riksrevisjonen konkluderte med at det var vanskelig å måle graden av måloppnåelse for de ulike tiltakene i og med at det ikke ble spesifisert resultatkriterier som gjorde det mulig å måle effekten av tiltakene [26, kap. 2.4]. En arbeidsgruppe i KIS som vurderte Nasjonal strategi for informasjonssikkerhet kom til samme konklusjon, og anbefalte blant annet at tiltakene burde vært koblet mot målsetningene i strategien [31]. Utvalget anbefalte også en samordning av tilsynsvirksomhetene samt at man undersøkte om disse var underlagt den samme sektoren som tilsynet skulle føre tilsyn med. En slik kobling bør naturligvis ikke forekomme siden det kan påvirke arbeidet til tilsynsvirksomheten i negativ grad.

Infrastrukturutvalget foreslo å etablere en nasjonal strategi for tilsyn med sikring av kritisk infrastruktur som hovedområde. Sikringen av kritisk infrastruktur var ett av områdene Riksrevisjonen gjennomgikk i Nasjonal strategi for informasjonssikkerhet hvor det ble funnet en rekke kritikkverdige forhold. En nasjonal strategi for tilsyn med sikring av kritisk infrastruktur er et fornuftig forslag med tanke på den tildels svake oppfølgingen av Nasjonal strategi for informasjonssikkerhet.

Et annet forslag for å sikre kritisk infrastruktur var å etablere en statlig tilskuddsordning for å forsikre at tiltak som faller utenfor en virksomhets eget ansvarsområde allikevel blir fulgt opp dersom tiltakene er viktige for rikets sikkerhet. En slik ordning ville blant annet sørget for at tverrsektorielle tiltak uten én klar hovedinteressent ble gjennomført og fulgt opp. Finansiering av slike tiltak representerer et betydelig problem. PT, DSB og NSM pekte alle i Riksrevisjonens rapport på problemet med å få finansiert tverrsektorielle tiltak som følge av uklar ansvarsfordeling [26, kap. 4.2.1]. Det har hersket en oppfatning om at FAD har vært departementet med ansvar for å initiere og koordinere *alle* tverrsektorielle tiltak. I St.meld. nr. 17 (2006–2007) presiseres det at FAD kun har et særskilt ansvar for *forebyggende*, tverrsektorielle tiltak.

Utvalget foreslo at staten burde vurdere offentlige innkjøp slik at sikkerhets- og beredskapsmessige konsekvenser ved bortfall av tjenester og varer kunne kartlegges. Det ble videre uttalt at krav til sikkerhet og beredskap også burde bli stilt til underleverandører av tjenester og varer. Kritisk infrastruktur bør ideelt sett kunne erstattes av et reservesystem hvis det primære systemet går ned. Problemstillingen har vært diskutert før i form av nasjonal autonomi, det vil si muligheten til å kommunisere innenfor landets grenser uten hjelp av utenlandske operatører. FFI undersøkte mulighetene for å realisere nasjonal autonomi og kom fram til at en mellomløsning var det mest fornuftige alternativet. Det ble anbefalt å opprettholde nasjonale backupløsninger på driftssiden for noen operatører. PT fikk i 2006 bevilget ca. 21 millioner kroner for å realisere denne løsningen [18, kap. 10.1.4.2]. Det er fornuftig å la all kritisk infrastruktur ha lignende løsninger med reservesystemer som kan ta over i tilfelle uhellet er ute.

Det ble anbefalt en økt informasjonsutveksling mellom virksomheter vedrørende sikkerhet og beredskap, og da spesielt mellom virksomheter med ansvar for kritisk infrastruktur. De ulike virksomhetene bør utvilsomt dra nytte av hverandres kunnskap og erfaringer. Spesielt nyttig vil en økt informasjonsutveksling kanskje være i startfasen av nye tiltak,

hvor det kan herske usikkerhet om hvordan disse tiltakene skal følges opp.

Endringer i Sikkerhetsloven

Infrastrukturutvalget anbefalte en gjennomgang av Sikkerhetsloven slik at nødvendige endringer relatert til objektsikkerhet kunne utføres. Det ble foreslått å ta utgangspunkt i virksomhetenes risiko- og sårbarhetsanalyser for å avgjøre hvilke objekter som burde sikres. Det ble videre anbefalt at virksomhetene førte dialog med myndighetene for å avgjøre om virksomhetens objekter fallt inn under Sikkerhetsloven.

Sikkerhetsloven ble kritisert av Riksrevisjonen for ikke å være detaljert nok, og det ble etterlyst utfyllende forskrifter for loven [26, kap. 5.1]. Det ble også påpekt at loven ble vedtatt i 1998, og at det ennå ikke er utarbeidet forskrifter til loven. Det er derfor på høy tid at forskriftene utarbeides og inkluderes i loven.

Arbeidet med å utarbeide forskrift om objektsikkerhet for Sikkerhetsloven avventer forestående endringer i Sikkerhetsloven. Arbeidet med endring av Sikkerhetsloven ble stilt i bero for å avvente Infrastrukturutvalgets utredning og høringen på denne. Høringen er nå gjennomført og arbeidet med en lovendring er gjenopptatt og forventes avsluttet i løpet av 2007 [32].

Å ta utgangspunkt i virksomhetenes egne ROS-analyser er en god måte å kartlegge skjermingsverdige objekter, i og med at virksomhetene selv kan være med å evaluere egne objekter. Samtidig er det viktig at også at en ekstern part, myndighetene, er med på å avgjøre hva som bør karakteriseres som skjermingsverdig. Vedrørende gjennomføring av ROS-analyser virker det som de fleste virksomheter gjør dette. Mørketallsundersøkelsen for 2006 viste at 83% jevnlig eller av og til utførte en slik analyse, mens 17% sa at de sjelden eller aldri gjorde dette. 11% av virksomhetene karakteriserte seg selv som samfunnskritisk infrastruktur, og følgelig faller mange av disse virksomhetene og deres objekter innunder Sikkerhetslovens definisjon av skjermingsverdig. Det er viktig at de virksomhetene som utgjør en del av samfunnsskritisk infrastruktur blir fulgt godt opp gjennom tilsynsvirksomhet slik at man er sikker på at de jevnlig utfører ROS-analyser.

Ivaretakelse av sikkerhets- og beredskapshensyn ved omreguleringer og omorganiseringer

Utvalget hadde bekymringer vedrørende ivaretakelsen av sikkerhets- og beredskapshensyn ved omreguleringer og omorganiseringer i offentlige virksomheter. Det ble derfor utarbeidet en liste over sikkerhets- og beredskapsrelaterte hensyn som burde tas ved omreguleringer/omorganiseringer. Det ble i tillegg anbefalt å ikke gjennomføre endringer samtidig i tilsyn og i sentrale virksomheter som tilsynet har ansvaret for. Utvalget anbefalte videre at virksomheter med kritisk infrastruktur ikke burde bruke outsourcing i tilknytning til sikkerhet- og beredskapsarbeid.

Alle disse forslagene er fornuftige, men effekten av slike forslag er diskutabel. Så lenge dette ikke blir noe annet enn retningslinjer, er det sannsynlig at mange virksomheter ikke vil følge de. En regulering gjennom forskrift eller eventuelt lov ville vært å foretrekke. En formell regulering med oppfølging gjennom tilsyn vil gi større bevissthet og sørge for at berørte virksomheter etterlever de hensyn som skal tas ved omreguleringer og omorganiseringer.

Offentlig eierskap

Utvalget anbefalte vurdering av offentlig eierskap innen hver enkelt sektor med tilhørende virksomheter med ansvar for kritisk infrastruktur. Det ble argumentert med at dersom en krisesituasjon oppstår, vil myndighetene uansett måtte ta ansvar for å gjenopprette normal drift.

Dersom en krisesituasjon skulle oppstå med regionalt eller nasjonalt omfang vil myndighetene på de respektive nivåer være ansvarlig for å løse situasjonen. Det er ikke gitt at enhver krisesituasjon kan takles bedre dersom den kritiske infrastrukturen er under en offentlig aktør sitt ansvarsområde. Utvalget pekte på tre forhold som talte til fordel for offentlige eierskap: 1) kritisk avhengighet (oppfyllelse av grunnleggende behov), 2) absolutt nødvendighet (ingen gode alternativer eksisterer som kan fungere som midlertidige løsninger) og 3) tett kobling (bortfall av én komponent medfører bortfall av alle).

Utfallet av en krisesituasjon avhenger av hvor godt kriseledelsen og aktøren ansvarlig for den kritiske infrastrukturen er forberedt, samt hvor gode samarbeidsrutiner som eksisterer mellom de. Uavhengig om en privat eller offentlig aktør har ansvar for kritisk infrastruktur, så er det viktigste momentet at den ansvarlige aktøren er lovpålagt å etterleve sikkerhet- og beredskapskrav for kritisk infrastruktur, og at etterlevelsen følges opp gjennom tilsyn. Det er likevel naturlig at myndighetene står ansvarlige for kritiske infrastrukturer av særskilt betydning og viktighet, og de tre kriteriene som utvalget utarbeidet virker passende for å betegne slike infrastrukturer.

Kartlegging av kritisk infrastruktur og sektorvise anbefalinger

Utvalget mente at nasjonal kritisk infrastruktur burde være under norsk eierskap. Dette kan være vanskelig å oppnå i praksis, men idealet bør likevel etterstrebes. Det er en uting å gjøre kritisk infrastruktur avhengig av utenlandske selskaper av flere grunner. Markedsøkonomien kan gi utydelige eierforhold og selskap kan gjennomgå eierskifte og få en ledelse med andre mål og interesser enn tidligere. Dersom et selskap går konkurs får man et stort problem med å finne noen som kan overta driften. Man vil heller ikke ha noen som kan ta seg av eventuelle driftsforstyrrelser eller -stopp i denne perioden. Det er derfor best at staten eller eventuelt norske selskaper som staten har stor tillit til er eiere av nasjonal kritisk infrastruktur.

Utvalget anbefalte også forslag vedrørende regulering av brukere tilknyttet Internett: pålegge alle Internettilbydere å levere sikkerhetsprogramvare til kundene deres og pålegge leverandører av trådløse nettverkskomponenter å levere disse med gode sikkerhetsinnstillinger og veiledninger på norsk. Dette er gode forslag. Mange brukere unnlater å installere antivirus av ulike grunner. Dersom leverandørene pålegges å levere antivirus til kundene, er det høyst sannsynlig at flere vil installere antivirus. Det bør gjennomføres et prøveprosjekt som avdekker effekten av dette tiltaket før det eventuelt iverksettes på nasjonalt nivå. Å levere trådløse nettverkskomponenter med gode sikkerhetsinnstillinger vil gjøre at brukerne slipper å gjøre det selv. Mørketallsundersøkelsen for 2003 viste at mer enn 30% av virksomhetene unnlot å sikre trådløse nettverk med kryptering. Tallet er omtrent det samme for Mørketallsundersøkelsen for 2006, og et slikt tiltak vil redusere dette tallet dramatisk.

I tillegg til disse to forslagene ble det også foreslått et annet, tredelt forslag som trenger nærmere utredning av Samferdselsdepartementet:

- Pålegge alle privatpersoner og virksomheter å bruke oppdatert sikkerhetsprogramvare ved oppkobling til Internett
- Pålegge Internettilbydere å kontrollere at deres brukere hadde oppdatert sikkerhetsprogramvare
- Utarbeide en IKT-sikkerhetsstandard som alle virksomheter med tilknytning til Internett pålegges å følge

Disse forslagene er godt ment, men vil være vanskelig å følge opp i praksis. Det finnes et stort mangfold av sikkerhetsprogramvare med ulike funksjoner. Noen tilbyr bare antivirus, mens andre tilbyr beskyttelse mot en rekke andre trusler. Å avgjøre hvilke av disse programmene som skal godkjennes som god nok sikkerhetsprogramvare er ikke trivielt. Det er heller ikke rettferdig hvis brukerne eller leverandørene tvinges til å betale for programvare fra en eller få spesifikke leverandører hvis de foretrekker å bruke andre alternativer. Det virker derfor mer hensiktsmessig at leverandørene pålegges å levere sikkerhetsprogramvare sammen med Internettilkoblingen, og så får det heller bli opp til brukeren å installere denne eller selv å finne et annet alternativ. Det finnes ingen incentiver for ikke å installere sikkerhetsprogramvare som vederlagsfritt følger med et abonnement. Helt vederlagsfritt vil det riktignok ikke være idet programvaren til syvende og sist må finansieres av kundene. De fleste vil likevel være enige om at man bør ta i bruk et program man betaler for uavhengig om man installerer det eller ikke, og da særlig hvis det kan bidra til økt sikkerhet. Det eneste hinderet med denne løsningen er at ikke alle har nok teknisk kompetanse eller forstår viktigheten av å installere sikkerhetsprogramvare. Dette problemet vil dog høyst sannsynlig eksistere selv om man pålegger kunder å installere slik programvare. En endring i regelverket medfører dessverre ikke en automatisk økning i folks bevissthet på området.

Det siste foreslåtte tiltaket om å pålegge majoriteten av virksomhetene knyttet til Internett å følge en IKT-sikkerhetsstandard virker også vanskelig å gjennomføre. Det er kanskje mulig (men dyrt) å sørge for at majoriteten av virksomheter tilknyttet Internett følger den samme sikkerhetsstandarden dersom det drives utstrakt tilsynsvirksomhet. Hvis teknisk mulig kunne man benyttet en form for automatisert kontroll fra en sentralisert tjener. Begge disse alternativene virker meget vanskelige å realisere.

Det siste forslaget under dette kapittelet gjaldt etableringen av en tilskuddsordning for visse oppgaver knyttet til sikring av kritisk infrastruktur. Dette er en ordning som til en viss grad eksisterer allerede i dag ved at staten finansierer enkelte sikkerhet- og beredskapstjenester slik som drifting av kystradionettverket. En økonomisk tilskuddsordning vil kunne sikre initiativ og økonomisk vilje til å gjennomføre tverrsektorielle tiltak uten én hovedinteressent. Ordningen ville også ha som mål følge opp sektorovergripende infrastrukturer. Per idag er det ikke Justis- og politidepartementets ansvar å finansiere tverrsektorielle tiltak, selv om departementet kan ta initiativ til å iverksette slike tiltak [18, kap. 6.6.3]. Utvalget foreslo at behov for økonomisk tilskudd måtte dokumenteres gjennom ROS-analyser.

Å etablere en tilskuddsordning for sikring og oppfølging av tverrsektoriell kritisk infrastruktur er et godt forslag. Finansiering og oppfølging av sektorovergripende tiltak uten en hovedinteressent er et betydelig problem. Den uklare ansvarsfordelingen som har vært

i oppfølgingen av Nasjonal strategi for informasjonssikkerhet har forverret oppfølgingen av slike tiltak ytterligere. Det er derfor ønskelig med en ordning som sikrer økonomisk initiativ og gjennomføring av tiltakene dersom ansvaret ikke entydig ligger hos ett enkelt departement.

Forskning og utredning

Utvalget foreslo å utvide FFI sitt mandat til å omfatte sivil sektor. Dette er fornuftig å gjøre siden FFI har forsket mye også på samfunnets sårbarhet i sivil sektor siden 1994. "Beskyttelse av samfunn" (BAS) prosjektene har eksempelvis vært svært relevante for sivil såvel som militær sektor. Et utvidet mandat ville forhåpentligvis gjort det enklere å finansiere fremtidige prosjekter med relevans for både sivil og militær sektor. Det tok lang tid å starte det siste BAS prosjektet (BAS5) fra opprettelsen av et slikt forskningsprosjekt først ble anbefalt. Videre var det vanskelig å få samlet nok midler til finansieringen av prosjektet. Man bør derfor prøve å sikre at kompetansen i FFI bevares og videreutvikles gjennom en mer forutsigbar finansieringsmodell enn den som har vært frem til nå.

Det ble anbefalt av utvalget å etablere et forskningsprogram for gjensidige avhengigheter i kritisk infrastruktur. Forskningsprogrammet SAMRISK ble etablert i 2006 og programmet viser til Sårbarhetsutvalget og Infrastrukturutvalget for bakgrunnen til opprettelsen. Programmet er fortsatt i en innledende fase og det gjenstår å se i hvilket omfang programmet vil dekke kritiske IKT-infrastrukturer og gjensidige avhengigheter i kritiske infrastrukturer generelt.

3.3.4 Konklusjon

Ansvarsfordelingen for beskyttelse av kritisk infrastruktur bør tydeliggjøres, blant annet ved å legge overordnet ansvar for visse oppgaver til JD. Disse oppgavene inkluderer å etablere og vedlikeholde en oversikt over nasjonal kritisk infrastruktur, være pådriver for samarbeid mellom virksomheter med ansvar for kritisk infrastruktur og koordinere forskning innen sikkerhet- og beredskapsarbeid. Virksomhetene bør føre dialog med myndighetene samt nytte egne ROS-analyser for å danne oversikt over kritisk infrastruktur. Det bør foreligge en formell forpliktelse overfor virksomheter med ansvar for kritisk infrastruktur å gjennomføre periodiske ROS-analyser slik at den nasjonale oversikten er oppdatert og nøyaktig til enhver tid.

For å oppnå en mer effektiv ressursutnyttelse mellom NSM, PST og DSB kan JD fungere som koordinerende enhet. Dersom ressursutnyttelsen i dag er tilfredsstillende, men har forbedringspotensiale, er det sannsynligvis tilstrekkelig at virksomhetene i samarbeid utreder tydeligere grenselinjer og enes om plassering av ressurser.

Infrastrukturutvalget utarbeidet en liste over gode sikkerhetsprinsipper for virksomheter med ansvar for kritisk infrastruktur. Informative tiltak er nødvendige, men hovedutfordringen ligger i å meddele informasjonen på en måte som får virksomhetene til å følge den opp. En informasjonshåndbok over myndighetsorganer og hva de kan være behjelpelige med bør utarbeides slik at både offentlig og privat sektor lettere kan finne frem til det fagorganet de har behov for.

Det bør utarbeides en sektorovergripende lov om beredskap for kritisk infrastruktur slik at det samme beredskapsnivået ivaretas på tvers av sektorer. Virksomhetenes ROS-analyser

samt samtale med med myndighetene bør være grunnlaget for hva som skal identifiseres som kritisk infrastruktur.

Ansvarsforhold vedrørende kritisk infrastruktur bør utredes for å få en mer mål- og resultatorientert arbeidsmetode. Måloppnåelse er et viktig kriterium ved evaluering av tiltak, og arbeidet med sikring av kritisk infrastruktur bør derfor fokusere på dette kriteriet for bedre å kunne vurdere effekten av tiltak.

Det bør etableres en nasjonal strategi for tilsyn med kritisk infrastruktur. Uten oppfølging gjennom tilsyn vil det ofte være at tiltak ikke oppnår den planlagte effekten, for eksempel på grunn av manglende ansvarsavklaring eller manglende vilje til oppfølging.

En statlig tilskuddsordning bør etableres slik at tiltak som faller utenfor en virksomhets ansvarsområde likevel blir gjennomført dersom tiltakene er av betydning for rikets sikkerhet. Ordningen vil blant annet bidra til enklere finansiering av sektorovergripende tiltak for kritisk infrastruktur.

Offentlige sektor bør vurdere sine innkjøp slik at sikkerhets- og beredskapsmessige konsekvenser ved bortfall av tjenester og varer kan kartlegges. Kritisk infrastruktur bør ideelt sett kunne erstattes av et reservesystem ved driftsavbrudd eller -stans.

De lenge etterlyste endringene i sikkerhetsloven og utarbeidelsen av forskrift om objektsikkerhet bør gjøres snarest.

Utvalgets liste over sikkerhets- og beredskapshensyn ved omreguleringer og omorganiseringer bør følges av alle virksomheter. En formell regulering kan være ønskelig for å ivareta slike hensyn mer effektivt.

Staten bør eie eller ha mulighet til å utøve tilstrekkelig kontroll over selskaper som er ansvarlige for kritisk infrastruktur dersom staten allikevel vil sitte med ansvar for å gjenopprette normal drift i en krisesituasjon. Infrastrukturene som kvalifiserer til denne beskrivelsen er: 1) meget kritisk infrastruktur som oppfyller grunnleggende behov, 2) kritisk infrastruktur som ikke har midlertidige reserveløsninger, 3) sett med kritiske infrastrukturer med tett kobling mellom seg.

Nasjonal kritisk infrastruktur bør ikke være under utenlandske selskaper blant annet på grunn av hensynet til nasjonal autonomi.

Det bør gjennomføres et prøveprosjekt hvor en eller flere Internettleverandører leverer sikkerhetsprogramvare til sine kunder. Dersom dette viser seg å være effektivt bør alle Internettleverandører pålegges å levere sikkerhetsprogramvare til kundene sine. Alle leverandører av trådløse nettverkskomponenter bør pålegges å levere disse med en sikker konfigurasjon. Å pålegge Internettilbydere, privatpersoner og andre virksomheter å bruke oppdatert sikkerhetsprogramvare er et tiltak som vanskelig kan følges opp i praksis, og det er derfor svært tvilsomt om man i det hele tatt bør prøve på dette.

FFI sitt mandat bør utvides til å omfatte sivil sektor for å sikre en bedre kontinuitet i arbeidet om samfunnets sårbarhet.

3.4 Datakrimutvalget

3.4.1 Bakgrunn for delutredning I og II

Datakrimutvalget ble opprettet av regjeringen Bondevik II 11. januar 2002. Mandatet ga utvalget i oppgave å utrede lovtiltak mot datakriminalitet. Delutredning I hadde tittelen

"Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi". Denne konvensjonen er bedre kjent under navnet datakrimkonvensjonen (ETS 185), og mandatet til delutredning I var å tilpasse norsk lov slik at den samsvarte med konvensjonens artikler. Norge undertegnet konvensjonen 23. november 2001. Delutredning I var ferdigstilt og ble avgitt til Justis- og politidepartementet 4. november 2003.

Delutredning II handler om forslag om straffebestemmelser tilknyttet datakriminalitet på nasjonal basis. Delutredning II var ferdigstilt og ble avgitt til Justis- og politidepartementet 12. februar 2007.

Målet med delutredning I var å utarbeide "forslag til nødvendige lovtiltak for gjennomføring av Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi" [33, kap .1.1].

Målet med delutredning II var å utarbeide "forslag til straffebestemmelser om datakriminalitet som kan tas inn i den spesielle delen i den nye straffeloven" [34].

Ingen arbeidsmetodikk er beskrevet i delutredning I. Under arbeidet med delutredning II ble det avholdt 18 fellesmøter. Videre ble det holdt 2 lukkede dagsseminarer for å innvie utvalgsmedlemmene i trusselbildet og kriminalitetsformer i dagens høyteknologiske samfunn [34].

Leder for delutredning I var sorenskriver Stein Schjølberg. Utvalget bestod blant annet av Christina Christensen (på det tidspunktet seniorrådgiver ved Samferdselsdepartementet), Beate S. Dagslet (rådgiver ved Datatilsynet), Bjørn Erik Thon (forbrukerombud) og Berit Svendsen (teknologidirektør ved Telenor). Bortsett fra sistnevnte var alle utvalgsmedlemmene utdannede jurister. Utvalget bestod av totalt 8 personer.

Utvalget som foretok delutredning II ble ledet av sorenskriver Knut Rønning. Totalt 6 personer var med i utvalget. Christina Christensen (underdirektør ved Samferdselsdepartementet), Christian With (rådgiver ved Datatilsynet), og Svein Willasen (forsker ved NTNU) var blant utvalgsmedlemmene. Kun sistnevnte hadde bakgrunn fra informasjonssikkerhet (telematikk ved NTNU). De resterende utvalgsmedlemmene var jurister.

Begge delutredningene fra Datakrimutvalget omhandler lovtiltak mot datakriminalitet. Alle forslagene som behandles i rapporten er følgelig av juridisk karakter.

3.4.2 Foreslåtte tiltak: Delutredning I

Tiltakene som gjengis fra delutredning I her er hentet fra [33, kap. 1.1, 2, 3, 4]. Målet med EU konvensjonen er å "lette bekjempelsen av datakriminalitet, både på nasjonalt og internasjonalt nivå" [33, kap. 2.1]. Datakrimutvalget vurderte norsk lovgivning opp mot konvensjonen og påpekte endringer i lovverket der det ble ansett som nødvendig. Konvensjonen omfatter i alt 48 artikler hvorav de 35 første omhandler lovgivning innenfor datakriminalitet. De siste 13 artiklene omfatter praktiske forhold slik som forslag til utvidelser på senere tidspunkt og eventuelle reservasjoner mot deler av enkelte artikler.

I 2003 kom det en tilleggsprotokoll (ETS 189) for konvensjonen vedrørende rasisme og xenofobi [4]. Protokollen anses som mindre relevant for oppgaven da den kun tar for seg ett enkelt emne og blir følgelig ikke gitt videre oppmerksomhet.

[4] Begrepet xenofobi stammer fra de greske ordene xenos og phobos som betyr henholdsvis fremmed/ukjent og frykt. Xenofobi er med andre ord det samme som fremmedfrykt.

For hver av de 35 første artiklene i den opprinnelige datakrimkonvensjonen (uten tilleggsprotokollen) vil tittelen bli gjengitt. Innholdet til hver enkelt artikkel gjengis ikke, men artiklenes titler gir likevel en grov oversikt over innholdet i konvensjonen. Hensikten med denne presentasjonen er å gi et overblikk over konvensjonens innhold, samt en oversikt over de endringer som måtte gjøres i norsk lovgivning for å etterkomme innholdet i konvensjonens artikler.

De 35 første artiklene i konvensjonen er fordelt på følgende områder [33, kap. 1.1]:

Artikkel 1 Begreper og definisjoner

Artikkel 2–13 Straffebestemmelser

Artikkel 14–22 Straffeprosessuelle forpliktelser

Artikkel 23–35 Regler for internasjonalt samarbeid

Artikkel 1: Begreper og definisjoner

Følgende definisjoner er gitt av konvensjonen (her gjengitt fra [33, kap. 1.4]):

Datasystem / Computer system "any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data"

Data / Computer data "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function"

Tjenestetilbyder / Service provider "i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii. any other entity that processes or stores computer data on behalf of such communication service or user of such service"

Trafikk data / Traffic data "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service"

Et datasystem blir i konvensjonen ansett som en hvilken som helst innretning bestående av maskinvare og/eller programvare. Dette gjør at ikke bare tradisjonelle datamaskiner omfattes av definisjonen, men også for eksempel mobiltelefoner og andre enheter styrt av mikroprosessorer. En slik utvidet definisjon av et datasystem tar i betraktning den omfattende teknologiske utviklingen som har funnet sted. I dag omfatter begrepet datasystem svært mye mer enn en tradisjonell datamaskin.

Konvensjonens definisjon av data bygger på ISO-standarden. Det innebærer at all informasjon som er elektronisk representert anses å være data. Programvare omfattes også av denne vide definisjonen.

Tjenestetilbyder blir definert til å være en offentlig eller privat aktør som tilbyr elektronisk kommunikasjon til brukernes datasystemer. Begrepet omfatter også tilknyttede enheter som lagrer eller prosesserer data for en tjenestetilbyder. Om en tjenestetilbyder

tar betalt for tjenesten eller om han retter seg mot en åpen eller lukket brukergruppe spiller ingen rolle. Rene innholdsleverandører regnes ikke som tjenestetilbydere.

Trafikkdata defineres som data som genereres av et datasystem i en kommunikasjonskjede. Hensikten med trafikkdata er å rute data mellom kommunikasjonspunkter. Som eksempler på trafikkdata nevnte konvensjonen avsender- og mottakeradresse, tidspunkt for kommunikasjonen samt størrelsen på den.

Artikkel 2–13: Straffebestemmelser

Artikler om straffebestemmelser ble inkludert i konvensjonen for å sørge for at handlinger knyttet til datakriminalitet på nasjonalt nivå ble deklarert straffbare i alle deltagerland, og at passende straff kunne ilegges for disse handlingene.

Artikkel	**Endring(er) nødvendig**
Artikkel 2: Datainnbrudd	X
Artikkel 3: Dataavlytting	
Artikkel 4: Dataskadeverk	
Artikkel 5: Systemskadeverk	
Artikkel 6: Ulovlig tilgjengeliggjøring av tilgangsdata	X
Artikkel 7: Elektronisk dokumentfalsk	
Artikkel 8: Databedrageri	
Artikkel 9: Datarelatert barnepornografi	X
Artikkel 10: Vern av opphavsrett og nærstående rettigheter	
Artikkel 11: Medvirkning og forsøk	
Artikkel 12: Foretaksstraff	
Artikkel 13: Tiltak og sanksjoner	

Tabell 3.3: *Konvensjonens straffebestemmelser. Artikler merket med "X" er artikler hvor Norge måtte endre nasjonal lovgivning eller bruke reservasjonsadgangen.*

Tabell 3.3 lister konvensjonens artikler om straffebestemmelser. Tabellen indikerer også hvilke av artiklene utvalget fant det nødvendig å gjennomføre lovendringer/-tillegg for eller artikler hvor reservasjonsadgangen ble brukt.

Strengt tatt er det bare artiklene 2–10 som omhandler kriminelle datahandlinger. Artiklene 11–13 er av en annen karakter. Artikkel 12 dreier seg om foretaksstraff, det vil si straff i forbindelse med juridisk ansvarlige personer i et foretak. Artikkel 11 omhandler medvirkning og forsøk vedrørende forbrytelser som faller inn under artikkel 2–10, mens artikkel 13 er om tiltak og sanksjoner for brudd på disse artiklene. Meningen med artikkel 13 er å sørge for at alle land oppfyller visse minimumskrav i lovgivningen relatert til brudd på artiklene 2–10. Blant annet kreves det at ileggelse av straff må skje i henhold til forbrytelsens alvor, og at fengselsstraff må kunne idømmes ved alvorlige brudd på en eller flere av artiklene.

Av alle artiklene om straffebestemmelser var det kun artikkel 2 vedrørende datainnbrudd som utvalget mente det måtte gjøres lovendringer for [5]. Utvalget mente den øvre strafferammen for datainnbrudd var for lav og gikk inn for å endre straffelovens § 145 første

[5] Ordet "lovendringer" omfatter ikke *lovtillegg* slik som utvalget har brukt det.

og annet ledd til "bøter eller fengsel inntil 6 måneder *eller begge deler*" [33, kap. 2.2.3]. På denne måten ville brudd på artiklene kunne straffes med både bøter og fengsel, og ikke bare én av delene.

I tillegg til lovendringen for datainnbrudd mente utvalget at lovtillegg måtte inkluderes for artikkel 6 om ulovlig tilgjengeliggjøring av tilgangsdata (passord, tilgangskoder etc.). Utvalget foreslo derfor et lovtillegg i straffeloven (§ 145 b) som ville kriminalisere spredning av tilgangsdata.

Det ble anbefalt å bruke reservasjonsadgangen mot innholdet i to artikler: artikkel 6 om ulovlig tilgjengeliggjøring av tilgangsdata samt artikkel 9 om datarelatert barnepornografi.

For artikkel 6 ble det anbefalt at Norge benyttet reservasjonsadgangen for å hindre kriminalisering av visse typer typer programmer (programmer som ved bruk kan føre til brudd på artikkel 2–5: for eksempel virus og hackerverktøy). Utvalget begrunnet denne anbefalingen blant annet ved at forberedelseshandlinger i norsk rett normalt er straffrie, og at besittelse av dataverktøy som kan gjøre skade kan kriminalisere uskyldige personer.

For artikkel 9 anbefalte utvalget at reservasjonsadgangen ble brukt for ikke å kriminalisere anskaffelse av barnepornografi. I norsk rett er i stedet "besittelse" og "innførelse" av barnepornografi kriminalisert. Utvalget mente derfor at ordet "anskaffelse" var overflødig idet handlingen vil kunne straffes etter at materialet er nedlastet.

Majoriteten av artiklene i konvensjonen var allerede i tråd med norsk lovgivning, inkludert artikkel 13 om passende tiltak og sanksjoner ved brudd på konvensjonen. Utvalget påpekte likevel at strafferammene ville vurderes i delutredning II.

Artikkel 14–22: Straffeprosessuelle forpliktelser

Artikkel 14–22 ble inkludert i konvensjonen for å nedfelle retningslinjer i lovverket vedrørende dataetterforskning.

Artikkel 14 og 15 inneholder bestemmelser av generell karakter for innføring av de resterende bestemmelsene 16–22. Artikkel 16-22 om dataetterforskning er gjengitt i tabell 3.4.

Artikkel	Endring(er) nødvendig
Artikkel 16: Hurtig sikring av lagrede data	X
Artikkel 17: Hurtig sikring og delvis avdekking av lagrede trafikkdata	X
Artikkel 18: Utleveringspålegg	
Artikkel 19: Ransaking og beslag	X
Artikkel 20: Innhenting av trafikkdata	X
Artikkel 21: Avlytting av innholdsdata	X
Artikkel 22: Jurisdiksjon	X

Tabell 3.4: *Konvensjonens straffeprosessuelle forpliktelser. Artikler merket "X" indikerer de bestemmelser utvalget fant det nødvendig å benytte reservasjonsadgangen mot eller gjennomføre lovendringer/-tillegg for.*

Utvalgets flertall (7 av 8 personer) anbefalte at det ble opprettet en ny lovbestemmelse om sikringspålegg siden straffeprosessloven § 216 ikke dekket kravet om hurtig sikring i artikkel 16 og 17. Sikringspålegg innebærer ikke automatisk innsyn. Politiet må søke om utlevering av materiale før det gis innsyn. Utvalgets flertall anbefalte også å inkludere en

bestemmelse om utlevering av trafikkdata som er sikret gjennom et sikringspålegg for å tilfredsstille artikkel 17. I teorien kunne Post- og teletilsynet gitt fritak fra tjenestetilbydernes taushetsplikt slik at sikret trafikkdata kunne blitt utlevert. På den måten måtte hvert eneste fritak blitt innvilget av Post- og teletilsynet, og utvalgets flertall fant dette lite hensiktsmessig.

For å oppfylle et krav om opplysningsplikt ved ransaking av et datasystem (artikkel 19), foreslo utvalget et lovtillegg (§ 199 a) i straffeprosessloven. Lovtillegget ville pålegge systemadministratorer eller andre med lignende kunnskaper til å gi opplysninger som ville lette gjennomføringen av ransakingen.

Vedrørende artikkel 20 om innhenting av trafikkdata fant utvalget at konvensjonen ikke var i samsvar med norsk rett. Ifølge konvensjonen tillater artikkel 20 å innhente trafikkdata i alle tilfeller hvor det er begått brudd på artikkel 2–11 [33, kap. 3.5.3]. Dette var ikke tilfelle i norsk lovgivning, hvor terskelen for å foreta en kommunikasjonskontroll (innhente trafikkdata) var høy. Utvalget anbefalte at Norge benyttet reservasjonsadgangen på dette punktet for å beholde denne høye terskelen for kommunikasjonskontroll.

Utvalget anbefalte at Norge benyttet reservasjonsadgangen for artikkel 21 om avlytting av innholdsdata. Å bruke reservasjonsadgangen ville ikke hindret politiet i å avlytte kommunikasjon, men det ville hindret tjenestetilbyder i å gjøre det. Utvalgets oppfatning var at det er verken nødvendig eller ønskelig at tjenestetilbyder blir pålagt å avlytte kommunikasjon, men at tjenestetilbyder kan bidra med teknisk assistanse til politiet under avlyttingen.

Vedrørende artikkel 22 om jurisdiksjon anbefalte utvalget en endring i straffeloven § 12 for å sikre at overtredelser begått av norske statsborgere kunne straffes i Norge uavhengig av hvilket land forbrytelsen fant sted i. Det ble derimot ikke anbefalt at en kriminell handling begått i utlandet av en utenlandsk statsborger burde kunne straffes i Norge [33, kap. 3.7.3].

Artikkel 23–35: Regler for internasjonalt samarbeid

Artikkel 23 omhandler grunnleggende, generelle prinsipper for samarbeid mellom konvensjonsstatene, mens artikkel 24–35 inneholder spesifikke lovbestemmelser om internasjonalt samarbeid. Tabell 3.5 gjengir konvensjonens artikler for internasjonalt samarbeid.

Utvalget så ikke behov for verken lovendringer eller lovtillegg for å etterkomme betingelsene i artikkel 23–35. Derimot ble det anbefalt å bruke reservasjonsadgangen for artikkel 29 om hurtig sikring av lagrede data. Begrunnelsen for dette var artikkelens opprinnelige ordlyd ga rom for at dobbelt straffbarhet [6] ikke måtte være oppfylt for at anmodning om hurtig sikring kunne finne sted. Dobbelt straffbarhet er et kriterium som ifølge utleveringsloven § 24 må være oppfylt før utlevering kan finne sted [33, kap. 4.2.2].

Det er viktig å understreke at reservasjonsadgangen ikke ville fått følger for utlevering med hensyn til brudd på artikkel 2–13 ettersom disse handlingene ville ha vært kriminalisert i alle konvensjonsstatene. Utvalget anså derfor at kravet om dobbelt straffbarhet sjelden ville være til hinder for gjensidig samarbeid.

For mange av artiklene om gjensidig samarbeid anså utvalget at endringer i interne retningslinjer ville være tilstrekkelig for å etterkomme betingelsene i artiklene. Et viktig

[6] En handling er dobbelt straffbar hvis den er straffbar i både landet hvor lovbryteren oppholdt seg under forbrytelsen samt landet som har vært gjenstand for forbrytelsen. Handlingen må med andre ord være straffbar etter begge lands rett.

Artikkel	Endring(er) nødvendig
Artikkel 24: Utlevering av lovbrytere	
Artikkel 25: Gjensidig bistand i straffesaker	
Artikkel 26: Mulighet for uoppfordret informasjonsmeddelelse	
Artikkel 27: Regulering av gjensidig bistand i tilfeller utenfor internasjonale samarbeidsavtaler	
Artikkel 28: Taushetsplikt og begrensninger i tilfeller utenfor internasjonale samarbeidsavtaler	
Artikkel 29: Hurtig sikring av lagrede data	X
Artikkel 30: Hurtig avdekking av lagrede trafikkdata	
Artikkel 31: Gjensidig bistand angående ransaking, beslag og utlevering av lagrede data	
Artikkel 32: Transnasjonal tilgang til lagrede data	
Artikkel 33: Gjensidig bistand til innhenting av trafikkdata i sanntid	
Artikkel 34: Gjensidig bistand angående avlytting av innholdsdata	
Artikkel 35: Opprettelse av et 24/7-nettverk	

Tabell 3.5: *Konvensjonens regler for internasjonalt samarbeid. Artikler merket "X" indikerer de bestemmelser utvalget fant det nødvendig å benytte reservasjonsadgangen mot eller gjennomføre lovendringer/lovtillegg for.*

punkt for å bedre samarbeidet mellom landene var artikkel 35 vedrørende forpliktelse til å etablere et 24/7 kontaktpunkt som på kort varsel kan bistå andre land med hjelp til dataetterforskning.

3.4.3 Diskusjon: Delutredning I

Europarådet ble opprettet i 1949 med det formål å være et forum for styrking av menneskerettigheter og demokrati i Europa. I dag består rådet av 46 medlemmer hvorav alle utenom de nyeste EU landene er inkludert. USA er et av landene med observatørstatus i Europarådet.

Som det går fram av oppsummeringen var det få endringer Norge måtte gjennomføre for å være i overensstemmelse med konvensjonen siden de fleste kravene i artiklene allerede var oppfylt andre steder i lovverket. Delutredning I ble fulgt opp i Ot.prp. nr. 40 (2004–2005), og konvensjonen trådde i kraft for Norge 1. oktober 2006 [34]. Utredningen tar utgangspunkt i de minimumskrav som konvensjonen angir, og gir ikke anbefalinger utover dette [34, kap. 4.2.1].

Personvern

Konvensjonen ble sterkt kritisert både av menneskerettighetsorganisasjoner og dataindustrien da de første utkastene ble offentliggjort [35]. Utkast nr. 19 av konvensjonen, ferdig i april 2000, var det første som ble gjort tilgjengelig for offentligheten [35]. Kritikerne av

konvensjonen mente at at den ga store fullmakter til ransakelse¸ beslagleggelse og overvåkning, men at den ikke vernet om privatlivet [35]. Fra de første utkastene av konvensjonen ble utarbeidet til den endelige versjonen var ferdigstilt ble det kun gjort små endringer i ordlyden til tross for kritikernes protester [35]. Det er også et tankekors at USA, som spilte en viktig rolle i utarbeidelsen av konvensjonen, ventet helt til august 2006 med å ratifisere den [36]. USA signerte konvensjonen i 2001, men fordi en slik traktat krever godkjennelse av senatet hadde den ingen effekt for landet i perioden 2001–2006. Først da senatet stemte og ga sin godkjennelse i 2006 trådde konvensjonen i kraft. Det er på sin plass å nevne at heller ikke Norge ratifiserte konvensjonen før i 2006.

Begrepsbruk

Begrepene som brukes i konvensjonen i tilknytning datautstyr og datakriminalitet er gjennomgående svært omfattende. Dette åpner for en langt mer vidtrekkende kriminalisering av datautstyr, programvare og aktiviteter enn tidligere. En slik vid begrepsbruk er uheldig siden den fort vil omfatte langt mer enn den burde. Man risikerer at uskyldige aktiviteter ender opp med å bli kriminalisert på grunn av den vidtrekkende begrepsbruken og fordi de enkelte landene har en del innflytelse på utformingen av lovbestemmelsene. Vid begrepsbruk kan virke spesielt uheldig i udemokratiske stater ettersom omfattende kriminalisering kan bli brukt som verktøy for å oppnå større kontroll over folket. En annen bekymring i tilknytning til udemokratiske stater er at det i konvensjonen ikke er krav om dobbelt straffbarhet for brudd på lovbestemmelser som ikke faller inn under artikkel 2–11. Det medfører at dersom en udemokratisk stat definerer kritikk av myndighetene som en forbrytelse så kan denne staten be om bistand fra andre land for å etterforske slike "forbrytelser" dersom de er av en internasjonal karakter.

Siden konvensjonen ikke har en eksplisitt lovformulering og kun grove lovbestemmelser, gis det for mye rom til hver enkelt stat å definere nøyaktig hva som skal kriminaliseres. Begrepene i artiklene burde vært mindre omfattende og artiklene burde vært mer detaljerte. Med så mange forskjellige stater og lovverk kan det dessverre være vanskelig å oppnå ratifisering av alle dersom ikke den enkelte stat gis en viss frihet til å utforme lovbestemmelsen. Denne friheten må derfor vektes mot detaljeringsgraden i innholdet slik at flest mulig land ønsker å ratifisere konvensjonen. Stater med liten eller meget liberal lovgivning innen datakriminalitet brukes ofte som plattform av kriminelle fra andre land. Det er derfor viktig at konvensjonen har flest mulige medlemsland som mål, slik at man reduserer antall fristater hvor datakriminalitet ikke har konsekvenser.

Tjenestetilbydernes bekymring

Under utarbeidelsen av konvensjonen uttrykte tjenestetilbyderne sin bekymring blant annet fordi det ble åpnet for å pålegge tjenestetilbyderne å gjennomføre overvåkning, og ikke bare gi teknisk støtte til politiet under overvåkningen. Den endelige versjonen av konvensjonen endret ikke på dette. Tjenestetilbyderne kan etter konvensjonen pålegges å gi teknisk støtte til politiet under overvåkning, men kan også pålegges å gjennomføre selve overvåkningen. Å overføre politioppgaver til tjenestetilbyderne er slett ikke nødvendig og heller ikke ønskelig for tjenestetilbyderne, noe tilbyderne selv uttrykte i et brev til flere representanter i Europarådet [37].

Positive effekter som følge av konvensjonen

På den positive siden har konvensjonen gitt en internasjonal harmonisering innen lovgivning relatert til datakriminalitet. Konvensjonen er ment å være et supplement, og ikke en erstatter, til allerede eksisterende traktater og lovgivning på området slik det heter i konvensjonens artikkel 39. Konvensjonen beskriver minimumsforpliktelser som landene må oppfylle for at den kan ratifiseres.

26 land ratifiserte konvensjonen umiddelbart da den var ferdigstilt, og til nå har totalt 43 stater ratifisert den. Ratifiseringen har gitt medlemslandene en felles definisjon på datarelaterte begreper, en til viss grad felles definisjon på datakriminalitet samt retningslinjer for internasjonalt samarbeid [36]. Informasjonsteknologien er i rivende utvikling, og en oppdatering av lovverket og samordning mellom landene har utvilsomt vært på sin plass. Samtidig er det viktig at lovverket kontinuerlig tilpasses den gjeldende situasjonen på internasjonal basis, og at denne utviklingen ikke stopper med datakrimkonvensjonen.

3.4.4 Konklusjon: delutredning I

Europarådets konvensjon mot datakriminalitet spesifiserer minimumskrav som deltagerlandene må oppfylle. Norge gikk inn for å oppfylle disse minimumskravene og opprettet Datakrimutvalget. Delutredning I fra utvalget kom med forslag til endringer i lovverket eller bruk av reservasjonsadganger slik at Norge kunne ratifisere konvensjonen, hvilket skjedde 1. oktober 2006.

Norge måtte gjennomføre relativt få endringer i lovgivningen for å kunne ratifisere datakrimkonvensjonen (jf. tabell 3.4, 3.4, 3.3). Endel endringer ble innført i forbindelse med de straffeprosessuelle artiklene, men innholdet i majoriteten av artiklene kunne allerede håndheves med hjemmel i eksisterende norsk lovgivning.

Konvensjonen ble sterkt kritisert da de første utkastene endelig ble offentliggjort for ikke å ta nok hensyn til personvern og samtidig gi vide lovhjemler for ransaking, beslag og lignende. Det skjedde få endringer på bakgrunn av denne kritikken.

Konvensjonen har gått fra å bli ratifisert av 26 til 43 stater (inkludert USA). For at konvensjonen skal få tyngde, er det viktig at så mange land som mulig ratifiserer den. Hvis ikke risikerer man at det fortsatt vil finnes fristater for datakriminalitet i fremtiden.

Artiklene i konvensjonen gir medlemslandene en viktig, felles plattform for tolkning av datakriminalitet og retningslinjer for internasjonalt samarbeid. Det er viktig at artiklenes hjemler gjennomgås og at det besørges at de tar tilstrekkelig hensyn til personvern.

3.4.5 Foreslåtte tiltak: Delutredning II

Lovbestemmelsene i tabell 3.6 er hentet fra [34, kap. 11]. Rapporten presenterer i hovedsak forslag til straffebestemmelser mot datakriminalitet. I alt foreslo utvalget 19 nye paragrafer under straffeloven i et eget kapittel med tittelen "Vern av data, databasert informasjon og datasystemer". I tillegg ble det også foreslått et mindre antall endringer i straffelovens eksisterende paragrafer, åndsverksloven og markedsføringsloven. Forslagene til nye paragrafer i straffeloven er gjengitt her [34, kap. 11]:

§ 1 inneholder definisjoner av begreper slik som datasystem, dataprogram og data. Ordlyden i definisjonene er i tråd med datakrimkonvensjonen.

Paragraf	Maksimum fengselsstraff
§ 1 Definisjoner	
§ 2 Elektronisk kartlegging av datasystem	6 mnd / 1 år
§ 3 Ulovlig anbringelse av utstyr m.v.	1 / 3 år
§ 4 Ulovlig tilgang til datasystem	3 / 6 år
§ 5 Informasjonstyveri	3 / 6 år
§ 6 Datatyveri	3 / 6 år
§ 7 Datamodifikasjon	3 / 6 år
§ 8 Uberettiget bruk av datasystem m.v.	1 / 3 år
§ 9 Etterfølgende befatning med ulovlig tilegnet data og databasert informasjon	3 / 6 år
§ 10 Ulovlig befatning med tilgangsdata	1 / 3 år
§ 11 Skadelig dataprogram og utstyr	1 / 3 år
§ 12 Selvspredende dataprogram	3 / 6 år
§ 13 Driftshindring	6 / 10 år
§ 14 Masseutsendelse av elektroniske meldinger	1 / 3 år
§ 15 Identitetstyveri og bruk av uriktig identitet	3 / 6 år
§ 16 Kontomisbruk	3 / 6 år
§ 17 Grovt uaktsomt datalovbrudd	
§ 18 Grovt datalovbrudd	
§ 19 Lite datalovbrudd	

Tabell 3.6: *Foreslåtte straffebestemmelser. Brudd på den enkelte bestemmelse ble foreslått straffet med bøter eller fengsel. Forslagene til fengselsstraffenes øvre ordinære ramme og øvre ramme ved grov overtredelse er gjengitt i høyre kolonne.*

§§ 2 og 3 omhandler forberedelseshandlinger som legger grunnlag for den kriminelle handlingen som leder til målet. Utvalget mente at elektronisk kartlegging av datasystem og ulovlig anbringelse av utstyr burde kunne straffes med bøter eller fengsel. Et eksempel på elektronisk kartlegging er portskanning. Begrunnelsen for å kriminalisere elektronisk kartlegging var at det ville ha en allmennpreventiv effekt og virke holdningsskapende. Utvalget mente at elektronisk kartlegging (utenom på egne systemer) er alvorligere enn for eksempel passiv avlytting siden kartlegging som regel krever at det aktivt tas kontakt med motparten (for eksempel ved portskanning).

§ 3 kriminaliserer det å bringe utstyr til et datasystem med den hensikt å begå informasjonstyveri eller skaffe tilgangsdata på uautorisert vis. Utstyr kan her være av fysisk karakter eller for eksempel programvare. For eksempel er installering av programvare for på uautorisert vis å skaffe seg tilgangsdata en handling som kriminaliseres av denne bestemmelsen.

§ 4 kriminaliserer det å skaffe seg ulovlig tilgang til et helt datasystem eller en del av et datasystem. Passordinnbrudd og andre utnyttelser av sårbarheter for å oppnå tilgang er typiske handlinger som rammes av denne bestemmelsen. Dersom det etter innbruddet blir begått datatyveri, datamodifikasjon eller annen uberettiget bruk av datasystemet, kan dette straffeforfølges med henholdsvis §§ 5, 6 og 8 i tillegg til § 4.

§§ 5 og 6 omhandler tyveri av henholdsvis informasjon og data. Data er definert som

følger: "Enhver representasjon av informasjon som lagres eller behandles av et datasystem eller som overføres i et elektronisk kommunikasjonsnett. I tillegg omfattes enhver representasjon av informasjon som ikke er lesbar uten bruk av teknisk utstyr" [34, kap. 9.1.4]. Informasjon er i denne sammenheng det samme som databasert informasjon eller utskrift av sådan. Forskjellen mellom data og databasert informasjon ligger i at førstnevnte kun kan leses og tolkes av en datamaskin. Databasert informasjon kan derimot tolkes av et menneske. Tolkningen trenger ikke være meningsfull. Poenget er at informasjonen kan oppfattes av et menneske på en eller annet måte (for eksempel ses eller høres). Et illustrerende eksempel er forskjellen mellom en kjørbar binærfil og kildekode. Kildekoden er databasert informasjon, mens binærfilen kun er data. Bestemmelsene omfatter tyveri av data og databasert informasjon som er lagret, er under behandling eller overføres [34, kap.9.5-9.6].

§ 7 kriminaliserer datamodifikasjon. Med begrepet datamodifikasjon menes endring, ødeleggelse, sletting eller skjuling av andres data [34, kap. 9.7]. Bestemmelsen omfatter endring av alle typer data. Dette gjør at ikke bare filer, men for eksempel også databaser kommer inn under bestemmelsen. Skjuling av andres data kan bety å flytte data eller kryptere de. Det viktigste stikkordet i denne bestemmelsen er "endring" siden begrepet omfatter alle typer datamodifikasjon.

§ 8 omhandler uberettiget bruk av andres datasystemer eller elektroniske kommunikasjonsnett. Åpne trådløse nettverk faller ikke under bestemmelsen. Eksempler på bruk er "handlinger som retter seg mot prosessene, tjenestene og kapasiteten på datasystemet, herunder alle dets komponenter" [34, kap. 5.6.5]. Når en person uberettiget bruker et datasystem spiller det ingen rolle hva formålet har vært med bruken av datasystemet. For eksempel vil det fra denne paragrafens ståsted være likegyldig om personen ønsket å skaffe en liste over innholdet på harddisken eller bruke datasystemet for å laste ned en ulovlig mp3 fil.

§ 9 kriminaliserer i hovedsak bruk og spredning av data og databasert informasjon skaffet på uautorisert vis. Paragrafen er beslektet med straffelovens paragraf om heleri. Typisk rammer § 9 tyveri av data og databasert informasjon (§§ 5 og 6), men den omfatter også informasjon som stammer fra brudd på § 2, det vil si informasjon fra elektronisk kartlegging [34, kap. 9.9]. Bestemmelsen er ment å være et supplement og presisering til straffelovens hjemler som allerede kan omfatte saker av en slik karakter [34, kap. 9.9].

§ 10 rammer uberettiget befatning med tilgangsdata. Med befatning menes fremstilling, modifikasjon, anskaffelse, besittelse og tilgjengeliggjøring av skadelige dataprogrammer og utstyr. Tilgangsdata omfatter passord, adgangskoder, krypteringsnøkler og lignende [34, kap. 9.10]. For at hjemmelen kan brukes kreves det at tilgangsdataene kan gi tilgang til data, databasert informasjon eller et datasystem [34, kap. 9.10].

§ 11 kriminaliserer all befatning med skadelige dataprogrammer og utstyr. Med skadelige dataprogrammer menes for eksempel programmer som kan skaffe tilgang til datasystemer, begå data- eller informasjonstyveri og datamodifikasjon. Bestemmelsen stiller krav til at anskaffelse, besittelse og spredning av slike dataprogrammer må være forsettlig (skje med viten og vilje). I tillegg er det et krav for straffbarheten at befatningen med det skadelige dataprogrammet må være urettmessig, hvilket betyr at formålet med befatningen må være ulovlig. Fysisk utstyr som for eksempel tasteloggere omfattes også av bestemmelsen. Utvalget nådde ikke enighet om § 11 burde inkluderes i loven. Et flertall stemte i favør av bestemmelsen.

§ 12 kriminaliserer all befatning (se § 11 for definisjon) med selvspredende dataprogrammer. Formålet med et slikt program er irrelevant og programmet vil bli rammet av bestemmelsen så lenge det er selvspredende. Å initiere spredning av et selvspredende dataprogram omfattes også av denne bestemmelsen.

§ 13 omhandler driftshindring eller såkalt tjenestenekt (på engelsk "Denial of Service"). Bestemmelsen gjør det mulig å straffe handlinger eller forsøk på sådanne som leder til tjenestenekt. Tjenestenekt kan oppstå for eksempel i et nettverk ved at noen sender et større antall pakker enn nettverket er dimensjonert for. Et datasystem kan også utsettes for tjenestenekt ved at det startes et stort antall ressurskrevende prosesser på systemet. Tjenestenekt ved for eksempel fysisk jamming rammes ikke av bestemmelsen.

§ 14 gir hjemmel for straff vedrørende masseutsendelse av elektroniske meldinger uten samtykke fra mottakerne. Bestemmelsen kriminaliserer med andre ord såkalt spam eller søppelpost. Det spiller ingen rolle om mottageren for eksempel er en fysisk person eller bedrift for at bestemmelsen skal gjelde [34, kap. 9.14]. Bestemmelsen rammer naturlig nok ikke meldinger som sendes ut på bakgrunn av eksisterende kundeforhold dersom ikke mottakeren har reservert seg.

§ 15 omhandler identitetstyveri og bruk av uriktig identitet ved elektronisk kommunikasjon. Bestemmelsen karakteriserer uriktig person som en annen fysisk eller juridisk person samt en fiktiv person. Det tas hensyn til om kommunikasjonen foregår mellom parter hvor situasjonen krever at korrekt identitet oppgis, eller om omstendighetene kan gjøre det naturlig å bruke pseudonym. Mange nettjenester krever for eksempel en epost adresse som kan verifiseres, men tillater brukeren å velge et pseudonym fremfor å bruke sitt virkelige navn.

§ 16 kriminaliserer kontomisbruk med forsett om vinning. Bestemmelsen straffer uberettiget bruk av en annens konto. Med konto menes adgang til visse økonomiske rettigheter (typisk bankkonti). Det er et vilkår at kontomisbruken kan medføre tap eller fare for tap.

§ 17 gir hjemmel for å straffe handlinger som overtreder §§ 7, 9, 10 og 12 annet ledd eller 13 selv om handlingen ikke er forsettlig [34, kap. 11.1]. Bestemmelsen gir slik hjemmel for handlinger der en person har opptrådd med grov uaktsomhet.

§ 18 definerer når datalovbrudd som kan oppfattes som grove. Ifølge bestemmelsen legges det vekt på den "skade som er voldt eller kunne ha vært voldt, om lovbruddet er begått ved å bryte en beskyttelse og om gjerningspersonen har hatt eller kunne ha hatt vinning og størrelsen av denne" [34, kap. 11.1].

§ 19 omhandler hva som faller inn under definisjonen "lite datalovbrudd". Ifølge bestemmelsen nyttes definisjonen av "lite datalovbrudd" dersom "skadepotensialet er lite og om gjerningspersonen ikke har eller kunne ha hatt vinning" [34, kap.].

I tillegg til forslaget om et nytt kapittel i straffeloven (med §§ 1-19) foreslo foreslo Datakrimutvalget også visse endringer i den eksisterende straffeloven, åndsverkloven og markedsføringsloven. Disse endringene er gjengitt i tabell 3.7 (jf. [34, kap. 11.2, 11.3, 11.4].

I rapporten bemerkes det at utvalgsmedlemmene ikke kom til enighet på tre punkter angående nye bestemmelser og endringer i eksisterende bestemmelser. Den første uenigheten gjaldt § 11 om skadelige dataprogrammer og utstyr. Flertallet (4 av 6) mente at denne bestemmelsen burde inkluderes i straffeloven.

Den andre uenigheten gjaldt forslaget om filtrering (§ 76b) som ville gi hjemmel til å pålegge tjenestetilbydere å filtrere nettsteder. Dette ble støttet av et mindretall (2 av 6).

Lov og paragraf	Endring
Straffeloven, kapittel 1: Straffelovgivningens virkeområde, § 7	Paragrafen gjelder "Handling som anses foretatt på flere steder". Utvalget foreslår å endre teksten slik at virkninger av straffbare handlinger under kapittelet "Vern av data, databasert informasjon og datasystemer" anses inntrådt i Norge dersom målet for handlingen har vært et norsk datasystem eller kommunikasjonsnett.
Straffeloven, kapittel 13: Inndragning, § 69	§ 69 gir hjemmel for å inndra "ting" som har vært brukt eller kan brukes til å utføre en straffbar handling. Elektronisk lagret informasjon er en slik "ting", og utvalget foreslår å inkludere "Dataprogrammer" som et eksplisitt eksempel på elektronisk lagret informasjon.
Straffeloven, kapittel 13: Inndragning, § 76	Paragrafen gjelder inndragning av informasjonsbærer og gir hjemmel for at den som må tale inndragningen kan kreve informasjonsbæreren utlevert etter at de ulovlige data er fjernet. Utvalget foreslår å endre dette slik at myndighetene kan velge om de vil levere tilbake selve informasjonsbæreren eller kun en kopi av de data som finnes på den (etter at de ulovlige data er fjernet).
Straffeloven, kapittel 13: Inndragning, § 76a	Utvalget foreslår § 76a som en ny bestemmelse med tittel "Særregler for inndragning av konto på datasystem". Bestemmelsen gir ved inndragning av konto på et datasystem hjemmel for å pålegge tjenestetilbyder å stenge den domfeltes tilgang til systemet samt slette innhold som tilhører domfelte.
Straffeloven, kapittel 13: Inndragning, § 76b	Et mindretall foreslo å inkludere en bestemmelse om filtrering av steder på Internett under § 76b. Følgende tekst ble foreslått: "Tjenesteyter kan pålegges å blokkere tilgangen til bestemte steder på Internett for sine brukere dersom innholdet ville kunne medføre straffansvar i Norge" [34, kap. 11.2].
Straffeloven og datakrimkonvensjonens tillegg	Datakrimkonvensjonen ble i 2001 utvidet til å omfatte rasistiske og xenofobiske ytringer og handlinger av slik karakter utført gjennom et datasystem. Konvensjonstillegget var ment å ramme vesentlig minimalisering og fornektelse av forbrytelser mot menneskeheten slik som for eksempel folkemord. Utvalget foreslo å ikke utarbeide nye artikler på dette området, og laget i stedet et forslag til tekst som kan innarbeides i eksisterende deler av lovverket der hvor dette temaet ikke er godt nok behandlet fra før.
Markedsføringsloven, § 2b	Utvalget foreslo at første ledd i denne bestemmelsen burde forby markedsføringshenvendelser uten samtykke fra mottaker til fysiske personer ved hjelp av automatisk oppringningssystem. Utvalget foreslo samtidig å oppheve § 2b tredje, fjerde og femte ledd.
Åndsverkloven, § 53	§ 53a og § 53c i Åndsverksloven, samt straffelovens §§ 145, 145b og 262 omhandler alle sammen uberettiget tilgang til data og tilretteleggelse for slik tilgang. Et flertall av utvalget foreslo derfor å "implementere det vesentlige innholdet i åndsverkloven § 53a og 53c i datakrimkapittelet i den nye straffeloven" [34, kap. 5.1.2].

Tabell 3.7: *Andre foreslåtte endringer enn det som er spesifisert i kapittelet "Vern av data, databasert informasjon og datasystemer".*

Den siste uenigheten dreide seg om harmonisering av enkelte bestemmelser i straffeloven og åndsverksloven. Alle utvalgsmedlemmene var enige at en harmonisering burde gjennomføres. De var derimot ikke enige om hvordan dette burde gjøres. Et flertall (4 av 6) gikk inn for at visse vesentlige deler fra åndsverkloven ble viet plass i datakrimkapittelet i den nye straffeloven. Mindretallet ville foreløpig beholde disse vesentlige delene i åndsverkloven, og ba om en videre utredning før spørsmålet ble endelig avgjort.

Utvalgsmedlemmene var enige om alt unntatt disse tre punktene.

3.4.6 Diskusjon: Delutredning II

Delutredning II var ferdigstilt 12. februar 2007. Departementet vil etter høringsfristen 25. mai utarbeide et lovforslag som skal fremmes for Stortinget. Det er ventet at proposisjonen om straffelovens spesielle del, inklusive bestemmelser om datakriminalitet, vil bli fremmet i løpet av 2008 [29].

Hvis utvalgets utredning blir fremmet og godkjent som den er for Stortinget, blir resultatet et nytt kapittel i den kommende straffeloven med tittelen "Vern av data, databasert informasjon og datasystemer". De 19 nye straffebestemmelsene fra kapittelet om datakriminalitet vil være hovedbidraget fra utredningen.

Hovedmålsetning

Et viktig arbeid som utvalget har gjort er å samle og eksplisitt uttrykke bestemmelser relatert til datakriminalitet i en særregulering. Norge tilfredsstiller kravene i datakrimkonvensjonen, men delutredning I tok utgangspunkt i den daværende lovgivningen og søkte hjemler fra flere forskjellige deler i straffeloven for å tilfredsstille konvensjonen istedenfor å lage en særregulering. Utvalget har under arbeidet med delutredning II sett det som hensiktsmessig å samle relevante bestemmelser på ett sted, noe som er en fornuftig avgjørelse tatt i betraktning antall bestemmelser utvalget har ansett som nødvendig å innføre. Kapittelet om "Vern av data, databasert informasjon og datasystemer" uttrykker eksplisitt de hjemlene som datakrimkonvensjonen krever i sine artikler og går i flere tilfeller lenger enn det datakrimkonvensjonen krever. Kapittelet er tenkt en plass i den nye straffeloven.

Med den raske utviklingen som har vært innen datakriminalitet er det klokt å skape oversiktliglig lovgivning på området. Dette argumentet forsterkes av at det mest sannsynlig vil være behov for mange endringer også i fremtiden grunnet den raske teknologiutviklingen. Eksplisitte lovformuleringer om datakriminalitet gjør at man unngår tolkninger fra lovbestemmelser som ble innlemmet i lovverket før datamaskinen ble oppfunnet.

En undersøkelse utført av Symantec i 2006 plasserte Norge som land nummer 5 på listen over opphavsland for angrep mot europeiske datasystemer [38]. Kun USA, Kina, Storbritannia og Tyskland var over Norge på rangeringen. Hvor stor del av angrepene som utføres av nordmenn vites ikke, men rangeringen illustrerer likevel viktigheten av at man må bruke alle tilgjengelige hjelpemidler for å bekjempe datakriminalitet, inkludert lovverket.

Forholdet til delutredning I

Forslagene i delutredning II går lenger enn forslagene som ble implementert for å kunne ratifisere datakrimkonvensjonen. Utvalget mente "at det på flere områder kan være ønskelig

å gå lenger i å oppstille et strafferettslig ansvar for handlinger som rammer eller misbruker dataressurser, enn det som følger som minimumskrav etter konvensjonen" [34, kap. 4.4.2]. Mer konkret er det §§ 2, 3, 8, 9, 14, 15 og 16 som strekker seg klart lenger enn det datakrimkonvensjonen krever (se tabell 3.8) [34, kap. 5.1.3].

Paragraf
§ 2 Elektronisk kartlegging av datasystem
§ 3 Ulovlig anbringelse av utstyr m.v.
§ 8 Uberettiget bruk av datasystem m.v.
§ 9 Etterfølgende befatning med ulovlig tilegnet data og databasert informasjon
§ 14 Masseutsendelse av elektroniske meldinger
§ 15 Identitetstyveri og bruk av uriktig identitet
§ 16 Kontomisbruk

Tabell 3.8: *Bestemmelser som går utover minstekravene i datakrimkonvensjonen.*

At utvalget har gått inn for en egen bestemmelse mot masseutsendelse av elektroniske meldinger er spesielt positivt med tanke på det omfang problemet har i dag. Det er riktignok tvilsomt om bestemmelen vil redusere problemet i særlig grad da mesteparten av slik epost kommer fra land som Kina og USA, men det er likevel utvilsomt riktig å forby det. Positivt er det også at utvalget går inn for å kriminalisere spredning av tilgangsdata, et emne som per idag ikke faller innunder straffeloven. Generelt sett kan innføringen av de fleste foreslåtte bestemmelsene forsvares som rettferdige. Det finnes likevel visse bestemmelser i forslaget som er mer kontroversielle enn andre.

Det er fullt forståelig at utvalget ønsker å betrakte §§ 3, 8, 9, 14, 15 og 16 som mer straffverdig enn det som er spesifisert i datakrimkonvensjonen. Det er vanskeligere å forsvare § 2 om elektronisk kartlegging, noe som diskuteres under avsnittet om forberedelseshandlinger. Handlinger som bryter mot de førstnevnte bestemmelsene kan medføre store konsekvenser og strenge reaksjoner er derfor viktig for allmennpreventive hensyn. Vel så viktig er det at personer som utfører handlinger som bryter med disse bestemmelsene møtes av en reaksjon som står i stil med alvorligheten av handlingens utfall. Reaksjonene mot datarelaterte forbrytelser hhittilils vært svært milde. Dette kan skyldes dels at lovgivningen ikke har holdt tritt med den eksplosive teknologiske utviklingen og at samfunnet ikke fullt og helt har innsett dimensjonen av de konsekvenser datakriminalitet kan få.

Tabell 3.9 illustrererrer de straffebestemmelser i utvalgets utkast som dekker de ulike artiklenes straffebestemmelser i datakrimkonvensjonen.

Om forberedelseshandlinger

§ 2 om elektronisk kartlegging er en av flere bestemmelser som straffer forberedelseshandlinger. Tabell 3.10 gjengir alle de lovbestemmelser i forslaget som omhandler såkalte innledende handlinger eller forberedelseshandlinger.

§ 2 kriminaliserer elektronisk kartlegging slik som portskanning. Utvalget mente dette burde gjøres for å oppnå en allmennpreventiv og holdningsskapende effekt. Elektronisk kartlegging kan inngå som en forberedelse for datainnbrudd og lignende, men trenger slett ikke gjøre det. Videre er slik kartlegging en metode som brukes av systemadministratorer

Artikkel i konvensjonen	Bestemmelse(r) i utvalgets utkast
Artikkel 2: Datainnbrudd	§ 4
Artikkel 3: Dataavlytting	§§ 5 og 6
Artikkel 4 og 5: Dataskadeverk og systemskadeverk	§§ 7 og 13
Artikkel 6: Ulovlig tilgjengeliggjøring av tilgangsdata	§§ 10 og 11
Artikkel 7: Elektronisk dokumentfalsk	Dekkes i dag av straffelovens §§ 179–186. Utvalget anbefalte en oppdatering i lovverket selv om delutredning I konkluderte med at dagens regler var tilstrekkelige for konvensjonen.
Artikkel 8: Databedrageri	§ 16
Artikkel 9: Datarelatert barnepornografi	Dekkes av straffelovens § 204a. Utvalget mente reguleringen av barnepornografi burde være medienøytral og ville følgelig ikke ha en egen regulering om dette i særreguleringen.
Artikkel 10: Vern av opphavsrett og nærstående rettigheter	§§ 4–6 og §§ 10–11
Artikkel 11: Medvirkning og forsøk	§§ 15 og 16
Artikkel 12: Foretaksstraff	Dekkes per i dag av straffeloven § 48a og § 48b. Reglene er videreført i ny straffelov §§ 27 og 28.
Artikkel 13: Tiltak og sanksjoner	Dekkes i hver enkelt bestemmelse under det foreslåtte datakrimkapittelet.

Tabell 3.9: *Forholdet mellom artikler i datakrimkonvensjonen og de bestemmelser i utvalgets utkast som dekker de respektive artiklene.*

Paragraf
§ 2 Elektronisk kartlegging av datasystem
§ 3 Ulovlig anbringelse av utstyr m.v.
§ 10 Ulovlig befatning med tilgangsdata
§ 11 Skadelig dataprogram og utstyr
§ 12 Selvspredende dataprogram

Tabell 3.10: *Forslag til lovbestemmelser som omhandler innledende handlinger.*

og sikkerhetsansvarlige for å avdekke tjenester som ikke burde kjøre på maskinene deres. Berettiget bruk av elektronisk kartlegging mot egne systemer vil naturlig nok ikke bli straffet av bestemmelsen dersom den trår i kraft.

§ 3 kriminaliserer ulovlig plassering av utstyr eller programvare for å foreta uberettiget avlytting av elektronisk kommunikasjon. Dette omfatter for eksempel installering av skjuvideokameramea for å fange opp PIN koder som tastes i en minibank eller installering av programvare eller fysisk utstyr for å fange opp passord på et datasystem. Det må kunne sies at en handling som bryter med § 3 normalt bør anses som mer alvorlig enn en handling som bryter med § 2 grunnet at terskelen for å bryte mot § 3 ligger høyere enn for § 2. Med andre ord kreves det mer for arbeid å utføre en handling som bryter mot bestemmelsen i § 3 enn § 2. Samtidig er også en handling som bryter mot § 3 en større inngripen mot datasystemet enn en handling som bryter mot § 2.

§ 10 kriminaliserer ulovlig befatning med tilgangsdata. Befatning innebærer all fremstilling, modifikasjon, anskaffelse, besittelse og tilgjengeliggjøring. Den forberedelseshandlingen som kanskje vil rammes mest av bestemmelsen er fremstilling av tilgangsdata slik som passordknekking. Prinsipielt burde det ikke være noe i veien for at en slik forberedelseshandling kriminaliseres siden handlingen i mange tilfeller kan sammenlignes med forsøk på tyveri av tilgangsdata.

§ 11 kriminaliserer befatning skadelig dataprogrammer og utstyr. Utvalget var ikke enige om denne bestemmelsen. Et flertall (4 av 6) stemte for. Ved høringsrunden for delutredning I tok særlig Økokrim til orde for at artikkel 6 burde innføres uten reservasjoner, og skadelige dataverktøy ble karakterisert som "elektronisk sprengstoff" av etterforskningsenheten [34, kap. 5.7.5]. Bestemmelsen kriminaliserer all befatning med slike verktøy. Befatning inkluderer også besittelse. Det er vanskelig å se hvordan befatning, og herunder spesielt besittelse, av slike verktøy kan kvalifisere til forberedelseshandlinger som bør kriminaliseres, siden majoriteten av kriminaliserte forberedelseshandlinger "gjelder alvorlige straffbare handlinger, for eksempel anslag mot rikets sikkerhet (straffeloven § 94) og andre terrorhandlinger (straffeloven § 147 a fjerde ledd)" [33, kap. 2.6.3.2].

Mindretallet argumenterte forøvrig for sitt syn med følgende utsagn: "Ser man bort fra besittelse av særlig farlige gjenstander, for eksempel plutonium og uran (straffeloven § 152 a) eller sprengstoff (straffeloven § 161) er det normalt ikke straffbart å besitte gjenstander som kan benyttes til kriminelle formål, heller ikke om dette var hensikten med anskaffelsen. Med unntak av selvspredende dataprogram (se kapittel 5.7.6), mener mindretallet at den type verktøy som omtales i artikkel 6, neppe kan sies å være verktøy som i seg selv er spesielt skadelig eller farlige. Som det vil bli redegjort for i det følgende, er det hovedsaklig snakk om dataprogrammer som i tillegg til å kunne brukes til å begå straffbare handlinger som datainnbrudd, også kan benyttes til lovlige og nyttige formål." [34, kap. 5.7.5].

§ 12 omhandler selvspredende dataprogram. På dette punktet var utvalget enstemmig. Av preventive hensyn kriminaliserer bestemmelsen befatning med slike programmer uansett hva formålet er med programmet. Egenskapen med å kunne spre seg selv er ifølge utvalget det som gjør en kriminalisering av all befatning viktig. All befatning unntatt besittelse ble foreslått kriminalisert siden besittelse som hovedregel skjer på ufrivillig basis av intetanende datamaskineiere. Bestemmelsen er fornuftig da ingen programmer har et reelt behov for å være selvspredende. De fleste programmer av denne typen er ondsinnede og kan komme i form av virus, ormer, eller programmer som muliggjør organisering av

botnettverk [7]. Uansett er slike programmer et stort problem på Internett og en kriminalisering kan forhåpentligvis avhjelpe situasjonen noe. Det er likevel viktig å huske på at Internett ikke kjenner noen landegrenser, og det spørs derfor om bestemmelsen vil kunne bidra med noe særlig utover det å gi en signaleffekt om at befatning med selvspredende programmer ikke tolereres.

Kriminalisering av innledende handlinger eller forberedelseshandlinger er et kontroversielt tema. Utvalget drøftet dette temaet vedrørende behandlingen av artikkel 6 (ulovlig tilgjengeliggjøring av tilgangsdata) i datakrimkonvensjonen. Denne drøftingen fra delutredning I er gjengitt her [33, kap. 2.6.3.2]:

> *"Ved vurderingen av om Norge bør reservere seg, er det etter utvalgets oppfatning naturlig å ta utgangspunkt i at artikkel 6 retter seg mot ulike forberedelseshandlinger. Etter norsk rett er slike handlinger normalt straffrie. Et grunnleggende synspunkt i norsk lovgivningstradisjon er at straffelovgivningen ikke bør ramme flere handlinger enn det reelt sett er grunn til å kriminalisere, jf. Straffelovkommisjonens prinsipielle drøftelse i NOU 2002: 4 Ny straffelov s. 79-86. Straff er samfunnets skarpeste reaksjon mot uønsket atferd, og bør brukes med varsomhet. Særlig varsom bør man være med å kriminalisere forberedelseshandlinger. Slike handlinger krenker normalt ikke beskyttelsesverdige interesser, og det kan være usikkert om den straffbare handlingen som forberedes, vil bli gjennomført. I straffeloven finnes det derfor bare få bestemmelser som retter seg mot forberedelseshandlinger. De fleste av disse gjelder alvorlige straffbare handlinger, for eksempel anslag mot rikets sikkerhet (straffeloven § 94) og andre terrorhandlinger (straffeloven § 147 a fjerde ledd)."*

I NOU 2002: 4 ("Ny straffelov") ble følgende sagt om kriminalisering av forberedelseshandlinger (kap. 5.2.4):

> *"Kommisjonen har drøftet spørsmålet om kriminalisering av forberedelseshandlinger på bakgrunn av en utredning skrevet av professor Erling Johannes Husabø ved Universitetet i Bergen. Husabø mener at det ikke er dokumentert tilstrekkelig behov for en så vesentlig utvidelse av straffeansvaret som et generelt forberedelsesansvar vil innebære. Et slikt ansvar vil medføre uheldige innskrenkninger i handlefriheten med økt vekt på straffverdigheten av rent subjektive forhold – gjerningsmannens sinnelag – noe som skaper bevisvanskeligheter og økt risiko for uriktige domfellelser. Et utvidet ansvar for forberedende handlinger innebærer også utvidet adgang til å anvende straffeprosessuelle tvangsmidler på et tidlig stadium, noe som blant annet vil gi større mengder overskuddsinformasjon. Erfaringer fra andre land viser dessuten at en generell regel om straff for forberedelseshandlinger lett vil bli abstrakt og upresis. Ifølge Husabø rammer ikke innvendingene i samme grad en eventuell generell regel om kriminalisering av avtaler om lovbrudd. Men også et slikt ansvar vil gjøre innhugg i den private handlefrihet og vil åpne for mer kontroll av privatlivet.*

[7] Botnettverk er nettverk av infiserte vertsmaskiner som styres av en eller flere datamaskiner. Mengden vertsmaskiner muliggjør for eksempel DoS angrep i svært stor skala.

> *Kommisjonen finner, i tråd med professor Husabøs syn, ikke grunn til å innføre et generelt straffebud rettet mot forberedelse av straffbare handlinger, heller ikke begrenset til visse typer forberedelseshandlinger, som avtaler om å begå lovbrudd."*

Datakrimutvalget konkluderte under delutredning I med at Norge burde bruke reservasjonsadgangen for artikkel 6 i og med at den rettet seg mot ulike forberedelseshandlinger som tradisjonelt sett er straffrie i norsk rett. Som drøftelsene viser eksisterer det tungtveiende grunner for ikke å kriminalisere forberedelseshandlinger på et generelt grunnlag. Man bør heller fokusere på å inkludere forberedelseshandlinger som skjerpende omstendigheter til mer alvorlige, kriminelle handlinger.

I delutredning II endret utvalget mening angående artikkel 6. Et flertall i utvalget for delutredning II mente at §§ 10 og 11 burde innføres slik at reservasjonsadgangen mot artikkel 6 kunne trekkes. Endringen har muligens sammenheng med at tilnærmet alle utvalgsmedlemmene ble byttet ut før arbeidet med delutredning II ble påbegynt. Videre bør man huske på at delutredning I kun gikk inn for å dekke minimumskravene i datakrimkonvensjonen. Følgelig ble det heller ikke gitt anbefalinger utover lovtiltak som dekket disse kravene.

Mindretallsforslaget om filtrering

Mindretallsforslaget om filtrering på IP nivå (§ 76 b) har fått mye oppmerksomhet i mediene. 2 av 6 utvalgsmedlemmer, inkludert utvalgets leder, stemte for forslaget. Uavhengig av at flertallet stemte imot, kommer forslaget til å bli lagt frem for justisministeren og bli behandlet i Stortinget. Justisministeren har stilt seg avventende til forslaget med følgene utsagn: "Jeg er en tilhenger av det frivillige filteret vi har i Norge i dag. Det er et viktig instrument i bekjempelsen av barnepornografi. Hvis vi skal vedta nye lover i forhold til filtrering, må vi passe på å ikke krenke ytringsfriheten og at de må være mulige å håndheve" [39]. Teknologenens eneste representant i utvalget, Svein Wilassen, tilhører flertallet som går mot dette forslaget. Han er tidligespesialetterforskerker ved Økokrim og nåværende stipendiat ved NTNU og har karakterisert forslaget som "hårreisende" og sammenlignet det med kinesisk nettsensur [39].

Mindretallet mente at lovverket må gjelde uavhengig av hvilken kanal materialet distribueres gjennom. I teorien er dette er et godt argument. I praksis vil det legge strengere restriksjoner på informasjonen nordmenn kan finne på nettet enn det de kan finne i magasiner/blader i kiosken. I dag selges for eksempel blader gjennom Narvesen med informasjon om pengespill i utlandet og hvordan man satser på dette. Bladene inneholder forøvrig også alkoholreklame. Markedsføring av slike pengespill og alkoholreklame er forbudt i Norge, men bladene selges allikevel fordi regelverket tillater dette sålenge bladene er produsert i utlandet og for et utenlandsk marked (jf. Alkohollovens forskrift § 9-3).

Markedsføringsloven omtaler ikke eksplisitt markedsføring fra utlandet, og det såkalte senderlandsprinsippet som omtales i flere EU direktiver har blitt normgivende innen dette området. Senderlandsprinsippet kan oppsummeres slik: "Den næringsdrivende skal forholde seg til regelverket i den staten der vedkommende er etablert. I tillegg innebærer prinsippet at andre EØS-staters myndigheter som hovedregel må godta den næringsdrivendes handlinger så lenge de er i overensstemmelse med regelverket i etableringsstaten" [40]. Dette

praktiseres i norsk rett. Unntatt fra prinsippet er markedsføring som kommer fra utlandet men er rettet spesifikt mot det norske markedet. Slike aktører må rette seg etter norsk lovgivning. Konsekvensen av å ha en regel om å filtrere alt innhold som er straffbart ifølge norsk lov vil blant annet pålegge Internett en strengere sensur for markedsføring enn det som gjøres for andre medier.

En omstridt sak som rammes av forslaget er pengespill. Pengespill slik som poker er forbudt på norsk jord, men det er derimot ikke forbudt å spille på tjenere som befinner seg i utlandet fra en norsk terminal. Hvis mindretallets forslag får gjennomslag vil blant annet alle utenlandske steder som tilbyr pengespill bli filtrert bort for brukerne. Et viktig argument for at vi i Norge har statlig kontroll over pengespill er å begrense spillavhengighet. Da er det et stort paradoks at det drives aggressiv markedsføring fra Norsk Tipping og Norsk Rikstoto sin side samtidig som det snakkes varmt om å skjerme de spillavhengige. Videre kan man spørre seg hvorfor kommunene nektes av kulturdepartementet å velge om de vil ha statlige spillemaskiner og hvorfor den norske stat indirekte og direkte har investert 2,3 milliarder kroner i utenlandsk kasinovirksomhet gjennom petroleumfondet [41].

Ser man på nabolandene Sverige og Danmark er situasjonen motsatt i de to landene. I Sverige har de konkludert med at det å spille pengespill over Internett via andre lands tjenere er lovlig. På den andre siden har man i Danmark konkludert med at pengespill via utenlandske tjenere er ulovlig siden virkningen av et slikt tilbud er tolket til å gjøre seg gjeldende også i Danmark [42, kap. 6.5].

En annen viktig faktor bak forslaget om filtrering var ønsket om å stoppe befatning med barnepornografi. I 2004 ble det etablert et frivillig filter etter et samarbeid mellom Telenor og KRIPOS [34, kap. 3.7.2]. I dag er de fleste Internettleverandører med på denne ordningen og blokkerer således alle nettsider som er svartelistet i denne sammenhengen. Filteret virker ikke mot peer-to-peer tjenester, epost og andre distribusjonsmetoder. Det er et faktum at mye av denne utvekslingen foregår i det skjulte. Mindretallet innså at et filter på leverandørnivå ikke vil blokkere all uønsket trafikk, men regnet med at det ville ha en viss effekt, og da spesielt på nye interesserte. Svein Willasen tilhørende flertallet mente at "dagens ordning, hvor politiet sporer opp den enkelte som distribuerer slikt innhold, vil bli undergravet av dette systemet" [39]. Politiet vil måtte gå gjennom rettssystemet for å få svartelistet hver enkelt nettside med barnepornografi, noe som vil lede til langt mer treghet i prosessen samtidig som viktige ressurser blir beslaglagt.

Flertallet fant at hensynet til ytringsfriheten måtte veie tyngst i spørsmålet om filtrering. Internett og dets infrastruktur er basert på åpenhet og frihet, og slik bør det være også i fremtiden. Mindretallet argumenterte med at ytringsfriheten ikke vil bli innskrenket siden filtreringen kun gjelder innhold som allerede er definert som straffbart ifølge norsk lov. Filtreringsmetodene som benyttes idag, innholdskontroll ved hjelp av søketermer og blokkering av målverter, er ikke avanserte nok til å tilby en rettferdig filtrering. Disse filtreringsmetodene vil gjøre at også legitimt innhold vil bli blokkert siden tjenere tilhørende én tjenesteleverandør ofte er ansvarlige for innhold fra flere forskjellige aktører [34, kap. 5.13.3]. Filtrering er med den nåværende teknologien slett ingen nøyaktig vitenskap. I dag er det forøvrig andre bestemmelser som gjelder for medier slik som TV og blader derom de publiserer sitt innhold fra utlandet og ikke spesifikt mot det norske markedet. Internett er et overnasjonalt medium og man kan således ikke uten belegg påstå at alle nettsider retter seg mot det norske markedet. Å innføre filtrering på Internett vil

derfor gi en inkonsekvent lovgivning samtidig som legitimt innhold vil bli blokkert.

Et bestemmelse om filtrering vil ikke ramme de ansvarlige for den straffbare handlingen. Den vil i stedet ramme nettleverandørene. Internettleverandørene vil kunne få den uønskede rollen som redaktør for Internetts innhold, og vil kunne straffes for ikke å følge pålegg om filtrering av nettsteder. Datakrimkonvensjonen tar sikte for at kriminelle handlinger skal bekjempes i opprinnelseslandet. Dette taler også imot en filtrering som virkemåte for å hanskes med uønsket innhold. Personene bak det ulovlige innholdet er de som bør stilles til rette, ikke nettleverandørene.

Ved å ha filtrering på tilbydernivå tvinger man også leverandørene til å sette av ressurser til å utføre en jobb som de ikke vil få kompensasjon for. Det vil forøvrig være ressurskrevende å gjennomføre filtrering også for domstolene. Mindretallet foreslo at hver enkelt nettside som strider mot lovgivningen skal svartelistes av domstolen etter manuell vurdering. Ifølge forslaget må en ny manuell vurdering til for å oppheve blokkeringen hvis innholdet på nettsiden endres.

I tillegg til å være ressurskrevende og kostbart vil filtrering ha begrenset effekt. Det finnes flere tekniske løsninger for å omgå eventuelle blokkerte sider. For eksempel kan man benytte en proxy, en slags mellommann, som kan formidle nettsidene til mottager istedenfor at nettsiden sendes direkte fra den blokkerte tjeneren til mottager (noe som er umulig hvis siden er blokkert).

Filtrering er slett ikke vanlig blant vestlige land vi liker å sammenligne oss med. Skulle dette forslaget få gjennomslag i Stortinget vil Norge ha en av de strengeste, om ikke den strengeste, Internettlovgivningen i Vesten. Blant ikke-vestlige land som bruker filtrering i svært utstrakt grad er Kina, Vietnam, Iran, Syria og Nord-Korea [43]. I Danmark og Sverige bruker man, som i Norge, kun et filter rettet mot barnepornografisk materiale [43].

3.4.7 Konklusjon: delutredning II

Hovedarbeidet gjort i delutredning II har vært å lage et kapittel om straffebestemmelser for datakriminalitet med tittelen "Vern av data, databasert informasjon og datasystemer". Kapittelet samler eksisterende lovbestemmelser som indirekte eller direkte er relatert til datakriminalitet og uttrykker disse eksplisitt sammen med forslag til nye lovbestemmelser. Arbeidet som er gjort med å samle og oppdatere bestemmelser er viktig fordi lovgivningen har hatt og fortsatt har problemer med å følge tempoet i teknologiutviklingen.

Av alle bestemmelsene om innledende handlinger kriminaliserer §§ 2 og 11 de mest uskyldige handlingene. Bestemmelsene omfatter henholdsvis elektronisk kartlegging av datasystem og skadelige dataprogrammer og utstyr. Disse bestemmelsene bør ikke inkluderes blant annet på grunn av norsk rettspraksis om at forberedelseshandlinger er straffrie sålenge konsekvensene av hovedhandlingen ikke er svært alvorlige. Et eksempel på forberedelseshandling som faller innunder denne definisjonen er terroranslag mot riket. §§ 2 og 11 kan neppe sies å oppfylle denne definisjonen. Hva angår de resterende forberedelseshandlingene i forslaget er disse av alvorligere karakter og en kriminalisering kan her lettere rettferdiggjøres selv om det er diskutabelt om dette er en fornuftig vei å gå. Et argument for kriminalisering av slike handlinger er allmennpreventive hensyn. Som hovedregel bør likevel forberedelseshandlinger være straffrie. Det er mer fornuftig at man anser

forberedelseshandlinger som en skjerpende omstendighet i de tilfeller de er blitt brukt for å gjennomføre en annen og mer alvorlig straffbar handling.

Angående mindretallsforslaget § 76 b om filtrering på tilbydernivå er svaret enkelt: en slik bestemmelse vil ødelegge prinsippene om åpenhet og frihet som Internett er bygget på og sannsynligvis gi Norge den strengeste Internettlovgivningen i Vesten. Ingen av de vestlige demokratiene vi liker å sammenligne oss med har et slikt filter. Filtrering av materiale som anses straffbart ifølge Straffeloven vil også komme til å blokkere legitime nettsider siden dagens filtreringsteknikker ikke er gode nok til å kunne skille mellom disse. Videre vil Internettleverandørene ved innføring av et slikt filter bli tildelt en sensurrolle som de verken bør eller ønsker å ha. Bestemmelsen om filtrering bør på bakgrunn av disse argumentene og flere andre ikke bli vedtatt av Stortinget.

Med Datakrimutvalgets delutredning II har lovbestemmelser om datakriminalitet fått en sårt trengende oppdatering. Dersom alle lovbestemmelsene blir godkjent som de er presentert i utvalgets rapport vil Norge få en svært restriktiv lovgivning på området. Det kan argumenteres for at lovgivningen vil bli i overkant restriktiv. Dette gjelder særlig hvis bestemmelsen om filtrering skulle få gjennomslag.

Kapittel 4

Andre sentrale arbeider om informasjonssikkerhet

Dette kapittelet tar for seg to andre arbeider som i likhet med de tre nedsatte utvalgene er helt sentrale i myndighetenes satsing på nasjonal informasjonssikkerhet. De to dokumentene som drøftes i dette kapittelet er Nasjonal strategi for informasjonssikkerhet og Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur. Nasjonal strategi for informasjonssikkerhet gir et helhetlig bilde av myndighetenes satsing på området, mens Riksrevisjonens undersøkelse gir en vurdering av dette arbeidet. For hvert av dokumentene gis en oppsummering før det diskuteres og konkluderes.

4.1 Nasjonal strategi for informasjonssikkerhet 2003

4.1.1 Oppsummering av strategien

Nasjonal strategi for informasjonssikkerhet ble foreslått som et tiltak i St.meld. nr. 17 (2001–2002). Denne meldingen hadde tittelen "Veien til et mindre sårbart samfunn" og kom i kjølvannet av Sårbarhetsutvalgets rapport. Stortingsmeldingen dannet grunnlaget for opprettelsen av den nasjonale strategien. NHD hadde ansvaret for strategien frem til FAD (daværende Moderniseringsdepartementet) tok over dette arbeidet høsten 2004 grunnet endringer i departementstrukturen.

Strategien tar utgangspunkt i en rapport utgitt av OECD: "Retningslinjer for sikkerhet i informasjonssystemer og nettverk" [44]. Strategien henvender seg først og fremst til myndighetene og næringslivet, men ønsker også å nå fram til privatpersoner og øke bevisstgjøringen på det området.

Formålet med strategien er definert som følger [44]:

1. "Å sikre en helhetlig tilnærming til arbeidet med informasjonssikkerhet som grunnlag for politiske beslutninger og prioriteringer."
2. "Å legge til rette for bedre koordinering av myndigheter som arbeider med informasjonssikkerhet."

Videre skal strategien bidra til [44]:

- "å redusere sårbarheten ved alminnelig bruk av IT og i kritisk IT-infrastruktur"
- "å legge til rette for trygg elektronisk forretningsdrift i privat og offentlig sektor samt sikre og pålitelige nettjenester fra det offentlige." (sic)

Strategien beskriver også regjeringens fire overordnede mål for informasjonssikkerhet [44]:

1. "Samfunnskritisk infrastruktur for elektronisk informasjonsutveksling skal være robust og sikker i forhold til de trusler den utsettes for. Kritiske informasjonssystemer skal være sikret slik at skadevirkningene ved sikkerhetsbrudd ikke er større enn hva som kan defineres som akseptabel risiko."
2. "Det skal bygges en sikkerhetskultur rundt bruk og utvikling av informasjonssystemer og elektronisk informasjonsutveksling i Norge. IT-sikkerhet skal være en sentral faktor ved forbrukernes og norske virksomheters bruk av IT."
3. "Norge skal ha en allment tilgjengelig samfunnsinfrastruktur for elektronisk signatur, autentisering av kommunikasjonspartere samt sikker overføring av sensitiv informasjon." (sic)
4. "Regelverk som berører informasjonssikkerhet skal håndheves og videreutvikles på en samordnet, og for brukere enkel og oversiktlig måte."

Foruten de overordnede målene defineres også en serie med overordnede tiltak. Disse overordnede tiltakene lyder som følger: [44]:

1. Beskytte kritisk IT-infrastruktur
2. Samordne regelverk for IT-sikkerhet bedre
3. Koordinere arbeidet med IT-sikkerhet
4. Gjennomføre risiko- og sårbarhetsanalyser
5. Klassifisere informasjon og informasjonssystemer
6. Bevisstgjøre alle aktører
7. Varsle og gi råd
8. Ansvarliggjøre bransjen og leverandørene
9. Sertifisere kritiske systemer
10. Styrke sikkerhetskompetansen
11. Legge til rette for allmenn bruk av elektronisk signatur/PKI (Public Key Infrastructure)
12. Delta i internasjonalt samarbeid

De 12 overordnede tiltakene er igjen delt inn i flere, mer konkrete deltiltak. Listen for deltiltakene gjengis her for å gi et detaljert bilde av hvordan strategiens mål er tenkt realisert (den ansvarlige part for gjennomføring av tiltak er gjengitt i parentes) [44]:

1. Beskytte kritisk IT-infrastruktur

- ➢ Risiko- og sårbarhetsvurdering av samfunnskritisk IT-infrastruktur (JD, FD, DSB, NSM og sektordepartementene)
- ➢ Prioritetsordning i telenettene (PT)
- ➢ Samlet sikkerhetsevaluering av offentlige telenett (PT)
- ➢ Utredning om robusthet mot feil og angrep i Internett (SD, NSM og NHD)

2. Samordne regelverk for IT-sikkerhet bedre

   - ➢ Regelverksgjennomgang og samordnet håndheving (JD og andre berørte departementer)
   - ➢ Utvikling av regelverk som berører IT-sikkerhet (aktuelle regelverksforvaltere og JD)
   - ➢ Utvikle en generell mal for policy for IT-sikkerhet i offentlige virksomheter, samt spesifikke deler tilpasset spesielle anvendelsesområder (AAD, andre relevante departementer og kommunesektoren)
   - ➢ Utvikle veileder for implementering av sikkerhet i private virksomheter (relevante bransjeorganisasjoner og sektormyndigheter samt Næringslivets sikkerhetsorganisasjon)
   - ➢ Felles IT-sikkerhetsnormer for helsesektoren (Sosial- og helsedirektoratet)

3. Nasjonal koordinering av arbeidet med IT-sikkerhet

   - ➢ Etablere Koordinerings- og rådgivningsutvalg for IT-sikkerhet (JD, FD, NHD og AAD)
   - ➢ Evaluere Senter for informasjonssikring (SIS) innen utgangen av 2004 og vurdere permanent ordning (NHD, JD og FD)
   - ➢ Vurdere om DSB skal få ansvar for veiledning og tilsyn av kommunene, fylkesmenn og andre virksomheter vedrørende krav til IT-sikkerhet i forbindelse med sivil beredskap (JD og FD)

4. Gjennomføre risiko- og sårbarhetsanalyser

   - ➢ Utvikling av verktøy og metoder for risiko- og sårbarhetsvurdering med fokus på små- og mellomstore bedrifter (NHD i samarbeid med bransjeorganisasjoner, regelverksforvaltere og internasjonale organisasjoner)

5. Klassifisere informasjon og informasjonssystemer

   - ➢ Klassifisering av informasjon og systemer, sikkerhetsnormer i private virksomheter (relevante bransjeorganisasjoner og sektormyndigheter i samarbeid med Næringslivets Sikkerhetsorganisasjon)

6. Bevisstgjøre alle aktører

   - ➢ Utvikle og spre informasjons- og veiledningsmateriell om IT-sikkerhet ved bruk av IT i husstandene, samt etablere en informasjonstjeneste på nett med generell informasjon og nyttige lenker til relevant tilleggsinformasjon og mulighet for å besvare spørsmål fra publikum (NHD og JD)

- ➢ Informasjonskampanje for å spre kjennskap til god praksis og utbre god praksis vedrørende sikkerhet for husstandenes datamaskiner (NHD og JD)
- ➢ Undervisning i IT-sikkerhet i skoleverket (NHD, Utdannings- og forskningsdepartementet og Nasjonalt Læringssenter)
- ➢ Øke kompetansen om IT-sikkerhet blant offentlige/private virksomheters ledere slik at de tar ansvar for å sikre at virksomhetene har tilstrekkelig IT-sikkerhetskompetanse i forhold til behov (NHD, AAD og bransjeorganisasjoner)

7. Varsle og gi råd
   - ➢ Vurdere etablering av et kriseteam for telesektoren (PT)
   - ➢ Tilgjengeliggjøre erfaringene og analysene fra VDI for aktuelle samarbeidspartnere samt etablere gode samarbeidsformer mellom Senter for informasjonssikring, Politiets datakrimsenter og VDI (NSM)
8. Ansvarliggjøre bransjen og leverandørene
   - ➢ Internettilbyderne bør sikre Internett aksess ved å bruke anerkjente sikkerhetsnormer og standarder, synliggjøre hva som kan forventes av tilgjengelighet, kapasitet, driftsstabilitet samt tilby tjenester som virusskanning, epost filtrering og oppsett av brannmur til brukerne
   - ➢ Tjenesteleverandører bør følge anerkjente sikkerhetsnormer og -standarder og gjøre kjent hvilket sikkerhetsnivå tjenesten tilbyr samt opplyse om eventuelle sertifiseringer av IT-sikkerhet som leverandørene har
   - ➢ Leverandørene av IT-systemer bør følge anerkjente sikkerhetsnormer og -standarder, opplyse om hvilken sikkerhet som kan oppnås ved anvendelse av produktet under gitte forutsetninger og tilrettelegge for enklest mulig bruk av sikkerhetsfunksjonalitet i systemene.
   - ➢ Klargjøring av ansvar for IT-sikkerhet ved bruk av utstyr som stilles til rådighet av tjenesteleverandør for andre.
   - ➢ Produkter og systemer rettet mot massemarkedet skal ledsages av lettfattelig opplysnings- og opplæringsmateriale innen IT-sikkerhet rettet mot relevante målgrupper (bruk, drift, sikkerhetsadministrasjon).
9. Sertifisere kritiske systemer
   - ➢ Etablerte sertifiseringsordninger som Norsk Akkreditering og SERTIT bør brukes mer av norske virksomheter (Norsk Akkreditering, NSM og NHD)
   - ➢ Etablerte standarder for IT-sikkerhet bør tas i bruk i offentlige og private IT-anskaffelser (både for kjøp av produkter, tjenester og utviklingsoppdrag), og norsk deltakelse i standardiseringsarbeid innen IT-sikkerhet bør styrkes (NHD, AAD, Norsk Teknologisenter og bransjeorganisasjoner)
10. Styrke sikkerhetskompetansen
    - ➢ Forskningsprogrammet IKT sikkerhet og sårbarhet (IKT SoS) er startet og bør dekke organisatoriske, bruksmessige og -tekniske sider ved IT-sikkerhet (Norges Forskningsråd, NHD, JD og FD)

- ➢ Starte et forskningsprosjekt (BAS5) som skal gi anbefalinger om tiltak for å sikre samfunnskritiske IT-infrastruktur og -systemer (DSB, NSM, JD, FD og NHD)
- ➢ Styrke sikkerhetsopplæring i utdanning hvor IT er en integrert del av utdanningen, og utarbeide læreplaner og materiell til støtte for slik undervisning (Utdannings- og forskningsdepartementet og NHD)
- ➢ Etablere flere utdanninger innen IT-sikkerhet på mastergradsnivå (Utdannings- og forskningsdepartementet i samarbeid med FD, JD, NHD, SD og Finansdepartementet)

11. Legge til rette for allmenn bruk av elektronisk signatur/PKI (Public Key Infrastructure)
    - ➢ Samordning av innføring og bruk av PKI i offentlig sektor skal skje ved det nyopprettede organet med dette formål under AAD (AAD og andre relevante departementer)
    - ➢ Prioriteres prosjekter som vil ta i bruk PKI-løsninger basert på felles krav, eller som vil gjenbruke eksisterende løsninger, samt vurdere samarbeidsprosjekter mellom offentlig og private leverandører der deltagerne kan utvikle flere typer tjenester basert på felles PKI-løsninger (AAD og NHD)
    - ➢ Leverandører av PKI-tjenester bør i felleskap utforme funksjonelle krav til samfunnsinfrastrukturen basert på behov fra leverandører av elektroniske tjenester og forbrukerne (aktuelle leverandører av PKI-tjenester og NHD)
    - ➢ Spesifisere sikkerhetsnivåene for kvalifisert sertifikat og kvalifisert signatur (NHD og aktuelle leverandører av PKI-tjenester)
    - ➢ Leverandører av PKI-tjenester utformer krav i fellesskap til testmiljø for samtrafikk dem imellom (aktuelle leverandører av PKI-tjenester og NHD)
    - ➢ Gjennomføre informasjons- og bevisstgjøringskampanjer mot forbrukerne og mot eksisterende/potensielle leverandører av elektroniske tjenester med hensyn på å ta i bruk samfunnsinfrastrukturen (aktuelle leverandører av PKI-tjenester og NHD)
12. Delta i internasjonalt samarbeid
    - ➢ Arbeide for at internasjonale fora som arbeider med IT-sikkerhet legger sine møter til Norge, slik at flest mulig norske aktører kan dra nytte av de internasjonale samarbeidsarenaene (alle departementer, næringslivets organisasjoner og standardiseringsorganisasjoner)
    - ➢ Deltagelse i EUs organ, ENISA, for nettverks- og informasjonssikkerhet (NHD, SD og UD)

4.1.2 Diskusjon

En kartlegging av oppfølgingen for de enkelte strategitiltakene har nylig blitt gjort av KIS. Kartleggingen resulterte i rapporten "Gjennomførte tiltak i Nasjonal strategi for informasjonssikkerhet 2003", offentliggjort 9. mars 2007 [25]. I rapporten beskrives fremdriften for

de ulike strategitiltakene i perioden 2003–2007. I det store og hele er det mange både pågående og avsluttede aktiviteter i forbindelse med strategitiltakene. I det følgende foretas det en gjennomgang av hva som har skjedd innenfor hvert av de 12 hovedtiltakene [25]:

1. Beskytte kritisk IT-infrastruktur [1]

   - BAS5 prosjektet i regi av FFI om metodikk for risiko- og sårbarhetsanalyse (jf. 5.1.2). Prosjektet er formelt avsluttet men en doktorgrad i tilknytning til ett av prosjektets tre hovedmål avsluttes ikke før i januar 2009 [13].
   - ROS-analyse er gjennomført i forbindelse med prioritetsordning i mobilnett som bekreftet at nettene egner seg for en slik ordning. PT har samarbeidet med Telenor og Netcom om å spesifisere påkrevd funksjonalitet. Teknisk test har blitt utført og den planlagte løsningen har blitt sendt sammen med et kostnadsoverslag til SD. DSB arbeider fortsatt med metodikk for utvelgelse av de kandidater som skal tildeles prioritering i nettene.
   - PT arbeider kontinuerlig med å kartlegge kritisk IKT-infrastruktur. I 2006 rettet kartleggingen seg mot transportnettene, og i 2007 rettes øynene mot tjenestenettene [45]. Målet er at data som samles inn skal kunne brukes til "analyser og simuleringer for å vurdere robusthet, sårbarheter og sikkerhetstiltak" [25]. Slik informasjon er blant annet blitt benyttet til å rangere viktige deler av IKT-infrastrukturen som bør ha prioritert ved tiltak for å sikre stabil tilgang på strøm.
   - PT har opprettet Internettgruppen, et forum primært for Internettilbydere som har fokus på robusthet mot feil og angrep i Internett.

2. Samordne regelverk for IT-sikkerhet bedre

   - I 2005 jobbet en arbeidsgruppe (ARI) i KIS med å identifisere mangler, overlapp og motstridenheter i ulike regelverk med relevans for informasjonssikkerhet. KIS opprettet på bakgrunn av denne gruppen i 2006 en ny arbeidsgruppe under navnet SARI: Samarbeidsgruppe for regelverk for informasjonssikkerhet. Gruppens arbeid med å gjennomgå ulike regelverk og samordne disse pågår fortsatt og skal være ferdig i løpet av 2007.
   - Statskonsult har i oppdrag fra FAD utarbeidet eksempelmodeller på prosessbeskrivelse vedrørende regelverk for informasjonssikkerhet. Resultatet kan nås fra nettstedet kunnskapsnettverk.no ved å trykke på linken "Informasjonssikkerhet, styringssystemer". Modellen beskriver stegene i en prosess for generell saksbehandling og illustrerer punkter i prosessen hvor man må ta hensyn til for eksempel loven om elektroniske signaturer.
   - Vedrørende implementering av IT-sikkerhet i private virksomheter ble det avholdt et møte i 2005. Partene i møtet var IKT Norge, Abelia, NHO, Næringslivets sikkerhetsråd og eForum. Det ble besluttet å ikke opprette nye fora, men heller utnytte de eksisterende. Næringslivsorganisasjonene skulle forøvrig fort-

[1] Strategien påpeker at begrepet informasjonssikkerhet som oftest er ensbetydende med tilgjengelighet og integritet i sammenheng med beskyttelse av kritisk IKT-infrastruktur.

løpende vurdere behov, prioritet og omfang av de tiltakene som er foreslått i strategien og berører næringslivet.

- ➢ Sosial- og helsedirektoratet utarbeidet i samarbeid med aktører i helsesektoren "Norm for informasjonssikkerhet i helsesektoren" og utga denne i september 2006. Normen er juridisk bindende for alle som har koblet seg til Norsk Helsenett.
  Oljeindustrien har også utarbeidet retningslinjer for informasjonssikkerhet i "Information Security Baseline Requirements for Process Control, Safety, and Support ICT Systems", som forøvrig trådde i kraft ved inngangen til 2007.

3. Koordinere arbeidet med IT-sikkerhet

   - ➢ Koordinerings- og rådgivningsutvalg for IT-sikkerhet ble opprettet i mai 2004 og ledes av FAD [46].
   - ➢ NorSIS ble etter tre og et halvt års prøvetid permanent etablert på Gjøvik fra og med januar 2006.
   - ➢ Vedrørende beredskap så ble nasjonalt beredskapsverk revidert vinteren 2003/2004. Dette skjedde med et fokus på sårbarhet som følge av IKT-avhengighet samt beskyttelse av kritisk IKT-infrastruktur.
     NSM og DSB utførte et felles prosjekt for å kartlegge grenselinjer seg imellom.

4. Gjennomføre risiko- og sårbarhetsanalyser

   - ➢ I 2004 ble det kartlagt ulike metoder for ROS-analyse med tanke på små- og mellomstore bedrifter, samt styringsmetoder for informasjonssikkerhet for slike bedrifter. Statskonsult overtok oversikten som ble videreutviklet i prosjektet som er nevnt tidligere under punktet om samordning av regelverk.

5. Klassifisere informasjon og informasjonssystemer

   - ➢ KIS opprettet i januar 2007 en arbeidsgruppe under navn KOBI: Klassifisering og beskyttelse av informasjon. Gruppen skal, litt forenklet sagt, "utarbeide en enkel, overordnet definering av klasser for informasjon, og hvordan informasjonen i de ulike klassene bør beskyttes" [46]. Etter planen skal gruppens rapport leveres i september 2007.

6. Bevisstgjøre alle aktører

   - ➢ Nettvett.no ble opprettet av PT i 2005 og gir råd og veiledning om informasjonssikkerhet til privatpersoner samt små- og mellomstore bedrifter.
     I 2005 ble det av SD, FAD og PT innført en IT-sikkerhetsdag rettet mot private og små bedrifter. Ved markeringen av dagen i 2006 ble det gitt ut en informasjonsavis i Aftenposten med opplag på 300.000.
     IKT Norge, NorSIS og PT skal i 2007 komme med forslag til hvordan man skal arbeide for å øke bevisstgjøringen rundt informasjonssikkerhet.
   - ➢ Medietilsynet har laget en læringspakke om informasjonssikkerhet for grunnskoler og videregående skoler. Utdanningsdirektoratet har laget en lignende pakke rettet mot lærerne.

- ➢ Et referanseforum om informasjonssikkerhet er opprettet i kraftbransjen. NVE avholder årlig seminaret "Informasjonssikkerhet i kraftforsyningen".

7. Varsle og gi råd

   - ➢ Et kriseteam for telesektoren ble vurdert opprettet av Forsvaret og telebransjen, men opprettelsen skjedde ikke på bakgrunn av vurderingen.
     For øvelser er det derimot opprettet en gruppe som skal jobbe for koordinerte tiltak og ressursbruk mellom aktørene, samt koordinert ledelse og flyt av informasjon til krisens eier.
     PT og NorCERT har inngått en samarbeidsavtale.
   - ➢ VDI ble permanent etablert fra og med 2003. NorCERT ble utviklet som prøveprosjekt på bakgrunn av erfaringene fra VDI. I januar 2006 ble NorCERT etablert som en permanent avdeling under NSM. NorCERT/NSM samarbeider blant annet med Politiets datakrimsenter, PT og NorSIS. Flere møter har blitt avholdt for bedre samarbeidet og trekke opp grenser mellom de ulike organisasjonenes ansvarsområder.

8. Ansvarliggjøre bransjen og leverandørene

   - ➢ PT har etablert Internettgruppen som et forum hvor aktører kan diskutere problemer relatert til blant annet sikker internettaksess. PT har også jobbet med å etablere flere samtrafikkpunkter mellom Internettilbyderne samt sikre ett eksisterende punkt (jf. kapittel 5.2.2).
   - ➢ PT jobber gjennom forumet Internettgruppen for at tilbydere av nett og tjenester skal lage sitt eget sett med normer og løsninger for sikkerhet.
   - ➢ PT formidler informasjon om Internett og sikkerhet til utstyrsleverandører.
   - ➢ Vedrørende ansvarsfordeling for IT-sikkerhet og bruk av utstyr stilt til rådighet fra tjenesteleverandør, så ble dette karakterisert som en løpende aktivitet. Det nevnes ingen arbeider som er utført på området.
   - ➢ Vedrørende IT-sikkerhet ved bruk av massemarked-produkter så karakteriseres dette tiltaket også som en løpende aktivitet. Ingen informasjon om aktiviteter står oppført.

9. Sertifisere kritiske systemer

   - ➢ I 2004 undergikk SERTIT en evaluering av Statskonsult, og i februar 2006 ble SERTIT internasjonalt anerkjent som sertifikatutsteder. Internasjonalt så representerer SERTIT Norge i Common Criteria Recognition Arrangement (CCRA). Gjennom deltagelsen til har Norge mulighet til å påvirke standardiseringsarbeid. SERTIT er forøvrig med i den daglige ledelsen av CCRA.
   - ➢ Vedrørende bruk og utvikling av standarder, så mottar Standard Norge årlig bidrag fra FAD og deltar i internasjonalt standardiseringsarbeid i tilknytning til IT-sikkerhet.

10. Styrke sikkerhetskompetansen

- ➢ NFR har hatt et femårig forskningsprogram under navnet IKT sikkerhet og sårbarhet (IKT SoS). Programmet har vært finansiert gjennom FAD og avsluttes formelt i 2007 selv om visse prosjekter avsluttes i 2008 [47].
- ➢ Høgskolen i Gjøvik har åpnet en mastergrad i informasjonssikkerhet. Styrking av informasjonssikkerhetsfaget i utdanning ble anbefalt i Sårbarhetsutvalgets rapport. Denne mastergraden er ikke et resultat av oppfølging fra regjeringen og departementens side, men et resultat av enkelte initiativtagere på Gjøvik og næringslivets etterspørsel etter kompetanse på området [9]. Det er senere også blitt etablert et bachelorstudium i informasjonssikkerhet på Gjøvik.

11. Legge til rette for allmenn bruk av elektronisk signatur/PKI (Public Key Infrastructure)

    - ➢ Et koordineringsorgan ble opprettet i februar 2003 for å tilrettelegge for innføring av PKI i offentlig sektor. Høsten 2004 ble organet nedlagt, men arbeidet fortsetter i Koordineringsorganet for eForvaltning (KOEF) i en egen faggruppe.
    - ➢ SEID-prosjektet (samarbeid om elektronisk ID og signatur) har omhandlet elektronisk ID (eID) og elektronisk signatur (eSignatur). Prosjektet har hatt 15 deltagere fra offentlig såvel som privat sektor. Prosjektgruppen har utarbeidet tekniske spesifikasjoner på områder de har funnet det nødvendig, og hensikten har vært å oppnå større samtrafikk og enkel bruk av eID og eSignatur.
    - ➢ I januar 2005 ble det publisert en felles kravspesifikasjon for PKI i offentlig sektor. Spesifikasjonen skal nyttes ved anskaffelse av PKI i statlig sektor og anbefales brukt også for kommunesektoren.
    - ➢ FAD har utarbeidet en ny strategi for eID og eSignatur i offentlig sektor. Strategien legges frem på våren 2007. En avtale for intern bruk av virksomhetsID og ansattID i offentlig sektor skulle etter planen være ferdig i 2006, men ble utsatt i påvente av den førstnevnte strategien som kommer i 2007.
    - ➢ To undersøkelser vedrørende forbrukernes holdninger til eID og eSignatur er gjennomført. Disse ble utført av Transportøkonomisk institutt og Norsk Gallup i henholdsvis 2005 og 2006.

12. Delta i internasjonalt samarbeid

    - ➢ FAD, SD og FD deltar i flere internasjonale fora knyttet til OECD, EU, NATO og de nordiske landende.

      DSB har samarbeidet med OECD om en felles studie på risikohåndtering i forskjellige OECD land.

      NVE deltar i en nordisk arbeidsgruppe vedrørende IT-sikkerhet i kraftforsyningen.

      PT er involvert i standardiseringsarbeid på flere områder i organisasjonene ITU og ETSI. I informasjonssikkerhetssammenheng kan man nevne TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networks), EMTEL (Emergency Communications) og Lawful Interception. Norge er også med i ENISA [2], men har der kun observatørstatus.

[2] ENISA, eller European Network and Information Security Agency, er EUs organ som jobber med

SERTIT representerer Norge i fire ulike komiteer i CCRA: Development Board, Management Committee, Executive Sub-Committee og Maintenance Board.
NorCERT (NSM) deltar i fire internasjonale grupper: 1) EGC (European Government CERT) består av de 8 viktigste nasjonale CERTene i Europa, 2) IWWN (International watch and warning network) er et forum for deling av informasjon om trusler og hendelser på Internett, 3) FIRST (Forum of Incident Response and Security Teams) består av 200 CERTer som driver forebyggende arbeid og hendelseshåndtering, 4) TF-CSIRT et forum for økt og bedre samarbeid mellom CERTer i Europa.

Det er meget positivt at det nå eksisterer en overordnet strategi for å forbedre nasjonal informasjonssikkerhet. Myndighetens tidligere satsing på området har vært noe sporadisk og ikke minst vanskelig å holde oversikt over. På forskningssiden har FFI fått bevilget midler til BAS prosjektene som i varierende grad har drøftet kritisk IKT-infrastruktur og sårbarhet, men det har ikke foreligget noen strategisk plan for å redusere sårbarheten i samfunnet som følge av IKT-avhengighet.

Det har vært etablert flere råd på myndighetsnivå for å håndtere utfordringene ved IKT og sikkerhet, eksempelvis Rådet for IT-sikkerhet i statsforvaltningen (RITS, 1996–1998), og Forum for IT-sikkerhet (FITS, 2000–2004) [46]. På bakgrunn av nasjonal strategi for informasjonssikkerhet ble Koordineringsutvalget for forebyggende informasjonssikkerhet opprettet i 2004. KIS har ansvaret for å koordinere myndighetenes satsing på informasjonssikkerhet, og er således et viktig ledd for å skape en bedre oversikt over arbeidet på området.

Man kan spørre seg hvorfor det har tatt såpass lang tid å innse behovet for en koordinert innsats på området. Strategien kom ikke før tre år etter at dot com boblen sprakk og all infrastruktur var kritisk avhengig av IKT [2]. Vidstrakt bruk og avhengighet til IKT i samfunnets infrastruktur utgjorde en svært reell trussel allerede da dot com boblen sprakk. Grunnen til at det har tatt så lang tid å utvikle en strategi på nasjonalt nivå er antageligvis sammensatt. Dels skyldes det nok at det har tatt tid å overbevise myndighetene om den trusselen utstrakt bruk av IKT uten tilsvarende sikring kan være for samfunnet, både med tanke på utilsiktede og tilsiktede hendelser. Det bør også nevnes at IT-industrien selv ikke alltid er flinke til å sette fokus på sikkerhet, og dersom industrien med all sin kompetanse ikke fokuserer på sikkerhet kan man heller ikke forvente at dette blir gjort andre steder, eksempelvis hos myndighetene.

En annen mulig årsak til satsingen på informasjonssikkerhet har kommet sent i gang kan være at det har virket lite fristende for myndighetene å se seg nødt til å investere i sikring av IT-systemer som man primært innførte for å kostnadseffektivisere offentlig sektor. Informasjonssikkerhet koster penger, og i denne sammenheng er det viktig at man foretar en så nøyaktig som mulig avveining mellom akseptabel risiko og kostnad ved å iverksette tiltak.

På den positive siden foreligger det hvertfall nå en strategi for nasjonal informasjonssikkerhet, selv om det har tatt tid før den er kommet. Strategien bidrar betraktelig til å skape et koordinert bilde av hva myndighetene gjør for å bedre nasjonal informasjonssikkerhet.

bedring av informasjonssikkerhet i unionen.

Den gjør det også enklere for myndighetene selv og andre ansvarlige aktører å beholde oversikten over hva som skjer på området.

Som det går fram av listen av tiltakene har skjedd en hel del innen satsing på informasjonssikkerhet siden strategien ble publisert i 2003. Det bør bemerkes at flere tiltak allerede var iverksatt før strategien ble publisert, men majoriteten av tiltakene ble påbegynt etter publiseringen av strategien [44].

I en vurdering av Nasjonal strategi for informasjonssikkerhet 2003 skriver KIS at strategien har et perspektiv på 2–3 år [31]. Det korte perspektivet skyldes den raske utviklingen på området. I februar 2006 nedsatte KIS en arbeidsgruppe for å evaluere den nasjonale strategien med hensyn til mål og utfordringer [48]. Gruppen avleverte rapport i mai 2006, og det ble da besluttet å revidere strategien. Tidsperspektivet på en ny strategi, eller "Retningslinjer for nasjonal informasjonssikkerhet" som den skal kalles, ble også her anbefalt å ikke overstige 3 år. Grunnen til dette tidsperspektivet skyldes at området er i rask utvikling. Da strategien ble publisert i 2003 var for eksempel trusler slik som botnett og phishing fraværende, mens de i dag er høyaktuelle.

Informasjonssikkerhet er et område i stadig utvikling, men selv om det skjer mange endringer er det ikke dermed sagt at det trengs en fullstendig ny strategi hvert tredje år. Sikkerhet er en prosess, og derfor krever mange av tiltakene en kontinuerlig oppfølging (såkalte løpende tiltak). Eksempler på dette er tiltak som bevisstgjøring og ROS-analyser, som om de skal ha en varig effekt og gyldighet, må følges opp med jevne mellomrom.

Den nåværende nasjonale strategien for informasjonssikkerhet ble publisert i juni 2003, mens revisjonen av den var ferdig i mai 2006. Det vil ta ytterligere noen måneder før den nye strategien er klar. Strategien er nå på høring i departementene, og disse må bli enige om en felles tekst før forslaget kan fremmes for regjeringen.

Etter fremdriftsplanen skal strategien offentliggjøres høsten 2007, sannsynligvis i begynnelsen av september [30]. Hvis den nye strategien publiseres i september, betyr det at den nåværende har vært gjeldende i 4 år og 3 måneder. Riktignok ble ingen nøyaktig dato for en oppfølger spesifisert i strategien, men en forsinkelse på over 1 år er relativt mye. Det er likevel to ting som gjør at en forsinkelse ikke spiller så stor rolle: den nye strategien (eller retningslinjene) vil kun være en revisjon av den nåværende, og det forventes ingen drastiske endringer. I tillegg arbeides det fortsatt aktivt med tiltak hos ulike aktører, slik at tiden ikke går til spille med å vente på den nye strategien. Grunnen til tidsoverskridelsen bør allikevel belyses av de ansvarlige partene slik at de kommende strategiene kan ferdigstilles i henhold til tidsplanen.

I revisjonen av nåværende strategi ble det påpekt at det burde vært en prioritering mellom de ulike tiltakene. Slik som tiltakslisten gjengis, presenteres alt som like viktig. Arbeidsgruppen som vurderte strategien anbefalte å prioritere følgende tiltak høyere enn andre [31]:

- Beskytte kritisk IT-infrastruktur
- Koordinere arbeidet med IT-sikkerhet
- Gjennomføre risiko- og sårbarhetsanalyser
- Bevisstgjøre alle aktører

Beskyttelse av kritisk IKT-infrastruktur er et svært viktig tiltak siden nedetid i slik infrastruktur kan få dramatiske konsekvenser i samfunnet. For å oppnå en helhetlig beskyttelse av infrastrukturen kreves det en koordinert innsats fra myndighetenes side. De to første tiltakene som foreslås gitt en høyere prioritet henger altså sammen og må begge utføres godt for å oppnå den ønskede beskyttelse av kritisk IKT-infrastruktur.

De to siste tiltakene som foreslås gitt høyere prioritet har også en forbindelse seg imellom. ROS-analyser bør primært utføres ved bedrifter og organisasjoner, og BAS5 prosjektet har arbeidet med metodikk for slik analyse som er rettet nettopp mot disse gruppene. Nå som prosjektet er avsluttet er det viktig at resultatene ikke blir liggende ubrukt. For å hindre dette må det arbeides med bevisstgjøring og om nødvendig formelle reguleringer slik at metodikken blir tatt i bruk.

Bevisstgjøring av alle aktører er et viktig tiltak. Informasjonssikkerhet omfatter alle som er i kontakt med datasystemer: privatpersoner, næringslivet og offentlig sektor. Selv om informasjonssikkerhet har betydning for alle, kan ulike aktører ha forskjellige behov innen informasjonssikkerhet. For privatpersoner er kanskje det viktigste aspektet tilgjengelighet til egne data, og følgelig bør sikkerhetskopiering vektlegges ved bevisstgjøring av denne gruppen. For bedrifter er kanskje konfidensialitet og autentisering andre og også svært viktige momenter dersom ansatte skal tillates å jobbe hjemmefra.

Bevisstgjøringstiltak har et relativt stort potensiale til å feile av ulike grunner. Årsaken kan være at målgruppen rett og slett ikke har interesse for temaet, ikke ser nytteverdi av informasjonen eller føler at det er tungvindt å følge de oppfordringer og veiledninger som gis. For å være sikker på at bevisstgjøringen har noen som helst effekt, er det derfor viktig å kunne måle graden av måloppnåelse. Dersom måloppnåelsen ikke er tilfredsstillende, bør man snarest skifte taktikk. I endel tilfeller vil det sannsynligvis lønne seg å iverksette tekniske tiltak for å kompensere for den manglende bevisstgjøringen. Denne avveiningen mellom tekniske tiltak og informasjonstiltak er noe man spesielt bør tenke på dersom privatpersoner er målgruppen. Offentlige og private virksomheter har ofte en IT-ansvarlig eller en IT-avdeling som kan ta seg av sikkerhetsspørsmål. Dette er ikke tilfellet for resten av befolkningen. Landets befolkning er en meget sammensatt gruppe som består av personer i alle aldre og med vidt foreskjellige interesser. Et stort antall av disse er helt uinteressert i teknologi og bruker den bare dersom det er helt nødvendig. Med fare for å generalisere for mye kan det hevdes at majoriteten av pensjonistene faller innunder denne kategorien. For slike brukergrupper kan man ikke vente at informasjonstiltak vil ha noen utpreget effekt, og investering i andre tiltak vil sannsynligvis gi en bedre uttelling. Et dilemma oppstår selvfølgelig når man er fullstendig avhengig av at brukeren er tilstrekkelig bevisst på visse sikkerhetsfaktorer. I slike tilfeller er man prisgitt informasjonstiltak og det beste man kan gjøre er å prøve å skifte meldingen i budskapet dersom man ikke oppnår en tilstrekkelig effekt med informasjonskampanjen.

Selvfølgelig ønsker man at også privatpersoner så godt som mulig beskytter seg fra de fleste trusler gjennom å oppdatere programvare, bruke brannmur og andre tiltak. Konsekvensen av ikke å gjøre dette kan for eksempel føre til at noen klarer å bryte seg inn i personens nettbank og stjele penger. Men dette er et tap som vil dekkes av banken, og nettopp dette gjør det mindre viktig for personen å være sikkerhetsbevisst. Konsekvensen er slett ikke dramatisk, i hvertfall ikke med dagens praksis. I fremtiden så vil kanskje regelverket stille større krav til forbrukeren med tanke på sikkerhet dersom en nettbank

skal kunne holdes ansvarlig for tapet. Kanskje det da vil betegnes som uaktsomt å ikke ha lastet ned sikkerhetsoppdateringer for operativsystemet.

Ved bevisstgjøring av brukere er det viktig å fokusere på faktiske konsekvenser som kan ramme dem selv eller deres bedrift. Informasjonssikkerhet kan være virke noe abstrakt for personer med ikke-teknisk bakgrunn, og en mer praktisk innfallsvinkel i bevisstgjøringen kan derfor være å foretrekke. Visse bedrifter har for eksempel leid inn selskaper for å drive såkalt social engineering [3] mot de ansatte. I etterkant blir de ansatte presentert for en anonymisert og aggregert statistikk av resultatene. Slike aktive tiltak som involverer de ansatte har en bedre effekt på bevisstgjøring enn for eksempel et foredrag.

Et annet viktig moment ved bevisstgjøring er at man begrenser budskapet til et minimum og tilpasser det mottageren. NorSIS sin veiledning om hvordan å sikre seg når man kobler seg opp mot internett er kortfattet og konsis: bruk brannmur, automatisk oppdatering og antivirus, og ikke glem å ta sikkerhetskopi [49]. Avslutningsvis minnes leseren på å være bevisst på andre trusler slik som sosial manipulering. For en bedrift kan selvsagt repertoaret av sikkerhetstiltak være langt større, men for privatpersoner er dette en kortfattet og effektiv måte for å sikre seg mot de aller fleste uønskede hendelser.

En arbeidsgruppe i KIS foretok en revidering av nåværende strategi i [31]. I denne rapporten ble det pekt på flere faktorer som kan forbedres, og i det følgende sammenfattes det som kan sies å være den mest aktuelle kritikken.

Strategien har ikke en klar kobling mellom målsetninger og tiltak. Dette er uheldig siden det vanskeliggjør arbeidet med å måle hvor langt man er kommet med å nå målsetningene. Tiltakene er heller ikke satt i en prioritert rekkefølge, noe som gjør det vanskelig for de ansvarlige instansene å skille mellom viktigheten av de forskjellige tiltakene. Det gjør også at man på departementnivå ikke vet for hvilke tiltak det bør investeres flest midler.

Arbeidsgruppen påpekte mangel på strategiens synlighet på regjeringsnivå og i næringslivet. Regjeringsskifte nevnes som en grunn til dette. Samtidig sies det at departementene og de berørte deler i offentlig sektor har beholdt fokus på strategien. Næringslivets oppfølging av strategien karakteriseres som laber, og det nevnes at det er få eller ingen midler myndighetene har for å pålegge næringslivet å følge opp tiltakene.

Selv om offentlig sektor ifølge denne evalueringen har hatt større fokus på strategien enn næringslivet, tyder ting på at sikkerhetsarbeidet er kommet lenger i næringslivet enn i offentlig sektor. En undersøkelse gjort av Gartner viser at IT-budsjettet i snitt utgjør 2,5% av omsetningen for bedrifter. Dette tallet varierer fra bransje til bransje, men i finansnæringen utgjør IT-budsjettet minst 12,5% av omsetningen [50]. Det er ikke tvil om at denne næringen bruker betydelige deler av dette på informasjonssikkerhet. Når man er ansvarlig for infrastruktur for betalingsformidling og 93% av alle transaksjoner foregår elektronisk [51], må det investeres midler i god sikkerhet. Kundene slippes gjennom nettbanker stadig lenger inn i bankenes systemer, og for å kunne tillate dette må man ha tilstrekkelig sikring mot misbruk. Finansnæringen er særdeles utsatt for økonomisk motivert datakriminalitet og møter blant annet også trusler fra organisert kriminalitet. Kredittilsynet utfører årlig en ROS-analyse som legges til grunn for arbeid med å bedre sikkerheten i bransjen.

I [52] er det utført en spørreundersøkelse om informasjonssikkerhet i privat og offentlig sektor. Datagrunnlaget er i minste laget siden kun 20 organisasjoner svarte på spørreun-

[3] Social engineering innebærer å manipulere mennesker til å utføre visse handlinger eller avsløre konfidensiell informasjon.

dersøkelsen (11 offentlige og 9 private), og avvik i forhold til et større representativt utvalg må derfor medberegnes.

Undersøkelsen viste følgende: 50% av hele utvalget fulgte en internasjonal standard for informasjonssikkerhet. 80% i offentlig sektor fulgte en slik standard, mens tallet var i underkant av 90% i privat sektor. Kun 80% av hele utvalget hadde rutiner for rapportering av sikkerhetshendelser: nesten 90% av utvalget i privat sektor hadde slike rutiner, mens tallet var offentlig sektor var litt over 70%. Omtrent det samme forholdet ble funnet da organisasjonene ble spurt om de hadde definert begrepet sikkerhetshendelse. Forholdet bikket enda mer i favør av privat sektor da man spurte om det forelå en klar ansvarsmyndighet å rapportere sikkerhetshendelser til: 70% av alle organisasjonene hadde en slik myndighet, og av bedriftene i privat sektor var tallet nesten 90%, mens tallet i offentlig sektor var på rundt 55%. Også når det kom til praktisk håndtering av sikkerhetshendelser kom offentlig sektor gjennomgående dårligere ut en privat sektor. Det ble avdekket at 75% av hele utvalget hadde opplæring i hva man burde gjøre hvis man oppdaget en sikkerhetshendelse. Her rapporterte ca. 55% i utvalget av offentlige sektor at de ansatte hadde slik opplæring, mens tallet for privat sektor var 100%.

NorSIS som er i kontakt med kommuner angående styrking av informasjonssikkerhet bekrefter at man i flere steder ikke har kommet særlig langt i arbeidet med informasjonssikkerhet [9]. Det kan virke som om majoriteten av virksomheten i offentlig sektor, eksempelvis kommunesektoren, ikke har vært flinke med å iverksette og følge opp tiltak for å bedre informasjonssikkerheten til tross for at det har vært utført flere tiltak på høyere nivå i offentlig sektor. Her har NorSIS og myndighetene en krevende oppgave foran seg med å sørge for at virksomhetene bevisstgjøres på området. Til syvende og sist er det likevel virksomhetenes eget ansvar å iverksette nødvendige tiltak slik som ROS-analyse. Det man kan bidra med fra høyere hold i departementene er stort sett regulering gjennom regelverk samt å gjennomføre tiltak for å bevisstgjøre virksomhetene (hvilket NorSIS er et eksempel på).

I riksrevisjonens rapport kvitteres det for gjennomføring av tiltak i Nasjonal strategi for informasjonssikkerhet, men heller ikke riksrevisjonen har undersøkt graden av måloppnåelse for de ulike målsetningene. Dette er et arbeid som helt klart bør gis høy prioritet. Man kan ikke fortsette å investere midler i sikkerhetstiltak dersom det viser seg at de har ingen eller svært lav effekt. Kost-nytte vurderinger nevnes i strategien, men bare med fokus mot bedrifter. I videreføringen av strategien bør det arbeides for at det, i den grad det er mulig, utføres konkrete kost-nytte vurderinger for å påvise at tiltakene faktisk gir nevneverdige resultater. Tiltak bør utarbeides på bakgrunn av risiko, kostnad og forventet effekt knyttet til de. I virkeligheten har man i stedet fokusert primært på ROS-analyser. Slike analyser involverer ofte kostnad og effekt som en del av grunnlaget for prioriteringen, men det avgjørende momentet for prioriteringen er som regel risikoen.

Arbeidsgruppen i KIS foreslo i sin rapport at det for kommende strategier blant annet legges økende vekt på forskning (etter IKT SoS foreligger det ingen planer), internasjonal tilnærming og samarbeid med privat sektor (samarbeidsformer og finansiering). Videre anbefales det å rette blikket mot fremtidige utfordringer, innføre tiltaksområder isteden for tiltak, øremerke midler for implementering av tiltakene og muligens ha ett ansvarlig departement for oppfølging av strategien. Til slutt nevnes det at Riksrevisjonens og Infrastrukturutvalgets rapport (NOU 2006: 6) bør tas hensyn til i utformingen av revidert

strategi [31].

Dette er i all hovedsak fornuftige endringer, men poenget med å utarbeide tiltaksområder istedenfor tiltak er ikke tydelig beskrevet og det er derfor noe usikkert hva som er hensikten med dette. Det er vanskelig å se hvordan dette konkret skal bidra til å bedre den nye strategien eller såkalte retningslinjer for informasjonssikkerhet. Et moment er at ansvaret for implementering av tiltak sannsynligvis vil flyttes ned til laveste utøvende myndighet dersom strategien kun skal angi overordnede retningslinjer og tiltaksområder. De som er endelig ansvarlige for å utføre tiltakene vil muligens stå noe mer fritt til selv å velge hva som bør prioriteres underveis i strategiperioden. På en annen side er det en fare for at generelle tiltaksområder vil medføre en mindre konkret plan og dermed mindre grad av måloppnåelse. Det er uvisst hva en endring fra tiltak til tiltaksområder vil gjøre med hensyn på ansvarslinjene mellom de ansvarlige aktørene.

4.1.3 Konklusjon

Den nasjonale strategien inneholder 12 hovedtiltak for å bedre informasjonssikkerheten i samfunnet. Strategien er viktig for å rette et permanent søkelys mot informasjonssikkerhet, men synligheten av den har vært dårlig i den nåværende regjeringen og næringslivet, mens den har hatt et større fokus i offentlig sektor. KIS har en svært viktig jobb med å følge opp tiltakene i strategien, og oppfølgingen er dokumentert i [25] og [31].

Det har foregått mange aktiviteter i offentlig sektor forbundet med strategitiltakene i perioden 2003–2007, men det er verdt å bemerke at flere tiltak, eksempelvis NorSIS og NorCERT, var planlagt før strategien ble utarbeidet for deretter på et senere tidspunkt bli innlemmet som en del av strategien da denne kom på bordet. Strategien har sterkt bidratt til å innordne tiltakene i en helhetlig nasjonal satsing på informasjonssikkerhet.

I en arbeidsgruppe nedsatt av KIS ble strategien kritisert for blant annet å ikke koble tiltak til målsetninger og ikke øremerke midler til tiltak i departementene. Det er heller ikke foretatt en direkte kost-nytte vurdering av tiltakene. ROS-analyser har fungert som mindre nøyaktige, indirekte kost-nytte vurderinger. Det er ikke foretatt en evaluering av måloppnåelse for de forskjellige målsetningene, ei heller i Riksrevisjonens gjennomgang av arbeidet.

Hvis ny strategi eller nye retningslinjer publiseres som forventet i september 2007 vil den nåværende strategien hatt gyldighet i over 4 år, mer enn 1 år lenger enn det som ble anbefalt ved utarbeidelsen. Den nye strategien bør liste tiltakene i prioritert rekkefølge og ha et økt fokus samarbeid med privat sektor. Ny strategi bør ifølge [31] fokusere på tiltaksområder og ikke konkrete tiltak, noe som er vanskelig å forstå hensikten med.

Det anbefales videre at følgende tiltak får høyere prioritet enn de andre: beskytte kritisk IT-infrastruktur, koordinere arbeidet med IT-sikkerhet, gjennomføre risiko- og sårbarhetsanalyser og bevisstgjøre alle aktører. Til slutt anbefales det også at den nye strategien tar hensyn til rapportene fra Riksrevisjonen og Infrastrukturutvalget.

4.2 Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur

4.2.1 Oppsummering

Riksrevisjonens rapport, dokument nr. 3:4 (2005–2006), ble lagt frem 22.11.2005 og gjennomgår myndighetens arbeid med å sikre IT-infrastruktur. Grunnlaget for innholdet er dannet gjennom intervjuer og utførelse av en spørreundersøkelse i statsforvaltningen, deriblant departementer, underliggende virksomheter og bransjeorganisasjoner som berøres av Nasjonal strategi for informasjonssikkerhet. Det har også foregått korrespondanse mellom Riksrevisjonen og departementene i den hensikt å gi departementene en mulighet til å svare på kritikken. Undersøkelsen omfatter evaluering av tiltak for telesektoren samt tiltak for IT-sikkerhet.

Revisjonen har gransket og vurdert følgende områder rundt prosessen med å sikre IT-infrastruktur [26, kap. 1]:

1. Organiseringen av myndighetenes arbeid
2. Plan- og gjennomføringsprosessene
3. Tiltakene som er iverksatt på området

Kapittel 3 i rapporten beskriver disse områdene mer utdypende og spesifiserer hvert enkelt revisjonskriterium i detalj [26]:

1. Organisering og planlegging av arbeidet med IT-sikkerhet
2. Prinsipper for organisering
3. Avklaringer av ansvars- og samarbeidsforhold
4. Planlegging og gjennomføring
5. Beskyttelse av kritisk IT-infrastruktur
6. Avgrensning av hva som krever særlig beskyttelse
7. Reduksjon av sårbarhet
8. Systemer og rutiner for å fange opp trusler
9. Håndtering av sikkerhetshendelser
10. Sikkerhetskultur
11. Offentlig sektor som drivkraft
12. Bevisstgjøring og kompetanseheving
13. Internasjonale standarder og veiledning
14. Telesikkerhet og -beredskap
15. Delegering av oppgaver
16. Tiltak for økt telesikkerhet og -beredskap
17. Virkemidler

18. Samferdselsdepartementets oppfølging

Alle punktene over ble undersøkt av Riksrevisjonen. Tre overordnede områder i den nasjonale satsingen ble viet spesielt mye oppmerksomhet i revisjonen. Disse områdene var:

- Organiseringen av forvaltningens arbeid med IT-sikkerhet
- Sikring av samfunnskritisk IT-infrastruktur
- Tilrettelegging for utvikling av god sikkerhetskultur

Riksrevisjonen la særlig vekt på at organiseringen av arbeidet hadde store mangler. Den største av manglene gjaldt manglende ansvarsavklaring mellom departementene i implementeringen og oppfølgingen av tiltak. Man fant også at det var manglende avklaring mellom fagorganer i det offentlige og bransjeorganisasjoner i næringslivet. Bransjeorganisasjonene mente det var vanskelig å finne ut hvilket IT-organ i det offentlige som hadde ansvar for hvilke forhold innen IT-sikkerhet.

Vedrørende satsingen rundt samfunnskritisk IT-infrastruktur fant Riksrevisjonen at det ikke forelå en felles definisjon for begrepet samfunnskritisk IT-infrastruktur og at slik infrastruktur ikke var identifisert og kartlagt. Det ble nevnt at det var igangsatt visse arbeider for å definere hva kritisk IT-infrastruktur er, men at disse ikke var ferdigstilt og at det ikke forelå noen oversikt over denne infrastrukturen. Rapporten påpeker at identifisering og kartlegging av kritisk IT-infrastruktur er en grunnleggende forutsetning for gjennomføring av ROS-analyser.

I tilknytning til samfunnskritisk IT-infrastruktur, fremhevet revisjonen også at det tok vel 2 år før et forskningsprosjekt [4] på sårbarhet og IKT-infrastruktur ble igangsatt fra det først ble omtalt i forslaget til statsbudsjett høsten 2002. Dette til tross for at Innst. S. nr. 9 (2002–2003) understreker viktigheten av robust infrastruktur i alle samfunnsviktige institusjoner, og at Nasjonal strategi for informasjonssikkerhet hadde beskyttelse av kritisk infrastruktur som ett av fire hovedmål. Riksrevisjonen var heller ikke fornøyd med pilotprosjektet Senter for informasjonssikring da senteret hadde et annet mandat enn det NorSIS har i dag. Mandatet til SIS under pilotprosjektet involverte systemer for å fange opp trusler, et område som i dag omfattes av NorCERT sitt mandat. Den siste kritikken under punktet samfunnskritisk IT-infrastruktur omhandlet manglende hendelseshåndtering og beredskapsplaner både på departementnivå og i andre virksomheter, private såvel som offentlige.

Vedrørende tilrettelegging for utvikling av god sikkerhetskultur mente Riksrevisjonen at det var iverksatt eller gjennomført få tiltak på området. Undersøkelsen viste også at privat sektor ikke anså offentlig sektor som en drivkraft og et eksempel til etterfølgelse i dette arbeidet.

4.2.2 Diskusjon

Som nevnt i oppsummeringen har Riksrevisjonen vurdert organiseringen av myndighetenes arbeid, plan- og gjennomføringsprosessene samt implementerte tiltak. Revisjonen av myndighetenens satsing og oppfølging på informasjonssikkerhet kan karakteriseres som

[4] Prosjektet, Beskyttelse av samfunn 5, er nå nylig avsluttet ved FFI.

gjennomgående svært kritisk og lite positiv. Rapporten er delt inn i et sett faktakapitler og et kapittel for vurdering av satsingen, hvilket gir et presist bilde av de faktiske forhold i tillegg til at man får innblikk i Riksrevisjonens skjønnsmessige vurdering av arbeidet.

I følgende delkapitler diskuteres de områdene som Riksrevisjonen spesielt konsentrerte seg om:

- Organiseringen av forvaltningens arbeid med IT-sikkerhet
- Sikring av samfunnskritisk IT-infrastruktur
- Tilrettelegging for utvikling av god sikkerhetskultur

Organiseringen av myndighetenes arbeid

FAD er departementet som skal ta seg av sektorovergripende spørsmål og er også ansvarlig for å initiere og koordinere tverrsektorielle tiltak. FAD fikk ansvaret for sektorovergripende spørsmål ved opprettelsen av departementet, noe som skjedde i 2004 grunnet endringer i departementstrukturen. I St.meld. nr. 17 (2006–2007) presiseres det at FAD skal ha ansvar for å initiere og følge opp alle *forebyggende*, tverrsektorielle tiltak og ikke alle tverrsektorielle tiltak generelt.

Før FAD hadde NHD ansvaret for å koordinere arbeid med IT-sikkerhet i næringslivet. I tillegg var det, før FAD tok over, NHD sitt ansvar å følge opp tiltakene i Nasjonal strategi for informasjonssikkerhet samt lede KIS. Å lede KIS har siden 2004 vært FAD sitt ansvar. KIS har et koordineringsansvar for arbeidet med informasjonssikkerhet i den nasjonale strategien. Rådet har ingen myndighet til å fatte vedtak, men er kun en møteplass for de ulike departementene. KIS ble opprettet i mai 2004 som følge av et tiltak i den nasjonale strategien. NorSIS og Datatilsynet er andre virksomheter underlagt FAD [26, kap. 4.1.1].

Justis- og politidepartementet har i oppgave å samordne og føre tilsyn med samfunnets sivile sikkerhet, herunder beredskap for kritisk infrastruktur. DSB, som blant annet har ansvar for utarbeidelse og vedlikehold av nasjonale beredskapsplaner, er underlagt JD. DSB har ifølge JD ikke fagansvar for informasjonssikkerhet, men jobber allikevel med å inkludere det i beredskapsarbeidet sitt. NSM, Politiets sikkerhetstjeneste (PST) og Politiets datakrimsenter (PDS) er også underlagt JD [26, kap. 4.1.2].

Forsvarsdepartementet er ansvarlig for forvaltning av Sikkerhetsloven, hvilket skjer gjennom direktoratet NSM. NSM rapporterer til FD for saker i militær sektor og til JD for saker i sivil sektor. NorCERT og VDI er underlagt NSM [26, kap. 4.1.3].

Samferdselsdepartementet har et sektoransvar for telesikkerhet og -beredskap. Departementet står også som ansvarlig forvalter av ekomloven. SD har et ansvar for alle tilbydere av elektroniske kommunikasjonsnett og -tjenester, herunder infrastruktur og andre installasjoner. Post- og teletilsynet er et forvaltningsorgan underlagt SD. PT har siden 2001 hatt et særskilt ansvar for telesikkerhet og -beredskap [26, kap. 4.1.4].

Både SIS, PT og DSB vurderte ansvarsfordelingen mellom departementene og fagorganene som uklar. SIS kommenterte at begrensede ressurser ble brukt til overlappende oppgaver. Bransjeorganisasjonene Abelia, IKT-Norge og NSR var heller ikke fornøyd med ansvarsfordelingen. Abelia påpekte at det spesielt var vanskelig å finne ut hvilke organer som er rene informasjonstiltak, og hvilke som er tilsynsorganer som kan fatte vedtak og/eller håndheve lovverk. Datatilsynet mente også at ansvarsfordelingen var uklar, men

at problemet vanskelig kan løses fullt ut [26, kap. 4.2.1]. Riksrevisjonen mente at det var behov for avklaringer vedrørende ansvaret for kritisk infrastruktur, ansvaret for Internett og kontakten med næringslivet.

NSM hadde et annet synspunkt enn de andre etatene og mente at selv om arbeidsdelingen og ansvarsforholdene umiddelbart kan synes uklare, skyldes dette kompleksiteten som må til for å ivareta mange ulike hensyn, deriblant "etablering og videreutvikling av en rekke forskjellige regelverk som også vil ha betydning for private aktører, tilsyn med etterlevelse av regelverkene, tilrettelegging for næringslivet, akademia og befolkningen generelt" [26, kap. 4.2.1]. NSM ønsket på en annen side en tydeliggjøring av omfanget av FAD sitt ansvar med IT-sikkerhetsarbeid i samfunnet [26, kap. 4.2.1].

Det kan forsvares at utydelig ansvarsfordeling kan skyldes et komplekst regelverk som man må ha for å ivareta mange ulike hensyn. Ideelt sett bør man streve for å etterleve regelverkene selv om de er komplekse, sålenge de ulike regelverkene er nødvendige for å ivareta flere hensyn. De ulike regelverkene bør da være presist formulert og ikke være overlappende, noe de fleste aktørene mente ikke var tilfelle. Et annet viktig moment vedrørende tydeliggjøring av ansvarsfordeling er etterlevelse av regelverk. Dersom regelverkene blir for mange og utydelige, vil de færreste aktørene ha mulighet og kapasitet til å orientere seg om forholdene. Man bør derfor ta høyde for en viss pragmatisme i utformingen av regelverkene slik at man veier kompleksiteten og mangfoldet av reguleringer opp mot etterlevelse av de samme reguleringene. Det kan argumenteres for at et konsolidert og noe forenklet regelverk vil gi en større effekt enn et spredt og komplekst regelverk, ved at førstnevnte i større grad blir fulgt opp av de berørte institusjonene. Datatilsynet påpekte at en tydeliggjøring av ansvarsfordeling bør omfatte et enhetlig regelverk, slik at ikke de enkelte etater utvikler sine egne regelverk på en måte de selv finner hensiktsmessig [26, kap. 4.2.4].

Samarbeidsgruppe for regelverk for informasjonssikkerhet (SARI) i KIS jobber per idag med å samordne regelverket for informasjonssikkerhet på bakgrunn av tiltak nummer to i Nasjonal strategi for informasjonssikkerhet. Flere rapporter, deriblant en rapport fra Statskonsult i 2006, "Arbeid med informasjonssikkerhet – fra juss til styring og rutiner", hevder at regelverk vedrørende informasjonssikkerhet ikke har store overlapp, og at fokus derfor bør flyttes fra samordning av regelverk til etterlevelse av regelverk [31]. Dette er ikke i samsvar med uttalelsene fra aktørene som ble intervjuet av Riksrevisjonen, og det kan derfor virke som det er forskjell på teori og praksis på dette området.

Majoriteten av de spurte etatene og organisasjonene mente altså at ansvarsfordelingen og arbeidsfordelingen var for dårlig avklart. Utydelig ansvarsfordeling medførte ifølge SIS at begrensede ressurser brukes på overlappende oppgaver. PT mente at en fragmentert ansvarsfordeling ikke bare er uhensiktsmessig, men at den også leder til en svekkelse av sikkerhetstilstanden. Tilsynet ønsket seg spesielt en avklaring av ansvaret for Internett, et område som PT ifølge ekomloven er ansvarlig for, men som andre aktører også har blandet seg inn i. PT, DSB og NSM pekte alle på problemet med å få finansiert tverrsektorielle tiltak som følge av uklar ansvarsfordeling, en type tiltak som allerede er krevende å gjennomføre fra før av [26, kap. 4.2.1].

Som man forstår hadde majoriteten av aktørene store betenkeligheter med den utydelige ansvarsfordelingen. Dette kommer også til syne i KIS sin vurdering av strategien og dens organisering, hvor det nevnes at ansvaret sannsynligvis ikke ble godt nok forankret i de departementer som har informasjonssikkerhet som hovedanliggende, men at disse

departementene likevel ble gitt gjennomføringsansvar av tiltak [31]. I denne vurderingen anbefales det også å presisere gjennomføringsansvar i strategien, samt vurdere om kun ett departement bør ha et slikt ansvar.

KIS er en møteplass for de ulike departementene vedrørende informasjonssikkerhet, men er kun en rådgivende myndighet. Det er derfor ønskelig å legge et samlet og overordnet ansvar hos ett enkelt departement for oppfølging av strategien, slik at man unngår dagens situasjon med en distribuert ansvarsfordeling uten en sentral myndighet som styrer det hele. Det virker naturlig at FAD kan påta seg denne sentrale rollen siden departementet allerede i dag har en meget fremtredende rolle på området. Forhåpentligvis vil en slik sentral myndighet gi en tydeligere ansvarsfordeling og færre spørsmål ved implementering av tverrsektorielle tiltak.

Sikring av samfunnskritisk IT-infrastruktur

Et av regjeringens fire overordnede mål i den nasjonale strategien er følgende (jf. kapittel 4.1):

> *"Samfunnskritisk infrastruktur for elektronisk informasjonsutveksling skal være robust og sikker i forhold til de trusler den utsettes for. Kritiske informasjonssystemer skal være sikret slik at skadevirkningene ved sikkerhetsbrudd ikke er større enn hva som kan defineres som akseptabel risiko."*

Ansvaret for kritisk infrastruktur følger samme ansvarsfordeling som for all annen infrastruktur, hvilket betyr at de enkelte departementene og sektorene er ansvarlige for sikkerhet- og beredskapsarbeid innenfor egne myndighetsområder. JD har allikevel en særstilling for å ivareta en helhetlig samordning på tvers av departementene. Per idag har departementet ansvaret for de fleste oppgavene som Sårbarhetsutvalget mente burde være samlet under ett departement, deriblant Politidirektoratet, PST, DSB, NSM (sivil sektor) og fylkesmennenes beredskapsarbeid [18, kap. 5.2].

NSM og DSB har også fremtredende roller i sikkerhet- og beredskapsarbeidet, herunder arbeid opp mot kritisk infrastruktur. Ifølge Riksrevisjonens undersøkelse hadde verken NSM og DSB en entydig oversikt over den infrastruktur og de installasjoner som omfattes av begrepet kritisk infrastruktur. Direktoratene henviste til at BAS5 prosjektet og til en viss grad Infrastrukturutvalget var forventet å gi ytterligere informasjon om dette.

BAS5 prosjektet er nå formelt avsluttet og har, i tillegg til å utvikle metodikk på tre forskjellige områder, utført fire case analyser innen fire ulike sektorer. Analysene ble foretatt ved et stort sykehus og ved et stort finansforetak samt for to store aktør innen henholdsvis kraftforsyningen og petroleumsbransjen [13, kap. 5.4]. I BAS5 prosjektet ble det også utviklet en veileder for risikoanalyse av IKT-systemer. Det bør nevnes at det allerede finnes en rekke metoder for ROS-analyse, og at BAS5 har fokusert på metodikk med særlig anvendelse på sektornivå eller på tvers av sektorene, selv om metodikken kan brukes også innad i andre virksomheter. Ifølge Riksrevisjonens rapport var det ikke klarlagt hvordan metodikken skulle benyttes videre av sentrale myndigheter. JD uttalte følgende: "... man legger opp til at den enkelte sektor må følge opp resultatene av BAS-5-prosjektet innenfor sitt ansvarsområde" [26, kap. 5.1.2].

Infrastrukturutvalgets rapport drøfter i kapittel 10 "Kartlegging av kritiske infrastrukturer og sektorvise anbefalinger", herunder elektronisk kommunikasjon. Utvalget beskriver

de grunnleggende elementene i IKT-infrastrukturen: aksessnett, transportnettet, tjenestenett og drifts- og støttesystemer. Det gis ingen ingen oversikt av kritisk infrastruktur på lavere nivå. Utvalget nøyer seg med å påpeke at transportnettet som er eid av Telenor utvilsomt utgjør en del av den kritisk IKT-infrastrukturen. Kapittel 10 drøfter i hovedsak virkemidler knyttet til sikring av kritisk infrastruktur. Utvalget drøfter blant annet statlig eierskap, reguleringer (ekomloven) og nasjonal autonomi som virkemidler. Organiseringen av IT-sikkerhetsarbeidet blir også nevnt, og i den sammenheng etterlyses det klarere ansvarsfordeling på departementnivå.

Utvalget konkluderer slik [18, kap. 10.1.4]: "Utvalget mener kjøp av tjenester og tilskudd til spesielle oppgaver for sikring av kritisk infrastruktur vil være et nødvendig virkemiddel sammen med regulatoriske bestemmelser. Det vises i denne sammenheng også til utvalgets forslag om en tilskuddsordning, jf. kapittel 6.6.3."

Utifra BAS5 prosjektet og Infrastrukturutvalgets rapporter kan man ikke konkludere med at kritisk IKT-infrastruktur er blitt identifisert og fullstendig kartlagt i de ulike sektorene. Det er nå opp til departementene og de underlagte virksomhetene å gjennomføre ROS-analyser, ved hjelp av blant annet metodikkene utviklet i BAS5 prosjektet, slik at en entydig oversikt over kritisk IKT-infrastruktur på sektornivå kan fremstilles. Oversikten er viktig slik at tiltak og midler kan brukes for å redusere sårbarheten der den er størst.

JD mener at en tverrsektoriell oversikt ikke nødvendigvis må utarbeides, siden "hver enkelt sektor anses å ha relativt god oversikt over hvor 'kritiske' IT-systemene systemene innen deres sektor er" [26, kap. 5.1.1]. Departementet påpeker at begrepet samfunnskritisk infrastruktur ikke er godt nok definert, men mener likevel at forebyggende tiltak vil bli gjennomført av den enkelte sektor. Dersom hver enkelt sektor ikke har utarbeidet gode nok ROS-analyser, vil dette kunne få konsekvenser blant annet av økonomisk art. NSM uttalte til Riksrevisjonen at "mangelfull oversikt gir en risiko for at den sikkerhetsmessige innsatsen og dermed ressursbruken rettes mot feil beskyttelsesmål" [26, kap. 5.1.1]. Det hjelper lite å iverksette tiltak hvis det gjøres på feil steder.

Man kan argumentere for at definisjon og beskyttelse av kritisk infrastruktur bør anses som et sektorovergripende anliggende idet man absolutt bør ivareta en konsistent sikring på tvers av sektorene. Man kan ikke kan tillate at enkelte sektorer har dårligere sikring av kritisk infrastruktur enn andre selv om majoriteten av sektorene skulle ha gjennomført tilfredsstillende sikring. Infrastrukturer må gis lik sikring dersom de er like kritiske, uavhengig i hvilken sektor det er snakk om. Som Riksrevisjonen og KIS har påpekt, har manglende ansvarsfordeling vært et gjennomgående problem i oppfølgingen av Nasjonal strategi for informasjonssikkerhet. Å legge det overordnede ansvaret til ett departement ville derfor være et tiltak som kan bidra til å sikre bedre oppfølging. Hvis departementet med dette ansvaret skal være i stand til å prioritere på tvers av sektorer, vil dette ikke kunne gjøres uten en overordnet oversikt på nasjonalt nivå. Et annet positivt moment med en nasjonal oversikt over kritisk infrastruktur er at den muligens vil kunne forenkle sikkerhet- og beredskapsarbeid samt kriseledelse på nasjonalt nivå.

Tiltak for å redusere sårbarheten i IT-infrastrukturen

Riksrevisjonens rapport peker på flere tiltak har vært planlagt for å redusere sårbarheten i IT-infrastrukturen:

- BAS5 prosjektet
- Utarbeidelse av sektorvise normer for informasjonssikkerhet
- Systemer for å fange opp trusler mot IT-infrastrukturen
- Systemer for håndtering av sikkerhetshendelser

BAS5 prosjektet — BAS5 prosjektet ble formelt avsluttet i 2007. Et slikt prosjekt om IKT-infrastrukturer og sårbarhet i samfunnet ble først omtalt i St.prp. nr. 1 (2002–2003). Prosjektet var fra begynnelsen ment å være et spleiselag, og JD sendte ut forespørsler til departementer og etater for å spørre etter midler. NSM og DSB fikk etterhvert i oppdrag av JD å prøve å skaffe midler for gjennomføringen av prosjektet. JD uttalte på et senere tidspunkt at det var vanskelig å få inn de nødvendige midlene, og at oppstarten til prosjektet ble forsinket på grunn av dette. I 2004 ble det søkt om støtte fra Norges forskningsråd og deres forskningsprogram om informasjonssikkerhet IKT SoS. Prosjektet ble innvilget ca. 5 mill. kr. fra NFR som dermed finansierte nesten halvparten av prosjektet [26, kap. 5.1.2]. Man kan stille spørsmål ved om man i hele tatt ville klart å samle inn nok midler til prosjektet, og ihvertfall prosjektets planlagte omfang, dersom IKT SoS ikke hadde vært opprettet i forkant av BAS5 prosjektet.

JD kommenterte at det ikke forelå noen planer for å koordinere de enkelte sektorenes ROS-analyser, siden departementet anså en slik aggregering for å ha begrenset verdi. JD mente at en samlet oversikt over ROS-analysene ikke ville bli brukt til daglig i og med at hver enkelt sektor har ansvaret for gjennomføringen av tiltakene. Departementet mente videre at hver enkelt sektor må følge opp resultatene av BAS5 prosjektet innenfor eget ansvarsområde, selv om departementet tidligere uttalte at de enkelte sektorene hadde en relativt god oversikt over egne kritiske infrastrukturer.

Det er et poeng at man ikke bør sammenstille de enkelte sektorenes ROS-analyser dersom de ikke vil bli brukt. En slik sammenstilling kan allikevel være nyttig i krisesituasjoner av nasjonalt omfang. Den kan også være nyttig dersom ansvaret for Nasjonal strategi for informasjonssikkerhet skal underlegges ett departement og det skal foretas tverrsektorielle prioriteringer. Finansdepartementet uttalte i forbindelse med den nasjonale strategien at finansiering av tiltak skal forekomme over de til enhver tid fastsatte rammene for departementens budsjetter. Hvis midler ikke blir øremerket av et eventuelt hovedansvarlig departement, vil tverrsektorielle prioriteringer ikke være et tema i det hele tatt, hvilket kan tale i favør av JD sitt utsagn om ikke å utarbeide en tverrsektoriell oversikt over ROS-analyser.

Utarbeidelse av sektorvise normer for informasjonssikkerhet — Ifølge Nasjonal strategi for informasjonssikkerhet skal de enkelte sektorene utarbeide normer for sikring med hensyn til konfidensialitet, integritet og tilgjengelighet. Da Riksrevisjonen avla sin rapport ble det kommentert at KIS per 12.11.2004 ikke hadde planlagt eller gjennomført tiltak på området, og at slike tiltak heller ikke var med i departementenes handlingsplaner [26, kap. 5.1.2]. Riksrevisjonen avla sin rapport 22.11.2005. I en rapport fra KIS datert 09.03.2007 kvitteres det for utførte tiltak [25]. Her kommenteres det at FAD har gitt Statskonsult i oppdrag å gjennomføre tiltak vedrørende generelle offentlige IT-sikkerhetsnormer, og at det er blitt utarbeidet eksempler på modeller tilgjengelige fra nettstedet kunnskapsnettverk.no. Ifølge nettstedet ble det publisert en lenke til prosessmodeller med regelverkshenvisninger

21.12.2006.

På nettstedet finnes resultatene av prosjektet. Det er produsert en generell saksbehandlingsmodell og to konkrete eksempler. Nytteverdien virker noe begrenset i og med at det finnes bare to eksempler. Det er også tidlig å si om modellen i det hele tatt er blitt tatt i bruk i offentlig sektor. I [25] kommenteres det at Statskonsult skal "formidle informasjon om modellen til aktuelle miljøer og stimulere til interaktivitet om temaet på nettsiden", hvilket forhåpentligvis vil resultere flere eksempler og økt nytteverdi for brukerne.

I 2006 ble det lansert felles IT-sikkerhetsnormer for helsesektoren. Oljeindustriens landsforening (OLF) har utarbeidet lignende retningslinjer for informasjonssikkerhet. Utviklingen av generelle offentlige IT-sikkerhetsnormer har FAD gitt i oppdrag til Statskonsult frem til nå har laget en prosessbeskrivelse for generell saksbehandling på kunnskapsnettverk.no.

Systemer for å fange opp trusler mot IT-infrastrukturen — Riksrevisjonen vurderte under dette punktet gjennomføringen av oppgavene som var pålagt VDI og SIS.

VDI er et system for å fange opp eksterne trusler rettet mot tilkoblede virksomheter. Systemet har fokus på å avdekke koordinerte angrep av nasjonal betydning. Interne trusler kan ikke kartlegges av systemet da de tilkoblede virksomhetenes utgående trafikk ikke analyseres.

Kun 10–15 større virksomheter var koblet til VDI ved oppstarten [26, kap. 5.1.2]. Riksrevisjonen mente antallet var begrenset og at systemet ga lite informasjon til allmennheten. Høsten 2000 ble VDI etablert som et prøveprosjekt, og under denne tiden ble svært lite eller ingen informasjon gjort tilgjengelig for allmennheten. VDI ble permanent etablert vinteren 2003. Fra desember 2003 ble månedsrapportene fra VDI gjort tilgjengelig for allmennheten fra nettsidene deres.

NSM pekte på at det begrensede antallet tilkoblede virksomheter var nødvendig for å opparbeide tillit og åpenhet mellom aktørene, noe som ville vært vanskelig med mange deltagere. Det ble også nevnt at man fryktet at man ville miste fokus med for mange deltagere. Tekniske begrensninger ble også nevnt som faktor til at utvidelser ikke har funnet sted, men NSM kommenterte videre at det ble jobbet med en forsiktig økning i antall tilkoblede virksomheter. Det har ikke vært mulig å vite hvor mange virksomheter som er koblet til VDI per dags dato da denne informasjonsen er konfidensiell, men det bekreftes at de tekniske begrensningene fortsatt er like aktuelle. Store volum med trafikkdata fra de tilkoblede virksomhetene begrenser effektivt antallet tilkoblinger VDI kan håndtere [53]. NorCERT/VDI prøver til enhver tid ha et så representativt utvalg av kritiske norske virksomheter som mulig, til tross for det begrensede antallet medlemmer. Et slikt representativt utvalg består blant annet av aktører fra kraftbransjen og Internettilbydere som leverer Internett til viktige samfunnsfunksjoner [53].

I tillegg til å fokusere på dataangrep fra Internett, arrangerer VDI et sikkerhetsforum 3–4 ganger årlig, hvor teknisk personell og strategisk ledelse samles fra de deltagende virksomhetene [26, kap. 5.1.3].

VDI skal kunne danne seg et representativt bilde av trusselen mot norske, kritiske virksomheter. Det er grunn til å spørre seg om et utvalg på 10–15 virksomheter virkelig kan være representativt på nasjonalt nivå. Det bør derfor foretas en vurdering om hva man kan gjøre for å overvinne de tekniske begrensningene og hvordan man eventuelt kan koble flere virksomheter til VDI. Et annet moment som bør vurderes er i hvor stor grad VDI

skal tilgjengeliggjøre informasjon fra systemet for allmennheten.

Senter for informasjonssikring (SIS) ble etablert som et prøveprosjekt i april 2002. To ganger ble prøveprosjektets periode forlenget, og senteret ble ikke permanent etablert før 01.01.2006. Senteret hadde som prøveprosjekt i oppgave å "framskaffe et helhetlig bilde av truslene mot norske IT-systemer basert på innrapportering av hendelser fra norske virksomheter" [26, kap. 5.1.3]. Det ble inngått avtale med 21 virksomheter om innrapportering av sikkerhetshendelser. I 2004 mottok senteret mindre enn 5 rapporter om sikkerhetshendelser, og Mørketallsundersøkelen for 2003 og samtaler mellom Riksrevisjonen og bransjeorganisasjonene IKT-Norge og Abelia viste videre at senteret var lite kjent i næringslivet. SIS konstaterte i sin årsrapport for 2004 at det var mangel på vilje i de norske virksomhetene til å rapportere hendelser. En del av den manglende viljen kan forklares med at det fantes lite incentiv for virksomhetene til å rapportere, idet de ikke fikk hjelp med å håndtere hendelsene. Meningen med innrapporteringen var å kartlegge trusler mot norske IT-systemer og deretter gjøre disse tilgjengelige for allmennheten, ikke fungere som et senter for hendelseshåndtering. For å øke incentiv til rapportering foreslo SIS derfor å knytte sin virksomhet tettere opp mot en CERT hvor man også kunne få hjelp til å håndtere hendelser [26, kap. 5.1.3].

Prosjekt NorCERT ble startet i februar 2004, og ble i april 2006 etablert som en permanent avdeling under NSM [20]. NorSIS har fått et annet mandat enn SIS hadde, og NorCERT har et ansvar med å yte hjelp til hendelseshåndtering av sikkerhetshendelser for alle virksomheter som er kritiske samfunnsfunksjoner og virksomheter med ansvar for kritisk infrastruktur. Mandatet til NorSIS er nå fokusert på bevisstgjøring rundt informasjonssikkerhet mot små og mellomstore bedrifter i offentlig såvel som privat sektor. NorCERT/VDI er ansvarlig for deteksjon og hendelseshåndtering av angrep. Med disse endringene i struktur og mandat ser det ut til at incentivet til innrapportering av hendelser har økt betraktelig.

Systemer for håndtering av sikkerhetshendelser — I Nasjonal strategi for informasjonssikkerhet vises det til at DSB skal utrede hvordan IT-sikkerhet kan integreres i beredskapsplanene. Da Riksrevisjonen publiserte sin rapport i 2005 var arbeidet med integreringen i sluttfasen. Dette arbeidet er per dags dato ennå ikke fullført hva angår planene på sentralt og regionalt nivå [54]. En rekke kommuner har kommet svært langt med å inkludere IKT i sine egne kriseplaner [54]. IKT-sikkerhet blir forøvrig inkludert som tema i alle DSB sine øvelser, og en større nasjonal øvelse er under planlegging med fokus på IKT-sikkerhet [54].

En undersøkelse i statlig sektor utført av Statistisk sentralbyrå i 2004 viste at kun 40% hadde en beredskapsplan på IT-området som var oppdatert de siste to årene. En lignende undersøkelse i 2003 viste at tallet var 41% i kommunesektoren. I privat sektor var tallet i 2004 på 16% for foretak med mindre enn 10 personer [26, kap. 4.1.4]. Det vites ikke hva tilsvarende tall er i privat sektor for større foretak, og det er derfor urimelig å sammenligne privat og offentlig sektor med ugangspunkt i disse tallene. En bør følgelig ikke trekke konklusjoner vedrørende beredskapsforholdet mellom privat og offentlig sektor på dette grunnlaget.

Datatilsynet sa seg enig i at det virker som både privat og offentlig sektor har en "lite planmessig tilnærming til informasjonssikkerhet" [26, kap. 4.1.4]. JD og FAD påpekte at det er den enkelte virksomhets ansvar å sørge for utarbeidelse og oppdatering av planer for gjenoppretting. FAD stilte også spørsmål ved hvorvidt departementets ansvar favner

med hensyn til utarbeidelse av beredskapsplaner for forvaltningen (inkludert kommunesektoren).

DSB har utarbeidet veiledninger i ROS-analyse og beredskapsplanlegging som kan tas i bruk av de enkelte virksomhetene for å stå bedre rustet i krisesituasjoner. Gjennomføring av kurs og øvelser blant virksomhetene ble også anbefalt av DSB for å bedre evnen til å takle krisesituasjoner [26, kap. 4.1.4].

DSB er ansvarlig for å initiere øvelser på departementnivå og i kommunesektoren. Øvelsene kan foregå i en enkelt sektor eller på tvers av sektorer. Det er DSB sin oppgave å lage scenarier for øvelsene med utgangspunkt i aktuelle trusselvurderinger. Noen av beredskapsøvelsene som har vært arrangert har inkludert svikt i sentral IT-infrastruktur. Disse øvelsene har i all hovedsak vært såkalte papirbaserte øvelser med ledere som målgruppe. DSB har uttalt at øvelsene ikke har vært tilstrekkelige for å identifisere nødvendige forebyggende tiltak. JD er enig i at de papirbaserte øvelsene ikke dekker alle nødvendige aspekter, men at det er vanskelig å gjennomføre realistiske øvelser med eksisterende IT-infrastruktur uten at det går på bekostning av sikkerheten [26, kap. 4.1.4]. Dette er godt poeng som bør vies mer oppmerksomhet i fremtidig beredskapsplanlegging. For å kunne gjennomføre realistiske øvelser er det viktig at man dekker operativ utførelse såvel som ledelse. Operativ utførelse kan kun skje dersom det finnes faktiske infrastrukturer som kan benyttes under øvelsen. Følgelig må man enten sørge for at man har alternative infrastrukturer i reserve som kan inngå i øvelsen (enten virtuelle eller fysiske), eller at øvelsen skjer i en periode hvor infrastrukturene brukes lite slik at eventuelle bortfall får mindre konsekvenser (for eksempel svært tidlig eller sent på dagen samt i helger eller ferier).

Riksrevisjonen omtalte også CERT og dens funksjon. Det ble kommentert at VDI har utført en oppgave som normalt ligger under en CERT. VDI har gitt advarsler ved angrep, men har ikke hatt i oppgave å svare på henvendelser og utføre gjenoppretting. Alle disse tre oppgavene blir som regel pålagt en CERT. Riksrevisjonen kommenterte at SIS hadde vært et kontaktpunkt og hatt ansvar for å behandle rapportering av hendelser, men at det ble bestemt at senteret ikke skulle ha noen CERT funksjon i prøveprosjektperioden som varte fram til utgangen av 2004 [26, kap. 5.1.4]. Rapporten omtaler NSM sitt arbeid for å opprette en nasjonal CERT. NorCERT ble startet som et prosjekt i februar 2004, og ble etablert som en permanent avdeling under NSM i april 2006 [20]. De oppgavene som hører til en nasjonal CERT funksjon slik som angrepsdeteksjon og hendelseshåndtering dekkes dermed av nåværende NorCERT/VDI.

Mørketallsundersøkelsen for 2003 viste at kun 9% av virksomhetene hadde en vaktordning for å håndtere brudd på IT-sikkerheten [26, kap. 5.1.4]. Det er lite som taler for at en vaktordning vil være økonomisk ulønnsom for virksomhetene, og det er derfor rart at ikke flere har en slik ordning. Vaktordningen vil for små og mellomstore bedrifter høyst sannsynlig begrense seg til at den vakthavende tar ansvar for eventuell gjenoppretting dersom det oppstår en hendelse. Det vil i de fleste tilfeller ikke være behov for å opprette en egen stilling for en slik vaktordning. Det kan derfor virke som at mangler innenfor sikkerhet- og beredskapsarbeid er årsaken til fraværet av en slik ordning, og ikke økonomiske forhold.

Tilrettelegging for utvikling av god sikkerhetskultur

Offentlig sektor som drivkraft for informasjonssikkerhet

Når det gjelder myndighetenens arbeid med å fremme en god sikkerhetskultur, fikk dette også mye negativ kritikk av Riksrevisjonen. Bransjeorganisasjonene i næringslivet, NSR, IKT-Norge og Abelia, var alle enige om at myndighetens arbeid på området var lite synlig i privat sektor. Organisasjonene mente også at sikkerhetskulturen i offentlig sektor ikke var et godt forbilde for privat sektor, og at privat sektor lå lenger framme i arbeidet med å fremme en god sikkerhetskultur [26, kap. 5.2.1]. Det er synd, men ikke overraskende at offentlig sektor har dårligere sikkerhetskultur enn privat sektor. Privat sektor er mer adaptiv og reagerer raskere når det oppstår behov for endringer enn offentlig sektor. I dette konkrete tilfellet kan det skyldes at næringslivet har innsett at dårlig sikkerhetskultur resulterer i betydelige økonomiske tap. Mørketallsundersøkelsen for 2003 anslo det samlede tapet for norske virksomheter til å være mer enn 5 milliarder kroner. Rundt 60% av de norske virksomhetene ble rammet av datakriminalitet eller andre uønskede hendelser. Undersøkelsen viste også at 70% av virksomhetene får ekstra arbeid på grunn av uønskede hendelser, og at bare 25% kunne anslå hvor mye de har tapt på grunn av uønskede hendelser. Kun 12% av virksomhetene hadde rutiner for å beregne tap som følge av uønskede hendelser. Blant de som oppga kostnadene var det gjennomsnittlige tapet på 200.000 kroner i direkte kostnader og 450.000 kroner i indirekte kostnader. Dårlig sikkerhetskultur og sikring av virksomhetenes systemer kan altså få store økonomiske konsekvenser. Samtidig er det et tankekors at mange er såpass dårlige forberedt når ca. 60% av virksomhetene ble rammet av datakriminalitet eller andre uønskede hendelser.

Ifølge OECD sin handlingsplan er det viktig at offentlig sektor fremstår som en mønsterbruker for å påvirke andre til å gjøre en innsats. Blant annet kan offentlig sektor, i kraft av å gjøre store innkjøp, påvirke utviklingen av produkter slik at sikkerhet får høyere prioritet. FAD mente at offentlig sektor har et ansvar for å utvikle en god sikkerhetskultur, men "at det er vanskelig å vurdere hvor å vurdere i hvor stor grad det offentlige bør satse på dette området" [26, kap. 5.2.1]. Datatilsynet mente at offentlig sektor har en spesielt viktig oppgave for å fremme god sikkerhetskultur i samfunnet, og at offentlig sektor i mye større grad kunne påvirket en slik kultur enn sektoren har gjort. Den Norske Dataforening utførte i 2004 en spørreundersøkelse om IT-anvendelse blant de 500 største private og offentlige virksomhetene i Norge. Undersøkelsen viste at virksomhetene i offentlig sektor forventet at forbedring av IT-sikkerhet ville få langt lavere prioritet i 2007. For private virksomheter var det liten endring i prioriteringen av IT-sikkerhet [26, kap. 5.2.1].

En grunn til at offentlig sektor ikke har utviklet en sikkerhetskultur i samme grad som privat sektor kan skyldes at det finnes få regler og normer for IT-sikkerhet rettet mot offentlig sektor. Mange andre land har slike regler. I USA må føderale virksomheter årlig fremlegge rapport for kongressen som viser at de har overholdt de lovbestemte kravene til IT-sikkerhet for føderale virksomheter. Situasjonen blir ikke automatisk bedre av å innføre regler: 7 av departementene fikk strykkarakter vedrørende oppfyllelsen av disse kravene så sent som i 2005 [26, kap. 5.2.1]. En tett oppfølging av at reglene overholdes er derfor viktig. Regler og normer, samt god oppfølging av disse gjennom tilsynsvirksomhet, vil over tid bidra til å øke sikkerhetskulturen i offentlig sektor.

Tiltak for bevisstgjøring og kompetanseheving

Riksrevisjonen undersøkte statusen på de tiltak innen bevisstgjøring som ble foreslått i Nasjonal strategi for informasjonssikkerhet. En informasjonstjeneste på Internett ble realisert gjennom opprettelsen av nettvett.no. Utviklingen av en undervisningspakke for grunn- og videregående skole var planlagt, men ikke gjennomført da Riksrevisjonen undersøkte status på området. I [25] nevnes det at SAFT (Medietilsynet) tilbyr en læringspakke med fokus på informasjonssikkerhet rettet mot grunn- og videregående skoler, og at Utdanningsdirektoratet også har utarbeidet en slik læringspakke rettet mot lærere. Pakken fra SAFT var planlagt utviklet våren 2005, men ble forskjøvet til våren 2006. Et annet tiltak i den nasjonale strategien er å utvikle og spre informasjons- og veiledningsmateriell om IT-sikkerhet til husstandene. Intet var spesifisert i tilknytning til dette under Riksrevisjonens arbeid. En informasjonskampanje i størrelsesorden 7–8 mill. kr. rettet mot husstandene var planlagt, men strandet fordi næringslivet ikke ville være med på en kampanje i denne størrelsen. Departementene syntes ikke det var riktig at finansieringen utelukkende skulle skje med offentlige midler, da de mente at ansvaret for bevisstgjøring delvis ligger hos næringslivet. Et annet bevisstgjøringstiltak, såkalt Nettvett-dag, ble gjennomført 26. april 2005 og også i 2006. I forbindelse med dagen i 2006 ble det også utgitt en informasjonsavis i Aftenposten med opplag på 300.000 eksemplarer. Nasjonal sikkerhetsdag ble gjennomført 24. april 2007 i samarbeid mellom PT og NorSIS og en rekke andre aktører. Det nevnes at en arbeidsgruppe er opprettet som innen første kvartal 2007 skal komme med forslag til hvordan slike bevisstgjøringsaktiviteter skal gjennomføres i fremtiden. Vedrørende IT-sikkerhet og produkter rettet mot massemarkedet hadde det ikke skjedd noe konkret på området under Riksrevisjonens arbeid, og ifølge [25] foreligger det anno 2007 fortsatt ingen konkrete resultater. Tiltaket foreslås videreført som et løpende tiltak i neste strategi.

Nasjonal strategi har flere tiltak som skal bidra til kompetanseheving innen informasjonssikkerhet. Blant annet skal det arbeides for at ledere av offentlige og private virksomhetene tar ansvar for at virksomheten har tilstrekkelig kompetanse innen informasjonssikkerhet. FAD mente at dette tiltaket ble dekket gjennom eksempelprosjekter og verktøykassen for ROS-metodikk. Å styrke undervisningen i IT-sikkerhet for studier hvor IT er en integrert del av utdanningen var et annet tiltak i strategien. Ingen konkrete tiltak hadde blitt utført på området da Riksrevisjonen utga sin rapport. Etablering av mastergradsstudier innen IT-sikkerhet var nok et tiltak. Ett slikt studium på masternivå ble opprettet ved HiG i 2002. Denne opprettelsen har derimot ikke kommet som følge av myndighetenes arbeid, men derimot som et initiativ fra næringslivet på bakgrunn av manglende kompetanse innen området [23]. Andre tiltak i den nasjonale strategien er å gjennomføre et forskningsprogram innen IT-sikkerhet samt gjennomføre et forskningsprosjekt om tiltak for å sikre samfunnskritisk IKT-infrastruktur. Disse tiltakene ble gjennomført ved opprettelsen av IKT SoS ved Norges forskningsråd og opprettelsen av BAS5 prosjektet ved FFI. IKT SoS og BAS5 ble begge formelt avsluttet i 2007.

Det er svært positivt at IKT SoS og BAS5 har blitt gjennomført som tiltak for kompetanseheving innen informasjonssikkerhet. Opprettelsen av mastergradsstudiet ved HiG er også et meget positivt bidrag til kompetanseheving på området, selv om det primært har kommet på bakgrunn av initiativ fra næringslivet. Med tanke på at kun NTNU og HiG tilbyr mastergradsstudier i informasjonssikkerhet, er det ønskelig at flere andre institusjoner også oppretter slike studier. Viktigheten av informasjonssikkerhet vil i fremtiden bare

øke i omfang.

Når det gjelder styrking av undervisning i IT-sikkerhet i utdanninger hvor IT spiller en sentral rolle, har det skjedd svært lite. Dette må følges bedre opp i den neste nasjonale strategien. IKT-Norge som Riksrevisjonen spurte i sin undersøkelse, uttalte at det "... er et meget stort behov for mer kompetanse når det gjelder sikkerhet på alle nivåer" [26, kap. 5.2.2]. SIS karakteriserte behovet for kompetanse innen informasjonssikkerhet som "skrikende" i den samme undersøkelsen.

Bruk av internasjonale standarder og veiledningsmateriale

SERTIT og Norsk Akkreditering har blitt opprettet for å sertifisere produkter og systemer med informasjonssikkerhet som kriterium. Norsk Akkreditering ble startet i 1991 som følge av EØS avtalen, mens SERTIT ble etablert nesten 10 år etter som offentlig sertifiseringsmyndighet for IT-sikkerhet.

Etter en evaluering av SERTIT 2004 ble det konkludert med at ordningen var faglig god, men for lite markedsfokusert og følgelig også lite kjent i næringslivet. FD mente at dette var bekymringsfullt siden det ble lagt ned mye ressurser på ordningen. FAD og JD påpekte at arbeidet med å gjøre SERTIT kjent og brukt må ses på som en langsiktig oppgave [26, kap. 5.2.3].

Det at sertifisering er såpass lite utstrakt i små og mellomstore bedrifter, kan hovedsaklig begrunnes med at sertifisering er en krevende og kostbar prosess. SIS kommenterte at det ikke fantes markedsmessige fordeler med å være sertifisert. Mindre virksomheter har gjerne begrensede økonomiske rammevilkår som gjør sertifisering av produkter og systemer lite attraktivt. Datatilsynet etterlyste handling for at SERTIT-ordningen skulle få den tiltenkte verdi, mens NSM ønsket at offentlig sektor burde gå foran med et godt eksempel ved selv å gå til innkjøp av sertifiserte produkter og systemer. FAD hadde derimot ingen konkrete planer for å fremme ordningen, som ifølge departementet var forutsatt å være markedsbasert. Bransjeorganisasjonen IKT-Norge mente at visse kunder, og da særlig det offentlige, har hovedfokus på pris. Dette fokuset gjør det vanskelig å fremme salg og bruk av sertifiserte produkter da disse er nødt til å prises høyere grunnet ekstra kostnader ved sertifiseringsprosessen.

Visse tiltak i Nasjonal strategi for informasjonssikkerhet er relevante for å fremme bruk av gode sikkerhetsstandarder eller -retningslinjer. Noen av disse retter seg spesielt mot tjenesteleverandørene, mens andre igjen retter seg mot private virksomheter. Riksrevisjonen påpekte at kun ett av sju relevante tiltak hadde blitt gjennomført, hvilket var utvikling av metoder og verktøy for ROS-analyse. Flere tiltak forelå det ingen konkrete planer for, mens andre igjen var planlagt gjennomført på et senere tidspunkt.

4.2.3 Konklusjon

Riksrevisjonens rapport har vurdert myndighetenes arbeid med å sikre IT-infrastruktur. Dette har skjedd gjennom en vurdering av organiseringen, plan- og gjennomføringsprosessene samt iverksatte tiltakene på området.

Rapporten fokuserer spesielt på Nasjonal strategi for informasjonssikkerhet siden majoriteten av myndighetenes (planlagte) arbeid på området er dokumentert i denne. Det

gis inntrykk av at de foreslåtte tiltakene i Nasjonal strategi for informasjonssikkerhet er tilfredsstillende, men at oppfølgingen av disse har sviktet.

Informasjonssikkerhet er en tverrsektoriell problemstilling, men FAD er departementet med den mest sentrale rollen i dette. Departementet leder KIS og er hovedaktør i oppfølgingen av Nasjonal strategi for informasjonssikkerhet. Andre sentrale departementer er FD (forvalter av Sikkerhetsloven), JD (ansvarlig for sivilt beredskapsarbeid, blant annet gjennom DSB), Samferdselsdepartementet (ansvarlig for telesikkerhet- og beredskap, forvalter ekomloven).

Rapporten vier spesielt stor oppmerksomhet til organiseringen av forvaltningens arbeid med IT-sikkerhet, sikringen av samfunnskritisk IT-infrastruktur og tilrettelegging for utvikling av god sikkerhetskultur.

I det følgende gjengis hovedkritikken under de tre nevnte aktivitetene:

- Organiseringen av forvaltningens arbeid med IT-sikkerhet
  - Manglende ansvarsavklaring mellom departementene har gitt seg utslag i dårlig gjennomføring og oppfølging av tiltak samt forsinkelser i utførelsen av disse. Arbeidsgruppen SARI i KIS jobber per i dag med samordning av regelverk vedrørende informasjonssikkerhet. Fokus bør flyttes til etterlevelse av regelverk etter dette arbeidet er ferdig. Avklaringer må også foretas mellom bransjeorganisasjonene og fagorganene slik at næringslivet vet hvor de skal henvende seg for ulike spørsmål relatert til informasjonssikkerhet.
  - En arbeidsgruppe i KIS vurderte organiseringen av Nasjonal strategi for informasjonssikkerhet, og anbefalte at det ble vurdert å legge overordnet ansvaret for oppfølging til ett departement. Informasjonssikkerhet er en tverrsektoriell problemstilling, og overordnet ansvar for oppfølging av tiltak bør derfor legges til ett departement slik at det ikke er tvil om hvem som er pådriver, og hvor etatene og bransjeorganisasjonene skal henvende seg ved uklarheter. FAD er en naturlig kandidat for denne oppgaven da departementet allerede spiller en nøkkelrolle i oppfølging av strategien.
- Sikringen av samfunnskritisk IT-infrastruktur
  - Riksrevisjonen fant at det ikke eksisterte en entydig tverrsektoriell definisjon på begrepet omfatter. En slik definisjon trengs for å kunne gjennomføre ROS-analyser og således prioriteringer av sikkerhetstiltak. BAS5 prosjektet har fremskaffet noe mer kunnskap på området, men de enkelte virksomhetene må følge opp arbeidet med å identifisere og kartlegge egen kritisk infrastruktur på en metodisk måte slik at en oversikt på sektornivå kan utarbeides. Oversikten er viktig for å prioritere tiltaksområder, og for å hindre at midler brukes på feil beskyttelsesmål.
  - Det er uklart om det er nødvendig å fremstille en entydig nasjonal, tverrsektoriell oversikt over kritisk infrastruktur. En slik oversikt vil ifølge JD ikke bli brukt i den daglige oppfølgingen av tiltak, siden dette ansvaret ligger på sektornivå. Dersom ett departement skal ha hovedansvar for oppfølging av tiltak samtidig som departementet blir ansvarlig for å øremerke midler til de ulike sektorene, vil

derimot en nasjonal oversikt over kritisk infrastruktur være av stor betydning for å kunne prioritere på tvers av sektorene.

- ❒ BAS5 prosjektet er formelt avsluttet og har utviklet metodikk for blant annet ROS-analyse på sektornivå og tverrsektorielt nivå. Det viste seg vanskelig å skaffe nok midler til prosjektet, og Norges forskningsråd finansierte nesten halvparten av prosjektet gjennom forskningsprogrammet IKT SoS. Det bør være større villighet blant departementene til å finansiere forskning som kan gi betydelige bidrag til sårbarhetsreduserende tiltak.
- ❒ Utarbeidelse av sektorvise normer for å beskytte kritisk IT-infrastruktur skulle ifølge Nasjonal strategi for informasjonssikkerhet gjennomføres. Det var ifølge Riksrevisjonens rapport ikke planlagt noen aktiviteter på området. I 2006 ble det lansert felles IT-sikkerhetsnormer for helsesektoren. Oljeindustriens landsforening (OLF) har utarbeidet retningslinjer for informasjonssikkerhet. Utviklingen av generelle offentlige IT-sikkerhetsnormer har FAD gitt i oppdrag til Statskonsult som til nå har laget én prosessbeskrivelse for generell saksbehandling på kunnskapsnettverk.no. Det er usikkert hvilket mål FAD har når det gjelder utvikling av generelle IT-sikkerhetsnormer, men det som så langt er produsert av Statskonsult kan ikke sies å være tilstrekkelig på noen måte.
- ❒ VDI er et system som fanger opp trusler mot norsk IT-infrastruktur. Ved opprettelsen hadde VDI kun 10–15 tilkoblede virksomheter. NorCERT/VDI gir offentliggjør lite informasjon om varslingssystemet for allmennheten. Offentlig tilgjengelig informasjon begrenser seg til en månedlig rapport på rundt 10 sider om registrerte hendelser. Det kan stilles spørsmål ved hvor representativt et slikt begrenset utvalg er av nasjonal IT-infrastruktur, og videre i hvilken grad NorCERT/VDI bør offentliggjøre informasjon fra varslingssystemet. Det offentliggjøres lite informasjon vedrørende suksessfulle angrep, tid til gjenoppretting av normal drift og andre opplysninger fra NorCERT/VDI. Det er derfor vanskelig å eksternt bedømme i hvilken grad NorCERT/VDI har oppnådd målene sine.

  SIS hadde under tiden som prøveprosjekt et mandat som gikk ut på å kartlegge sikkerhetshendelser ved hjelp av innrapportering fra virksomheter. I 2004 mottok SIS mindre enn 5 rapporter, og bare 1 av 3 virksomheter hadde kjennskap til senteret. Mandatet til SIS ble senere endret slik at fokus ble vridd mot bevisstgjøring og senteret byttet forøvrig navn til NorSIS. NorSIS har hatt flere tiltak for å øke bevisstgjøringen. Senteret lanserte i samarbeid med VG en sikkerhetsskole på Internett. Det er likevel mye arbeid som gjenstår før kunnskapsnivået i informasjonssikkerhet blant allmennheten og kommunesektoren er tilfredsstillende.

➢ Tilrettelegging for utvikling av god sikkerhetskultur

- ❒ Bransjeorganisasjonene IKT-Norge, Abelia og NSR var alle enige om at myndighetenes arbeid på dette området var lite synlig i næringslivet.
- ❒ Ifølge OECD sin handlingsplan bør offentlig sektor være et foregangsbilde for å fremme god sikkerhetskultur. Datatilsynet var enig i dette, mens FAD viste

mer tilbakeholdenhet og syntes det var "vanskelig å vurdere i hvor stor grad det offentlige bør satse på dette området".

- En mulig årsak til at sikkerhetskulturen i det offentlige ikke anses som spesielt god, kan være mangel på etablerte normer og regelverk, samt rutiner for å sjekke at disse blir fulgt opp på riktig måte.

Kapittel 5

Offentlige institusjoner og informasjonssikkerhetsarbeid

Dette kapittelet handler om sentrale offentlige organisasjoner og andre institusjoner i tilknytning til myndighetenes nasjonale satsing på informasjonssikkerhet. De mest vesentlige organisasjonene som er involvert i myndighetenes arbeid er kartlagt sammen med relevante arbeider som er gjort på området. Følgende organisasjoner er inkludert: Forsvarets forskningsinstitutt (FFI), Post- og teletilsynet (PT), Koordineringsutvalget for informasjonssikkerhet (KIS), Norges forskningsråd (NFR), Nasjonal sikkerhetsmyndighet (NSM) og de underliggende seksjonene VDI, NorCERT og SERTIT samt NorSIS. I tillegg nevnes relevante utdannings- og forskningsinstitusjoner.

5.1 Forsvarets Forskningsinstitutt (FFI)

5.1.1 Om organisasjonen

Forsvarets forskningsinstitutt har bidratt med viktig forskning på samfunnssårbarhet. Forskningen har omfavnet militære, men også sivile aspekter av samfunnet ved krigstid, fredstid og under kriser.

FFI består av fem avdelinger: Analyse, Ledelsessystemer, Land- og luftsystemer, Maritime systemer og Beskyttelse. I tillegg eksisterer det en felles planenhet [55].

5.1.2 Prosjekter

Flere av prosjektene utført av FFI har rørt ved viktigheten av telenettet og IKT-installasjoner som kritisk infrastruktur. Det har vært utført en serie av prosjekter tilknyttet samfunnets sårbarhet fra 1994 og frem til 2007. Disse har blitt gitt navnet "Beskyttelse av samfunnet" (BAS) og er gjengitt her [56, 57, 58, 59, 60, 13]:

- 1994–1997 Beskyttelse av samfunnet (BAS1)
- 1997–1999 Sårbarhet i offentlig telekommunikasjon (BAS2)
- 1999–2001 Sårbarhet i kraftforsyningen (BAS3)

- 2001–2003 Sårbarhet i transportsektoren (BAS4)
- 2004–2007 Critical Information Infrastructure Protection (BAS5)

BAS prosjektene har vært utført som et samarbeid mellom Forsvarets forskningsinstitutt og Direktoratet for samfunnssikkerhet og beredskap. Andre aktører har også vært involvert i prosjektene. Prosjektene har hatt ca. 2 års varighet og det har vært ca. 7–8 årsverk per prosjekt [22]. Det siste prosjektet i denne rekken, BAS5, hadde et budsjett på 12 millioner kroner [56].

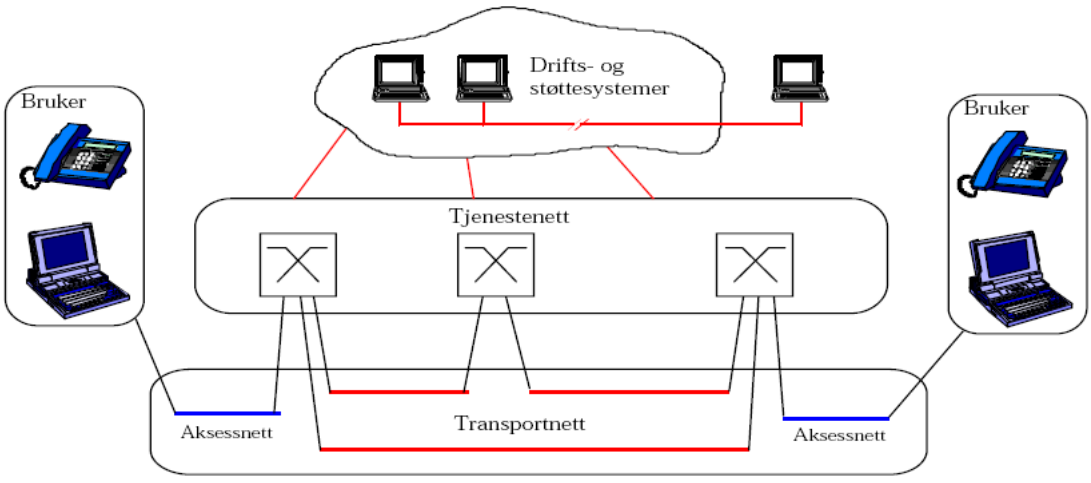
Av de fem BAS prosjektene som har vært utført hittil, er det BAS2 og BAS5 som er mest relevante for denne oppgaven. Innholdet fra de andre rapportene vil derfor bli sammenfattet kortere. Det bemerkes at sluttrapportene for BAS prosjektene kun oppsummerer hovedpoenger fra delarbeider gjort i tilknytning til prosjektene. Sluttrapportene gir således bare et overordnet bilde av det arbeidet som er gjort for hvert enkelt prosjekt.

BAS1 – Beskyttelse av samfunnet

I BAS1 ble telenettets sårbarhet påpekt, og det anbefalt å øke satsingen på tiltak for økt robusthet og fleksibilitet innen telekommunikasjon. FFI rangerte tiltak innen telekommunikasjon som det viktigste satsingområde etter kraftforsyningen og ledelse i krisehåndtering. Rapporten inneholdt også en avhengighetsanalyse som konkluderte med at tilnærmet alle sektorer var avhengige av telekommunikasjon [57, kap. 8.2]. BAS1 prosjektet pekte ut spesielt sårbare sektorer og la dermed grunnlaget for videreføringen av BAS prosjektene som skulle omhandle tele-, kraft- og transportsektoren.

BAS2 – Sårbarhet i offentlig telekommunikasjon

Primæroppgaven i BAS2 var å analysere sårbarheten i offentlig telekommunikasjon. Videre skulle prosjektet vurdere konsekvensene av tap av telekommunikasjon, og evaluere tiltak som kunne minske sårbarheten og konsekvensene [58].



Figur 5.1: *Telenettets oppbygging [58, kap. 3.2].*

Som illustrert i figur 5.1, er tjenestenettet en del av telenettet. Tjenestenettet består av et sett med tjenestenoder som tilbyr funksjonalitet for teletjenester til brukerne. En telesentral for formidling av telefoni er den vanligste formen for tjenestenode. Tjenestenoder kan også formidle datatrafikk seg imellom.

Rapporten pekte på problemet med en reduksjon av antall tjenestenoder i tjenestenettet som følge av ønske om mer effektiv drift og tjenesteproduksjon [58, kap. 3.3]. En reduksjon og sentralisering av tjenestenoder fører til økt sårbarhet i nettet, siden antall veier i nettverket reduseres. Et annet problem som ble tatt opp var at stadige nye tjenester og konvergens av eksisterende tjenester i nettet førte til økt kompleksitet, noe som kan være en trussel i seg selv. Stor kompleksitet kan gi et uoversiktlig bilde av hvordan systemer virker og gjøre det vanskelig å kartlegge konsekvensene av eventuelle feil.

Avmonopoliseringen av telemarkedet førte til nye aktører og konkurranse mellom disse. Et negativt aspekt ved dette er at markedet vil utvikle seg uten noen form for koordinert styring. Konkurranse leder gjerne til mindre økonomiske gevinster, noe som kan gi et for stort fokus på lønnsomhet og et for lite fokus på sikkerhet og robusthet. I rapporten nevnes det at aktørene på telemarkedet sørger for høy driftsikkerhet av egne tjenester og tiltak mot normale driftsforstyrrelser, men at det fokuseres lite på tiltak mot mer usannsynlige og alvorlige hendelser. Den lille sannsynligheten for at slike alvorlige hendelser finner sted gjør det økonomisk sett lite attraktivt for operatørene å beskytte seg mot de.

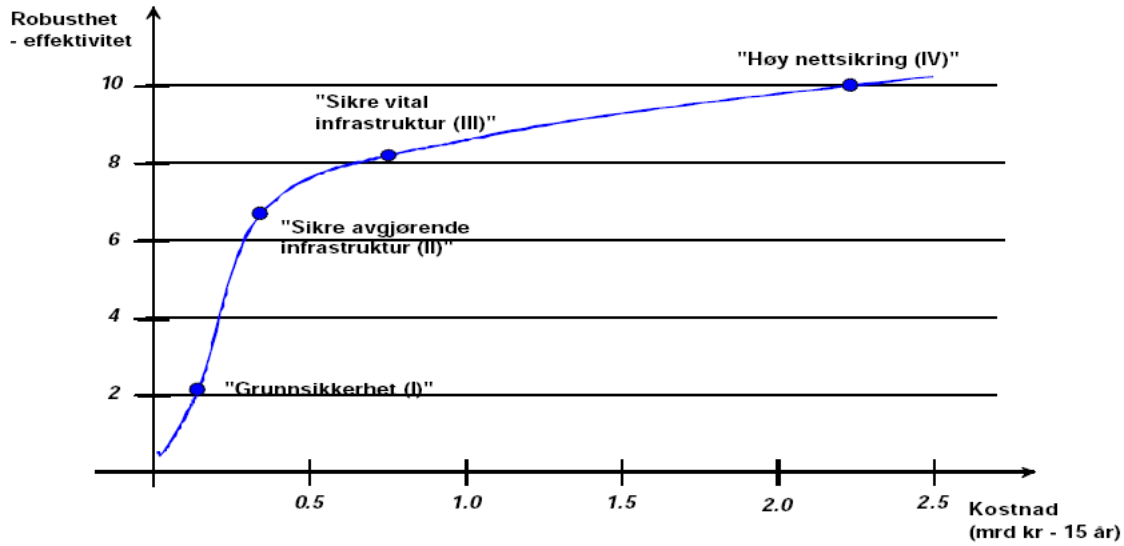
For å motvirke en ukontrollert utvikling av telenettet med hensyn på sårbarhet, anbefalte prosjektgruppen offentlige inngrep i markedet. Staten burde sette premisser for utviklingen og bevilge ressurser der dette er nødvendig [58, kap. 4.1]. Tiltak for å forebygge sårbarhet i telenettet kunne blitt finansiert gjennom offentlige midler. Eventuelt kunne telemyndigheten kommet med lovpålegg om tiltak. Ifølge rapporten hadde myndighetene gjennom lovverket anledning til å stille konsesjonsbetingelser til tjenesteleverandører med mer enn 25% markedsandel [58, kap. 4.1]. Skulle slike konsesjonsbetingelser eller andre pålegg bli benyttet, vil det være viktig at de ikke er "urimelige og konkurransevridende" [58, kap. 4.1].

Prosjektgruppen utarbeidet fire hovedstrategier for å sikre offentlig telekommunikasjon: Grunnsikkerhet, Sikre avgjørende infrastruktur, Sikre vital infrastruktur og Høy nettsikring. Summen av kostnadene til alle tiltakene og deres effektivitet varierte mellom strategiene og kan sees i figur 5.2.

"Grunnsikkerhet" var rettet mot tjenestenett og å sikre prioritert kommunikasjon til viktige brukere [58, kap. 5]. Målet var å få en nødvendig basis for sikkerhet, men strategien var på ingen måte tilstrekkelig i seg selv. Tiltakene omhandlet styrking av driftsfunksjonen i operatørenes nett og økt informasjonssikkerhet for drift og tjenesteproduksjon i ulike telenett [58, kap. 5].

"Sikre avgjørende infrastruktur" bygde på strategien om grunnsikkerhet. Målet var her å sikre infrastrukturen som var avgjørende for telenettets tilgjengelighet: driftssentraler og fjernsentraler i Norges fem største byer. Angrep rettet mot disse installasjonene kunne ramme hele nasjonen. Tiltakene var rettet mot de viktigste teleoperatørene og omfavnet fysiske og elektroniske trusler. Kostnaden knyttet til disse tiltakene ville være begrenset og effekten langvarig [58, kap. 5].

"Sikre vital infrastruktur" forutsatte realisering av de to første strategiene. Målet med denne strategien var å beskytte infrastruktur i større byer fra fysiske og elektroniske angrep.



Figur 5.2: *Strategialternativer for sikring av offentlig telekommunikasjon – forholdet mellom effektivitet og kostnad [58, kap. 5].*

Angrep på vital infrastruktur ville i hovedsak få regionale virkninger. Strategien ville oppnå en "betydelig økning i sikring for en mindre økning i kostnader" [58, kap. 5]. For større menneskeskapte utfordringer ville tiltakene i en slik strategi ikke være tilstrekkelige.

"Høy nettsikring" var den siste og mest omfattende strategien i det den forutsatte at tiltakene i alle de andre strategiene hadde blitt realisert. Tiltak omfattet å sikre femten punkter i landet med fjellanlegg, foreta en betydelig styrking av transportnettstrukturen samt en bedre funksjon for brukerprioritet på telenettet som omfattet alle teleoperatører [58, kap. 5]. Rapporten påpekte at et telenett alltid vil være et utsatt mål i krigstid, og derfor ikke kan sikres 100%. "Høy nettsikring" var heller ikke ment å være taket for de tiltak som kunne implementeres for å bedre sikkerheten.

Prosjektgruppen mente at strategien "Sikre vital infrastruktur" burde realiseres for å ta igjen det tapte arbeidet på sikring av telenettet årene i forveien. Strategien "Høy nettsikring" ville blitt svært mye dyrere å realisere enn strategien for sikring av vital infrastruktur, og det var på bakgrunn av den økonomiske forskjellen at denne anbefalingen kom [58, kap. 5]. Totalt 760 millioner kroner (i 1999) ville blitt brukt for å realisere sikring av vital infrastruktur over en periode på 15 år. På lang sikt mente naturlig nok prosjektgruppen at man burde prøve å realisere strategien "Høy nettsikring". Tiltakene som ble foreslått tilsa at det var et behov for "sterkt offentlig engasjement og en stor andel av offentlig finansiering" [58, kap. 4.1].

Sluttrapporten til BAS2 inneholder ikke en detaljert oversikt over foreslåtte tiltak for de fire strategiene. For nærmere beskrivelse av tiltak henvises det til FFI/RAPPORT-99/00241 og FFI/RAPPORT-99/00242 som er gradert henholdsvis konfidensiell og begrenset. Det finnes derfor ingen mulighet til å beskrive innholdet i disse rapportene her.

BAS3 – Sårbarhet i kraftforsyningen

Denne rapporten beskrev blant annet sårbarheten ved bruk av IKT i drifts- og styringssystemene. Tidligere var det ansatte som overvåket og betjente disse systemene. Etterhvert ble IKT tatt i bruk slik anleggene kunne fjernstyres fra noen få driftsentraler. De fleste aktørene deler lokalnettverket sitt i to for å skille mellom prosesstyring og administrasjon [59, kap. 5.1.2]. Administrasjonsnettverket har eksterne forbindelser, men prosesstyring bør ideelt skje på et lukket nettverk for å hindre uvedkommende utenfra tilgang. På grunn av økende behov for datautveksling mellom prosesstyring og administrasjon er det blitt vanlig å koble de to nettene sammen. Denne sammenkoblingen av nettene blottlegger prosesstyringen for datakyndige personer og ble betegnet som kanskje den største enkeltsårbarheten i kraftforsyningen [59, kap. 5.1.2].

Driften av kraftforsyningen er også avhengig av godt samband. Sambandet brukes for å overføre datatrafikk men også for å kontakte personell ute på oppdrag. Før var dette sambandet stort sett eid av kraftforsyningen selv, men senere ble kraftforsyningen avhengige av teletjenester fra det offentlige markedet. Kraftforsyningen er derfor avhengig av at teleselskapet ansvarlig for kommunikasjonen har god beredskap i tilfelle et uventet problem skulle oppstå [59, kap. 5.1.2].

I delkapittelet "IKT-avhengigheten eksploderer" (se [59, kap. 5.2.4]) spås det en stadig økende avhengighet til IKT som vil føre til færre ansatte. Det nevnes også at mye praktisk kompetanse vil gå tapt, og at personell som kun er vant med å regulere alt fra en datamaskin vil kunne få problemer med å forstå hva som er årsaken til feil som oppstår. Det blir påpekt at kraftselskapenes IKT-systemer i økende grad vil være basert på standardiserte systemer med kjente sikkerhetshull for å øke interoperabiliteten og kostnadseffektiviteten mellom selskapene.

Rapporten anbefaler å oppdatere regelverket slik at IKT-trusler, og ikke bare fysiske trusler, blir tatt hensyn til. Som i BAS2 ble flere strategialternativer også foreslått i BAS3. Den mest elementære strategien inneholdt sikringstiltak av IT-systemene i kraftforsyningen samt opprettelsen av et kompetansesenter på informasjonssikkerhet som kunne bistå bransjen med informasjon om sårbarhet og informasjonssikring. Kostnaden for tiltakene i denne strategien var beregnet til 70 millioner kroner (i 2001) over 10 år. Et billig alternativ, men langt fra nok for å oppnå tilfredsstillende sikring av kraftforsyningen [59, kap. 7].

BAS4 – Sårbarhet i transportsektoren

I BAS4 blir ondsinnede dataprogrammer nevnt som ett av fire mulig virkemidler for å ramme transportsektoren. Selv om terrorister stort sett har brukt tradisjonelle midler for å ramme transportsektoren, peker rapporten på at det er stor usikkerhet knyttet til bruk av IKT som virkemiddel i fremtiden.

Økende avhengighet til IKT systemer for styring av logistikk bidrar også til økt sårbarhet i transportsektoren [60, kap. 3.1]. Ofte er det mange involverte parter i transportering av gods, og disse må kunne kommunisere med hverandre.

Trafikkstyring er en kritisk og svært IKT avhengig funksjon innen luftfart og jernbanesektoren [60, kap 3.5]. I fremtiden er det mulig at trafikkstyring også blir kritisk avhengig av IKT innen sjøtransport og vegtransport.

Ifølge rapporten har dereguleringen som har skjedd i hele transportsektoren ført til økt fokus på økonomi. Tiltak for å fremme sikkerheten og beredskapen har kun blitt gjennomført der det har blitt lovpålagt av myndighetene [60, kap. 3.6]. I tillegg har økende avhengighet til IKT skapt en større IKT-avdeling samtidig som personellstaben er blitt redusert. Det vil derfor bli en stor utfordring for bedriftene å gå tilbake til manuelle systemer og manuelt arbeid dersom kritiske IKT-systemer går ned.

Rapporten konkluderer med at IKT-systemer innen logistikkstyring og til en viss grad trafikkstyring er spesielt sårbare. Transportkapasiteten ville blitt kraftig redusert dersom IKT-systemer for logikkstyring gikk ned. IKT kan forøvrig også brukes i en krisesituasjon for å lette beredskapsarbeidet: man kan effektivt kartlegge hvilke ressurser som er tilgjengelige [60, kap. 5.1].

For å redusere sårbarheten i transportsektoren, anbefales det at virksomheter i transportsektoren etablerer relasjoner til NorSIS. Videre anbefales det at den nasjonale strategien for informasjonssikkerhet lager en ramme for IKT-sikkerhet til transportsektoren. Rapporten peker også på nødvendigheten av at objektsikkerhetsforskriften omfatter "IKT-baserte prosessystemer innen viktige samfunnsinfrastrukturer" [60, kap. 5.2].

BAS5 – Critical Information Infrastructure Protection

BAS5 handlet i hovedsak om metodikk for å analysere samfunnskritiske IKT-systemer. Viktige hovedmål for prosjektet var å utvikle og anvende metodikk for [13, kap. 1.2]:

- Identifisering og rangering av kritiske samfunnsfunksjoner og IKT-systemer
- Risikoanalyse av samfunnskritiske IKT-systemer
- Effektivitetsvurderinger av tiltak som kan redusere sårbarheter i IKT-systemer

Disse tre metodikkene skulle gi svar på følgende spørsmål [13, kap. 1.2]:

- Hva er de mest samfunnskritiske virksomhetene og IKT-systemene? (mål nr. 1)
- Hvordan kan risiko og sårbarhet i de kritiske IKT-systemene analyseres? (mål nr. 2)
- Hvordan kan man velge blant ulike tiltak for å øke sikkerheten i IKT-systemene? (mål nr. 3)

De tre målene er bare delvis nådd i og med at prosjektgruppen ikke rakk å teste metodikk for det første og siste punktet. For metodikken under punkt én ble kun mindre tester anvendt For det siste punktet ble det opprettet en doktorgrad som ennå ikke er fullført men ventes fullført januar 2009 [13].

Rapporten peker på at det historisk sett ikke har vært mangel på tiltak for IKT-sikkerhet, men at manglende rammebetingelser har vært i veien for at slike tiltak har kunnet blitt gjennomført og videre være en del av en kontinuerlig arbeidsprosess. Mye arbeid har blitt lagt ned i forbindelse med forskning og utredninger for å lage tiltakslister, men gevinsten av dette arbeidet har ikke vært like stor som arbeidsmengden bak det skulle tilsi [13, kap. 3.1]. Prosjektgruppen mener dette delvis skyldes at problemstillingen om sårbarhet i infrastruktur har økt i kompleksitet i nyere tid.

Den økte kompleksiteten skyldes blant annet [13, kap. 3.2]:

- Mer kompleks tjenesterealisering i infrastrukturen
- Flere tverrsektorielle avhengigheter
- Privatisering av Televerket og mange ulike tjenesteleverandører
- Mer dynamisk trusselbilde

Økt kompleksitet er ikke det eneste problemet. Teknologiutviklingen foregår i et så høyt tempo at tiltakene som foreslås av utredningsgrupper i visse tilfeller ender opp med å bli foreldet før de kan realiseres. Et eksempel på dette er stortingsmeldingen som kom i kjølvannet av BAS2 prosjektet. Kun et fåtall av tiltakene i denne meldingen ble gjennomført, hvilket tyder på at den teknologiske og markedsmessige utviklingen gikk for fort til at tiltakene kunne bli implementert. Norsk forvaltningsskikk må også ta sin del av ansvaret for at dette skjedde siden behandlingen av tiltakenes iverksettelse har tatt for lang tid [13, kap. 3.3].

Rapporten argumenterer for at det mangel på IKT-sikkerhetstiltak ikke er et problem, og at det faktiske problemet består i å sørge for at "et målrettet sikkerhetsarbeid skjer fortløpende og med klare målsettinger, slik at de tiltak som anses som nødvendige faktisk blir iverksatt fortløpende" [13, kap. 3.3]. For å oppnå dette målet må man bruke gode arbeidsprosesser med vekt på metodiske tilnærminger.

Identifisering og rangering av kritiske samfunnsfunksjoner og IKT-systemer

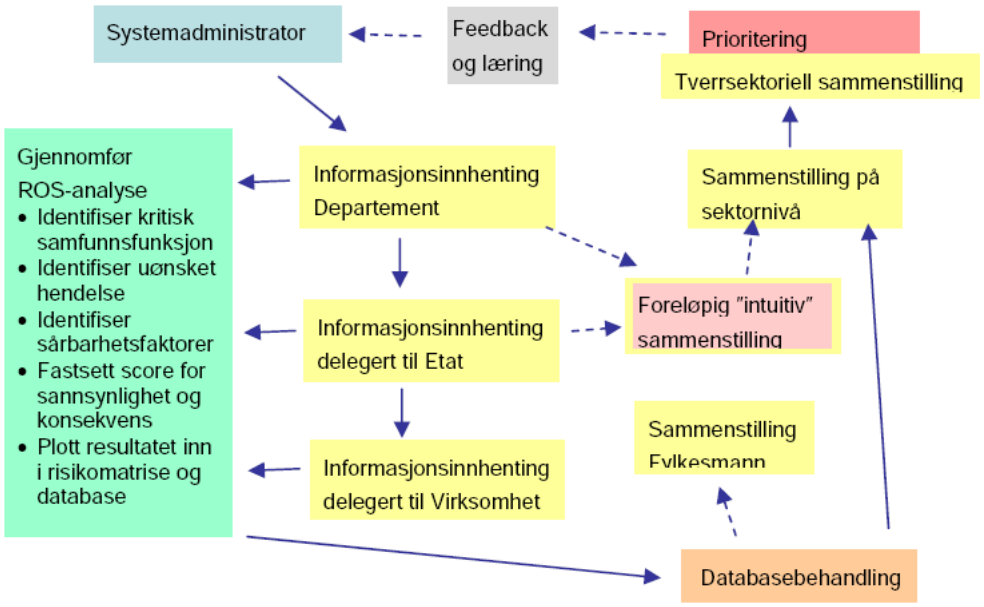
Prosjektgruppen utviklet en metodikk for å rangere og prioritere alle kritiske samfunnsfunksjoner [1]. Alle kritiske infrastrukturer (inkludert kritiske IKT-systemer) er en del av de kritiske samfunnsfunksjonene.

BAS5 utviklet et system for beslutningsstøtte, og ikke et system for automatisk rangering av kritiske samfunnsfunksjoner. Dette betyr at vurderinger fra relevante beslutningsmiljøer er grunnsteinen i prosessen for å rangere samfunnsfunksjonene. Eksperter innenfor fagområdene kan også bidra til rangeringen, selv om de ikke alene kan stå bak rangeringen [13, kap. 4.1].

Som en del av arbeidet med BAS5 ble det utført en bakgrunnstudie hvor deltagerne av prosjektet undersøkte om det fantes metodikker i noen andre land lik de BAS5 hadde som mål å utvikle. Det ble ikke funnet en helhetlig metodikk i bruk for rangering av kritiske samfunnsfunksjoner og infrastruktur i disse landene. Derimot ble det funnet mye metodikk som var relevant for denne problemstillingen i BAS5, slik som metodikk for nasjonale ROS-vurderinger og analyse av gjensidige avhengigheter [13, kap. 4.2].

Rangering av kritiske samfunnsfunksjoner er tett knyttet til risiko- og sårbarhetsvurderinger. ROS-analyser bør derfor være en viktig del av beslutningsgrunnlaget for prioriteringen av samfunnsfunksjonene. BAS5 prosjektets metode for rangering av kritiske samfunnsfunksjoner består av to elementer. Det første er utviklingen og forankringen av en løpende prosess i ansvarlige departementer og blant andre som har ansvar og kunnskap innen egen sektor. Det andre er at det brukes en ROS-basert teknikk for å støtte den førstnevnte prosessen [13, kap. 4.3]. Prosessens sykel er illustrert i figur 5.3.

[1] Begrepet er definert som følger: "Kritiske samfunnsfunksjoner er alle funksjoner som samfunnet er avhengig av for å dekke befolkningens grunnleggende behov" [13, kap. 2].



Figur 5.3: *Prosess for beslutningsstøtte til rangering/prioritering av kritiske samfunnsfunksjoner. Heltrukne piler angir hovedløpet i prosessen. Deltrukne angir mulige tilleggssteg [13, kap. 4.3].*

Prosjektgruppen nevner visse krav som må oppfylles for at prosessen skal virke som planlagt: en overordnet koordinator på nasjonalt nivå, utnyttelse av det ordinære ansvarsprinsippet for å strukturere arbeidet samt etablering av tverrsektorielle felles prosedyrer og standarder [13, kap. 4.3]. Felles standarder er nødvendig siden metoden skal kunne brukes til å understøtte prioriteringer på tvers av samfunnssektorene. Valg av en konkret metodikk for ROS-analyse er opp til den enkelte sektor eller virksomhet å avgjøre, men resultatene fra slike analyser må uten unntak følge et bestemt format. Blant faktorene som skal innrapporteres fra ROS-analyser er følgende: en hierarkisk organisert liste over kritiske samfunnsfunksjoner og uønskede hendelser, sannsynlighet, konsekvenser og elleve andre variabler inkludert sted, geografisk omfang og befolkningstetthet.

Prosjektgruppen forutsetter opprettelsen av en database slik at prioriteringer kan foretas på tvers av virksomheter og sektorer, og etter ønsket variabel. Metodikken som benyttes for rangering er fleksibel nok til å anvendes på flere nivåer: rangering av sektorer innen et samfunn, virksomheter innen en sektor eller objekter innen en virksomhet [13, kap. 4.2]. Det påpekes likevel at metodikken spesielt er myntet på (tverr)sektorielle problemstillinger.

Rapporten anbefaler at metodikken *ikke* brukes for å utvikle generelle, langvarige og statiske prioriteringslister. Dette er fordi endringstakten i dagens moderne samfunn er svært høy. ROS-analyser som utføres i tilknytning til denne metodikken må derfor revideres jevnlig. Som et eksempel på at det kan være vanskelig og ikke minst uheldig å lage generelle og statiske prioriteringslister nevner prosjektgruppen mobiltelefoni. Det har fra flere hold vært ytret ønske om en prioriteringsordning på mobilnettet slik at ansvarlige aktører er sikret prioritert tilgang i krisesituasjoner hvor nettet overbelastes. Hvem som

bør ha prioritert tilgang avhenger sterkt av hva slags krisesituasjon det er snakk om. For eksempel krever en redningsaksjon i forbindelse med en trafikkulykke og et strømbrudd i forbindelse med svikt i infrastruktur håndtering av vidt forskjellige aktører.

Som et ledd i videreføringen av arbeidet ble det anbefalt at metoden ble testet ut i større skala da kun mindre tester ble utført under utviklingen av metoden. Videre ble det anbefalt at NSM og DSB burde prøve å forankre ansvaret for prosessen bak metoden samt videreutvikle selve metoden. Som forslag til videreutvikling foreslo prosjektgruppen å utvikle et hierarki over sannsynlige hendelser, vurdere for hvilke scenarier prioritering er meningsfullt samt undersøke hvordan man kan håndtere ukjent risiko.

Risikoanalyse av samfunnskritiske IKT-systemer

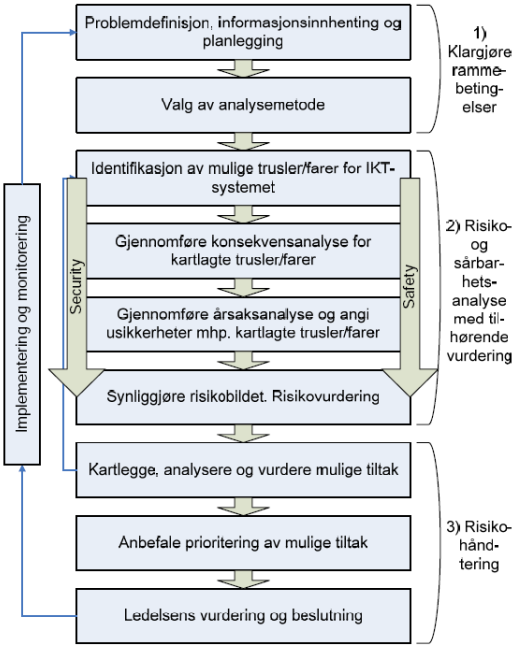
Delmål nummer to i BAS5 var å utvikle en metodikk for risikoanalyse av samfunnskritiske IKT-systemer. ROS-analyser kan gi verdifull informasjon om hvor sårbarhet og risiko gjør seg gjeldende i størst grad og således bidra til å realisere risikoreduserende tiltak i henhold til en prioriteringsliste. Tiltak kan være rettet for eksempel mot teknologi, arbeidsprosesser eller kravspesifikasjoner, og de kan realiseres både med tanke på eksisterende systemer og utviklingen av nye systemer. Tiltakene kan prioriteres i henhold til ROS-analyser, men også i henhold til kosteffektivitetsanalyser og kostnytteanalyser [13, kap. 5.1].

ROS-analyser har vært benyttet innen kjernekraft og olje- og gassindustrien i flere år. For IKT-systemer finnes det også allerede et stort antall ROS metoder, og prosjektgruppen valgte derfor å bygge å eksisterende resultater og komplementere med egen forskning hvor nødvendig. Prosessen for risikostyring som BAS5 prosjektet endte opp med er illustrert i figur 5.4.

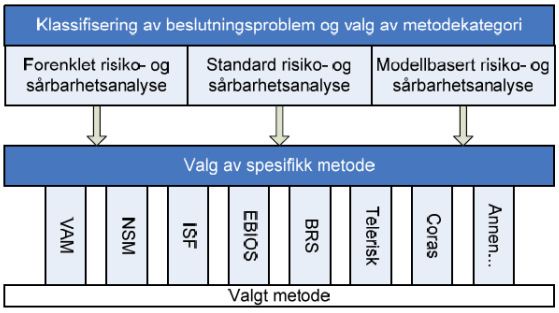
Prosessen inneholder tre hovedaktiviteter som vist i figuren: klargjøring av rammebetingelser, gjennomføring av ROS-analyse og risikohåndtering. Det å velge metode for ROS-analyse av IKT-systemer er en viktig del av prosessen. Ulike metoder har forskjellige styrker og svakheter, og det er derfor viktig å finne rett verktøy for jobben. Figur 5.5 illustrerer forskjellige metoder og overordnede klasser. Metoder tilhørende klassen "Forenklet ROS" benytter en kvalitativ tilnærming eksempelvis i form av gruppediskusjoner. Metoder under de to andre klassene bruker i stedet en kvantitativ tilnærming og mer formelle metoder. I alt evaluerte prosjektgruppen sju forskjellige metoder, hvorav fire ble prøvd på reelle caseanalyser [13, kap. 5.3.2].

Arbeidet med caseanalysene ledet prosjektgruppen til å lage en overordnet veileder for å utføre ROS-analyse av samfunnskritiske IKT-systemer. Veilederen tar for seg alle tre stegene i risikostyringsprosessen, og ble laget fordi ROS-analyser av IKT-systemer gjøres i stort omfang og varierer mye i kvalitet. Det ble derfor understreket at god ledelse og gjennomføring av ROS-arbeid faktisk er viktigere enn valg av metodikk for ROS-analysen. Noe av den sprikende kvalitetsforskjellen blant analysene som gjøres i dag kan muligens forklares med at ROS-analyse av IKT-systemer skiller seg fra ROS-analyser i tradisjonelle sektorer på flere vis [13, kap. 5.5.1]:

- Tilsiktede handlinger spiller en sentral rolle når IKT-sikkerhet skal vurderes. Dette er en utfordring å håndtere metodisk.
- Teknologien er kompleks. Det er vanskelig å få en god oversikt over systemene, og det mangler ofte tegninger som gir en helhetlig beskrivelse av systemene som skal



Figur 5.4: *Risikostyringsprosess [13, kap. 5.3.1].*



Figur 5.5: *Valg av metode for ROS-analyse [13, kap. 5.3.2].*

analyseres. I tillegg er det vanskelig å utvikle tegninger som kan benyttes til risikoanalysene. Dette gir store utfordringer i forhold til å identifisere mulige hendelser, og ikke minst i forhold til det å få en god forståelse av sammenhenger og avhengigheter systemene imellom.

- Brukerne av IKT-systemene mangler ofte en detaljert systemforståelse. De har et forhold til informasjonen som IKT-systemet gir dem, men liten forståelse for teknologien som ligger bak.
- Organisasjonen som bruke systemene er ofte distribuerte og med svært ulikt kompetansenivå.
- Det er få eller ingen som både har en god forståelse av både IKT-systemer og av fagområdet risikoanalyse.
- Teknologien endrer seg veldig raskt. Dette medfører at man ofte har begrenset erfaringsdata som kan bruke inn i analysene.

Oppsummert kan man si at denne delen av BAS5 prosjektet laget "en risikostyringsprosess for ROS-analyser av IKT og en formalisert prosess for valg av metodikk", samt "en overordnet veileder for ROS-analyse av IKT-systemer" [13, kap. 5.6].

Effektivitetsvurderinger av tiltak som kan redusere sårbarheter i IKT-systemer

Mesteparten av arbeidet i tilknytning til denne oppgaven pågår i forbindelse med en doktorgradsstudie på Høgskolen i Gjøvik og er ikke ferdig før januar 2009. Resultatene som her presenteres er derfor foreløpige og dekker ikke hele problemstillingen.

Etter en ROS-analyse er utført av et IKT-system vil man ha kommet fram til en mengde forskjellige tiltak som kan implementeres for å bedre sikkerheten. Siden de sikkerhetsansvarlige ikke har ubegrenset med midler må de finne ut hvilke tiltak som er de mest effektive slik at nettopp de tiltakene kan implementeres. Ett aspekt ved en slik prioritering er preventive kontra skadereduserende tiltak. For å hjelpe sikkerhetsansvarlige i å velge de mest effektive tiltakene under rammebetingelser tar doktorgradsstudien for seg følgende forskningsspørsmål [13, kap. 6.1]:

- Hvilke forskjellige betydninger kan legges til begrepet "effektivitet av informasjonssikkerhetstiltak"?
- Hvilke metoder og metrikker gir gode målinger av effektivitet, og hvilke brukererfaringer finnes mht. å måle effektivitet av sikkerhetstiltak?
- Hvilke metrikker kan gi bedre målinger på effektiviteten av organisatoriske og tekniske informasjonssikkerhetstiltak, bli forstått av ledelsen og bidra til organisasjonens læring?
- I hvilken grad vil støy rundt beslutningsprosessen påvirke måling og rapportering av effektivitet av implementerte sikkerhetstiltak?

Studien benytter seg blant annet av materiale fra Mørketallsundersøkelsen i 2006 som ble utarbeidet av Næringslivets sikkerhetsråd, Politiets datakrimsenter (PDS) og NorSIS.

Det arbeidet som så langt er utført ved studien omhandler sammenheng mellom enkelttiltak og sikkerhetshendelser, analyse av Mørketallsundersøkelsen datagrunnlag (med fokus på aksesskontroll og beskyttelse av lagrede data) samt effektiviteten av organisatoriske tiltak [13, kap. 6.4].

Annet arbeid som er planlagt utført i studien omfatter statistiske metoder for analyse av effekt ved implementering av flere tiltak samtidig og en teoristudie på effektivitet av informasjonssikkerhetstiltak [13, kap. 6.5].

5.2 Post- og teletilsynet (PT)

5.2.1 Om organisasjonen

Post- og teletilsynet (PT) er et forvaltningsorgan som er underlagt Samferdselsdepartementet, og har i oppgave å regulere post- og telesektoren. PT ble opprettet i 1987 (da under navnet Statens teleforvaltning) som følge av liberaliseringen på telekommunikasjonsområdet og fikk ansvaret med å regulere operatørenes rolle i markedet [61]. Organisasjonen er selvfinansiert og mesteparten av inntektene kommer fra gebyrer. I underkant av 90% av den totale inntekten fra gebyrene kommer fra tilbydere av elektroniske kommunikasjonsnett og tjenester, sertifikatutstedere, innehavere av løyve til bruk av nummer, navn, adresseressurser (for eksempel domenenavn) og frekvenser [62].

5.2.2 Arbeid

Lov om elektronisk kommunikasjon (ekomloven)

I Ot.prp. nr. 58 (2002–2003) ble det lagt frem et lovforslag som skulle avløse den daværende teleloven og annen regulering. Teleloven trådde i kraft i 1. januar 1996 og hadde til hensikt å tilrettelegge for liberalisering av telesektoren i Norge. Loven var ment å fungere i en overgangsperiode for å sikre konkurranse og etablering av nye aktører mens telemonopolet ble avviklet. Utvikling innen teknologi og marked ga etterhvert et behov for endringer i lovverket, og teleloven ble derfor erstattet av ekomloven med virkning fra 25. juli 2003. Det er Post- og teletilsynets oppgave å forvalte loven. Ekomloven søker å regulere sektoren med utgangspunkt i generell konkurranserett, og vil kun pålegge sektorspesifikke forpliktelser overfor tilbydere som befinner seg i et marked uten tilstrekkelig konkurranse [63, kap. 1.1].

Lovens formål er definert i § 1 og lyder slik: "Lovens formål 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, samt stimulere til næringsutvikling og innovasjon". Loven skal også legge forholdene til rette for nyskapning og innovative tjenester samtidig som den skal fremme krav til sikkerhet og integritet [63, kap. 1.2.2].

For å nå formålet med loven ble det foreslått at "virksom og bærekraftig konkurranse skal være det viktigste virkemidlet for å sikre god utnyttelse av samfunnets ressurser og gi høyere verdiskapning innenfor området for elektronisk kommunikasjon" [63, kap. 1.2.1].

Arbeidet for å nå målet skal følge disse prinsippene [63, kap 1.2.1]:

Minimumsregulering Bruk av sektorspesifikk regulering skal kun brukes dersom målene i regelverket ikke kan nås ved alminnelig konkurranserett.

Teknologinøytralitet Regelverket skal ikke favorisere bruk av bestemte teknologier.

Ikke-diskriminering Virksomheter med sterkt dominerende markedsposisjon skal ikke tillates å bruke denne for å skade konkurransen.

Hovedpunktene i ekomloven er følgende [63]:

- Gå fra sektorspesifikk konkurranseregulering til generell konkurranseregulering.
- Harmonisere regelverket med EUs regelverk for elektronisk kommunikasjon.
- Utvide lovens virkeområde til å omfatte alle kommunikasjonsnett, inkludert telenettet som var dekket av teleloven, slik at alle nettverkene får felles betingelser. Kun overføringen av signaler reguleres gjennom loven, ikke innholdet i tjenester som leveres via nettverkene.
- Begrense reguleringer vedrørende etablering og drift til et nødvendig minimum med et rettslig rammeverk.
- Videreføre ordningen med at markedsdominerende tilbydere kan pålegges forpliktelser for å tilrettelegge for andre aktører, men heve terskelen for å bli utpekt som markedsdominerende tilbyder.
- Individuelle konsesjoner til tilbydere skal kun omfatte begrensede ressurser som frekvenstillatelser og nummer. Telenors konsesjon, gitt på grunn av selskapets sterke markedsstilling, oppheves av den grunn. Telenors forpliktelser fra konsesjonen videreføres likevel i annen avtale slik at tjenester som levering av telefoni til hele landet, drifting av telefonautomater og opplysningstjeneste samt andre nødvendige tjenester opprettholdes.
- Angående klageordning for tilbydere så omgjøres "Statens teleforvaltningsråd" til "Klagenemnda for elektronisk kommunikasjon" og får utvidet kompetanse slik at alle enkeltvedtak fattet av Post- og teletilsynet med hjemmel i ekomloven som hovedregel blir behandlet av klagenemnda.
- Klageordning for brukere foreslås realisert ved å utvide Tele kompetanse fra bare å omfatte telepriser til også å omfatte klager vedrørende leveringspliktige tjenester og klager på tjenester som en tilbyder har sterk markedsstilling på. Nytt navn på Teleklagenemnda blir "Brukerklagenemnda for elektronisk kommunikasjon".
- Konsesjonsplikten for forvaltning og bruk av knappe ressurser (frekvenser og nummer) opprettholdes. Regulering av frekvensplanlegging og tildeling av tillatelser til bruk av frekvenser skjerpes og saksbehandlingen for å innvilge tillatelser tydeliggjøres. Frekvenser i det elektromagnetiske spekteret er en begrenset ressurs, og med økende etterspørsel av ledige frekvenser er det behov for å innføre strengere krav for slik tildeling.
- Videreføring av reglene om kommunikasjonsvern og kommunikasjonskontroll hvor "trafikkdata som hovedregel skal slettes eller anonymiseres så snart oppbevaring ikke lengre er nødvendig for fakturering" [63, kap. 1.2.2]. Tilbyders plikt vedrørende tilrettelegging for situasjoner hvor politiet har lovbestemt tilgang til trafikkdata fjernes

fra forskriften [2] og lovfestes i stedet. Utfyllende bestemmelser om tilretteleggingsplikten slik som plikt til å lagre trafikkdata i en bestemt periode nedfelles i en forskriftshjemmel.

- ➢ Videreføring av regulering vedrørende sikkerhet og beredskap. Ta inn bestemmelse som gjennomfører strategien for telesikkerhet og beredskap slik som beskrevet i St.meld. nr. 47 (2000–2001) – "Om telesikkerhet og -beredskap i et telemarked med fri konkurranse".

Nettvett reglene og nettvett.no

Nettvett.no ble opprettet i 26. april 2005 av Post- og teletilsynet på oppdrag fra Samferdselsdepartementet. PT har samarbeidet med aktører fra IKT-sektoren vedrørende nettstedets innhold, og blant bidragsyterne finner man Telenor, NorSIS, Næringslivets sikkerhetsråd, Datatilsynet og en rekke andre aktører [64]. Nettstedet retter seg både mot private samt små og mellomstore bedrifter og formidler informasjon knyttet til sikker bruk av Internett.

Blant temaene som tas opp for private brukere er nettbank og e-handel, fildeling og lynmeldinger. For bedrifter nevnes blant annet risikovurdering, sikkerhetsstrategi og hjemmekontor. Nettsiden dekker mange viktige sikkerhetsproblemstillinger ved bruk av IKT, og innholdet kvalitetssikres av PT og de andre bidragsyterne. De forskjellige problemstillingene i tilknytning til sikkerhet er forklart på en kortfattet, oversiktlig måte som personer med ikke-teknisk bakgrunn også kan forstå. I 2006 hadde nettstedet ca. 222 900 besøkende [45].

Sikkerhet og beredskap i nett

Å bidra til økt teleberedskap og sikkerhet er at av ansvarsområdene til PT. I årsmeldingen for 2006 skriver PT at de vil prioritere sikkerhets- og beredskapstiltak for Internett i økende grad.

I samsvar med ekomloven § 2-10 mottok PT i 2006 en tilskuddpost på 21,7 millioner kroner for tiltak innen telesikkerhet og beredskap. Midlene ble brukt på flere områder [45]:

- ➢ Sikre nasjonale behov for kommunikasjonsnett og -tjenester i krise- og beredskapssituasjoner gjennom avtale med Telenor.
- ➢ Dekke merkostnader ved innkjøp for opprettholdelse av sikkerhet- og beredskapstiltak. Avtale ble inngått med Telenor og NetCom. Sistnevnte ble pålagt beredskapsforpliktelser fra starten av 2007.
- ➢ Sikre samtrafikkpunktene (NIXene) for Internett i Norge. PT inngikk en avtale med UiO og USIT (Universitetets Senter for Informasjonsteknologi) om sikringen. USIT samarbeider med Universitet i Tromsø og Stavanger om etablering av nye IXer.

Det siste tiltaket er spesielt interessant. Frem til nå kun har vært én og to NIXer i drift. NIXene er de mest sentrale komponentene i infrastrukturen av den norske delen av Internett siden de er ansvarlige for å koble sammen alle større nettleverandører. Riktignok har noen

[2] Stortinget kan gi fullmakt til regjeringen for utarbeidelse av mer inngående regulering enn det en lov gir. Slik inngående regulering nedfelles i forskrifter av lovens forvalter og ikke av Stortinget, slik tilfellet er for lover. Forskrifter har derfor lavere rang enn lover.

av de største aktørene koblet seg direkte opp mot hverandre, men NIXene er likevel den viktigste kommunikasjonskanalen mellom nettleverandørene. I alt 60 Internettleverandører er koblet sammen gjennom disse to NIXene som befinner seg i vanlige lokaler på to steder i Oslo og driftes av UiO [65]. De siste to årene har trafikken på NIX mer enn tredoblet seg og antall tilkoblede har økt fra 45 til 60 [66]. Driften av NIXene finansieres gjennom en årlig tilkoblingsavgift, mens UiO bidrar med kompetanse på området.

Det finnes også andre samtrafikkpunkter som blir lokalt driftet i Trondheim (TRDIX) og Bergen (BIX). Disse IXene er svært små knutepunkter i det TRDIX og BIX bare kobler sammen henholdsvis 2 og 3 nettleverandører [66]. Planen for å bedre dagens system innebærer at det etableres fire regionale IXer under en felles organisasjon som vil ha ansvaret for alle knutepunktene. Knutepunktene skal befinne seg i Bergen, Trondheim, Tromsø og Stavanger [65]. To av de regionale IXene erstatter altså BIX og TRDIX som nå er drevet lokalt, mens det opprettes to nye IXer i Tromsø og Stavanger. Planen er at utvidelsen skal skje i løpet av 2007. I Tromsø og Trondheim er det meste klart per 14. mai 2007 mens det ennå pågår arbeid vedrørende Bergen og Stavanger [67].

Regionale IXer vil gjøre det mulig for Internettleverandører å utveksle data lokalt, istedenfor å sende de via Oslo. Dette vil bedre forsinkelse og jitter [3] hvilket vil heve kvaliteten for tjenester som VoIP og andre sanntidstjenester. Arbeidet med regionale IXer er inspirert av modellen til svenske NetNod som er bygget på regionale knutepunkter [65].

Foruten NIXene, BIX og TRDIX eksisterer det i dag også et antall forbindelser til utlandet som kan begrense skaden dersom en IX skulle gå ned. Dette har aldri skjedd så det er vanskelig å vite nøyaktig hva som vil skje i et slikt tilfelle [67]. Man antar at de fleste Internettilbyderne har noe reservekapasitet på de øvrige forbindelsene, men et ytelsestap vil nok merkes dersom en eller begge NIXene går ned [67]. Spesielt gjelder dette rundreisetid for trafikken, siden neste samtrafikkpunkt da kanskje befinner seg i Stockholm eller Amsterdam.

Å øke redundansen ved å gå bort fra dagens stjernetopologi i infrastrukturen er et viktig arbeid som vil øke motstandsdyktigheten ved problemer, angrep eller på annen måte bortfall av en IX. Samtidig vil man redusere forsinkelse, jitter og spare båndbredde i hovedtrafikkårene mellom Oslo og andre store byer.

Annet sikkerhetsrelatert arbeid

Annet sikkerhet- og beredskapssrelaterte arbeider PT jobber eller har jobbet med med inkluderer følgende:

Kartlegging av kritisk infrastruktur — Et internt prosjekt startet i 2004 har hatt dette som oppgave. Prosjektets oppgave er å definere sikkerhetskrav til forskjellige deler av nettet gjennom å finne de mest kritiske fysiske og logiske delene av infrastrukturen. I 2006 rettet kartleggingen seg mot transportnettene, og i 2007 skal tjenestenettene for mobiltelefoni, fasttelefoni, Internett/datatjenester og overføringskapasitet kartlegges [45].

Risiko- og sårbarhetsanalyser av kritisk infrastruktur — PT foretar ROS-analyser for å utarbeide konkrete tiltak som kan virke risiko- eller sårbarhetsreduserende [68].

[3] Variasjon i forsinkelse.

Samarbeid med kraftbransjen — PT arbeider for at vitale punkter i kommunikasjonsnett skal ha en prioritert og sikker kraftforsyning [68].

Nasjonal autonomi — PT gjennomførte i samarbeid med FFI en studie om temaet i 2004 og 2005. Prosjektet Teleberedskap i fritt konkurransemarked (TIFKOM) anbefalte at PT burde stille nasjonal autonomi som krav til operatørene[4]. FFI anbefalte i stedet en annen løsning: "Nasjonal backup: Opprettholdelse av nasjonale backupløsninger på driftssiden for noen operatører". PT sluttet seg til denne konklusjonen og fikk i 2006 bevilget ca. 21 millioner kroner for å sette planen ut i live [18, kap. 10.1.4.2]. Utvalget for kritisk infrastruktur (NOU 2006: 6) støttet også denne konklusjonen, og understreket at å gjennomføre planen per idag er kostnadsmessig overkommelig, men at dette neppe vil være tilfelle i fremtiden.

Prioritet i mobilnettet — På bakgrunn av St.meld. nr. 47 (2000-2001) – "Telesikkerhet og -beredskap i et telemarked med fri konkurranse" har PT i samarbeid med NetCom og Telenor Mobil utført en forundersøkelse om temaet. Det ble anbefalt å innføre en "always on" prioritetsmekanisme basert på anerkjente standarder i både Telenor Mobil og NetCom sine nett. Videre ble det anbefalt at antall prioriterte brukere blir begrenset til ca. 5000, at operatørene pålegges å åpne for nasjonal roaming for de prioriterte brukerne og at prioritetsfunksjonen ikke må påvirke nødandrop negativt. Ifølge årsmeldingen for 2006 er forventet kostnad en engangsinvestering på ca. 20 millioner kroner samt 2 millioner kroner i årlig drift [45]. DSB har arbeidet med å identifisere brukerne som skal gis prioritet. Ifølge årsmeldingen utreder Danmark og Sverige også muligheten vedrørende prioritering i mobilnett, og PT har delt sine erfaringer med svenske PTS.

Lov om elektroniske signaturer (esignaturloven) — PT er ansvarlig for forvaltning av esignaturloven som trådde i kraft i 2001. Med hjemmel i denne loven fører PT tilsyn med utstedere av såkalte kvalifiserte sertifikater [5] for digital signering (eSignatur) og identifisering (eID). I utgangen av 2006 var det registrert totalt 9 slike utstedere [45]. PT var også involvert som observatør i SEID prosjektet (Samarbeidsprosjekt om eID og eSignatur), hvis mål var å tilrettelegge for bruk av PKI. En rekke aktører, offentlige såvel som private, deltok i dette prosjektet som ble avsluttet i 2005 [70].

Samarbeid med andre land og organisasjoner — PT samarbeider med NATO, ITU og ETSI [6] om standardisering. PT er aktive også i andre internasjonale fora. Det samarbeides også med de andre nordiske landene for å finne løsninger på felles problemstillinger slik som introduksjon av en prioritetsfunksjon i mobilnett.

Robusthet mot feil og angrep i Internett — PT har etablert et forum (Internettgruppen) for aktører og myndigheter hvor man kan diskutere robusthet i Internett. Primært består forumet av Internettilbydere og andre som direkte håndterer opp-

[4] Nasjonal autonomi innebærer mulighet til å kommunisere innenfor landets grenser uten hjelp av utenlandske operatører.

[5] Kvalifiserte sertifikater kan kun utstedes av virksomheter som godkjennes av PT. Disse virksomhetene må følge spesielt strenge krav som følge av blant annet esignaturloven. En fordel med slike sertifikater i internasjonal sammenheng er at regelverket for kvalifiserte sertifikater er tilnærmet likt over hele Europa, noe som letter bruken av slike sertifikater på tvers av landegrensene [69].

[6] International Telecommunication Union og European Telecommunications Standards Institute.

gaver i tilknytning til Internett [25]. En egen Abusegruppe er også etablert som en arbeidsgruppe. Videre har Samferdselsdepartementet bedt PT om å jobbe for at Internettilbyderne skaper en bransjenorm for sikkerhet. Dette arbeidet er igangsatt hos PT [25].

5.3 Koordineringsutvalget for informasjonssikkerhet (KIS)

5.3.1 Om organisasjonen

KIS ble opprettet i mai 2004 av Fornyings- og administrasjonsdepartementet (FAD) på bakgrunn av et foreslått tiltak i Nasjonal strategi for informasjonssikkerhet 2003. Før denne opprettelsen eksisterte det andre råd som var involvert i IT-sikkerhet, deriblant Rådet for IT-sikkerhet i statsforvaltningen (RITS, 1996–1998), og Forum for IT-sikkerhet (FITS, 2000–2004) [46]. KIS kan anses å være en videreføring av disse to koordineringsutvalgene.

KIS skal fungere som et "tverrsektorielt koordineringsorgan for regelverksforvaltere og tilsynsmyndigheter med ansvar innen informasjonssikkerhet" [46]. Utvalgets målsetning er "å samordne tilsynsvirksomhet, videreutvikle IT-sikkerhetsregelverket og få til en samordnet håndheving av IT-sikkerhetsbestemmelser for å samordne etterlevelse hos brukerne" [46]. Ved opprettelsen ble KIS pålagt å følge opp Nasjonal strategi for informasjonssikkerhet. Utvalget har ingen myndighet til å fatte vedtak, men bidrar med råd og veiledning for å utvikle strategien.

Utvalget ledes av FAD, har nestleder fra JD og sekretariat i NSM. Medlemmene av utvalget består av representanter fra sentrale departementer og direktorater på IKT-sikkerhetsområdet [46].

5.3.2 Arbeid

Majoriteten av aktiviteten i KIS foregår i arbeidsgrupper som nedsettes etter behov. Tabell 5.1 gjengir de arbeidsgruppene som har vært nedsatt av KIS så langt. De to første gruppene i tabellen har ikke avsluttet sitt arbeid ennå.

Arbeidsgrupper	
Samarbeidsgruppe for regelverk for informasjonssikkerhet (SARI)	2007–
Arbeidsgruppe for klassifisering og beskyttelse av informasjon (KOBI)	2007–
Arbeidsgruppe for utarbeidelse av Nasjonal strategi for informasjonssikkerhet 2007–2010	2006–2007
Arbeidsgruppe for videreføring av nasjonal strategi for informasjonssikkerhet	2006

Tabell 5.1: *Arbeidsgrupper nedsatt av KIS.*

Samarbeidsgruppe for regelverk for informasjonssikkerhet (SARI)

SARI har et mandat som består av fire oppgaver: 1) identifisere inkonsekvent begrepsbruk i terminologi for IKT-sikkerhet og undersøke hvordan dette kan motvirkes, 2) lage en oversikt over krav som stilles til styringssystemer i regelverkene på informasjonssikkerhetsområdet, og utarbeide forslag til hvordan kravene kan oppfylles gjennom ett felles styringssystem, 3) fremme forslag til hvordan informasjon om regelverk på informasjonssikkerhetsområdet best kan formidles til virksomheter og 4) gjennomgå og eventuelt fremme forslag til forenkling i regelverk for behandling av fortrolig/taushetsbelagt informasjon [46]. Arbeidsgruppen har levert rapport for første del av mandatet om identifisering av inkonsekvent begrepsbruk.

Arbeidsgruppe for klassifisering og beskyttelse av informasjon (KOBI)

Mandatet til KOBI gir gruppen fire oppgaver [25]: "1) gi en kort oversikt over nasjonale og internasjonale standarder og sertifiseringsordninger for klassifisering og beskyttelse av informasjon, 2) liste opp relevant lovverk som stiller krav til beskyttelse av sensitiv informasjon, 3) foreslå en fremgangsmåte for gradering av informasjon i klasser og 4) utarbeide forslag til hvordan beskytte informasjon i de ulike klassene." Arbeidsgruppen skal etter planen levere sin rapport i september 2007 [46].

Arbeidsgruppe for utarbeidelse av Nasjonal strategi for informasjonssikkerhet 2007–2010

Hensikten med arbeidsgruppen har vært å utvikle en nasjonal strategi for informasjonssikkerhet som avløser strategien fra 2003. Strategien er sektorovergripende og representerer en helhetlig tilnærming til IKT-sikkerhetsarbeidet [46]. På grunn av stadige endringer på området anbefales det at strategien har et tidsperspektiv på maksimalt 3 år.

Arbeidsgruppen har ferdigstilt sitt arbeid og leverte rapporten til FAD 15. mars 2007. Den endelige strategien offentliggjøres etter behandling av departementet.

Arbeidsgruppe for videreføring av nasjonal strategi for informasjonssikkerhet

Denne gruppen hadde følgende mandat: "... å vurdere Nasjonal strategi for informasjonssikkerhet 2003 i forhold til mål, utvikling og trender, og en vurdering av om det var nødvendig å oppgradere dokumentet og hva som eventuelt burde gjøres" [46].

Arbeidsgruppen anbefalte i hovedsak å lage en ny strategi med utgangspunkt i strategien fra 2003. Det ble videre anbefalt at en arbeidsgruppe underlagt KIS burde utvikle strategien, og at privat sektor burde involveres. Tiltakene i strategien fra 2003 burde også utkvitteres i FADs stortingsmelding om IKT-politikk [46].

Rapportens innhold diskuteres mer dyptgående i kapittel 4.1 om Nasjonal strategi for informasjonssikkerhet.

5.4 Norges forskningsråd (NFR)

5.4.1 Om organisasjonen

Norges forskningsråd (NFR) er en organisasjon som gir råd i forskningspolitiske spørsmål og er ansvarlig for å fordele 5,4 milliarder kroner årlig til forskningsformål [71].

Hva som skal forskes på kommer til uttrykk i departementenes årlige tildelingsbrev til NFR. I disse beskrives krav, ønsker og budsjettallokering fra departementenes side. Etter NFR er informert om disse sakene følger som regel en dialog og møysommelig budsjettforslagsprosess mellom partene [72]. Regjeringen har mulighet til å pålegge NFR å gjennomføre større satsinger, men dette skjer sjelden uten dialog. Vanlig prosedyre er at departementene bearbeider budsjettforslagene fra NFR og at aktuelle temaer drøftes internt i Regjeringen før det endelige budsjettet fastsettes. Ofte kommer også næringslivet og ulike forskningsmiljøer med forslag til NFR. Disse forslagene behandles av NFR og blir eventuelt fremmet som forslag til satsingsområde i budsjettforslagene [72].

De forskningspolitiske retningslinjer fra Regjeringen og Stortinget som NFR skal ta hensyn til kommer altså som regel til syne gjennom departementenes budsjettproposisjoner. Et annet dokument som er med på å tegne opp retningslinjene for forskning er Forskningsmeldingen. Denne legges som regel frem hvert fjerde år. Det er en stor grad av tverrpolitisk enighet angående innholdet i Forskningsmeldingen, og den nåværende regjeringen Stoltenberg II så ingen grunn til å endre innholdet i meldingen som ble lagt frem av den forrige regjeringen (Bondevik II) [72].

NFR er delt inn i tre fagdivisjoner: Vitenskap, Store satsinger og Innovasjon. Divisjonen "Store satsinger" har som oppgave å "identifisere og utrede nasjonale strategiske forskningsbehov, og arbeide for å bygge opp kunnskap og forskningskapasitet på prioriterte områder" [71]. Satsingen "Store programmer" ligger under denne divisjonen, og det er med dette programmet NFR har gitt forskning på informasjonssikkerhet et løft de siste årene ved etableringen av programmet IKT sikkerhet og sårbarhet (IKT SoS). Andre store programmer slik som VERDIKT og SAMRISK har også bevilget visse midler til prosjekter med fokus på IKT og sikkerhet, men IKT SoS fokuserte utelukkende på informasjonssikkerhet. I slike store forskningsprogrammer innvilges støtte til et antall ulike prosjekter basert på søknad og overensstemmelse med programmets målsetning.

5.4.2 Forskningsprogrammer

Tabell 5.2 viser tre ulike store satsinger som NFR har utført. Av disse er det førstnevnte program IKT SoS som er mest relevant for informasjonssikkerhet da det i programmet fokuseres utelukkende på dette temaet. Alle de tre programmene blir diskutert i dette kapittelet.

Forskningsprogrammer	**Periode**
IKT sikkerhet og sårbarhet (IKT SoS)	2003–2007
Kjernekompetanse og verdiskaping i IKT (VERDIKT)	2005–2014
Samfunnssikkerhet og risiko (SAMRISK)	2006–2010

Tabell 5.2: *Forskningsprogrammer med relevans for IKT og sikkerhet.*

IKT sikkerhet og sårbarhet (IKT SoS) 2003–2007

IKT SoS ble etablert i 2003 og formelt avsluttet i 2007. Programmet ble startet på oppdrag fra Nærings- og handelsdepartementet med en målgruppe bestående av norske universiteter, høgskoler og forskningsinstitutter. Direkte næringslivsdeltakelse var begrenset på grunn av prosjektformen. Totalt budsjett for programmet var 59 millioner kroner [73]. Grunnen til at IKT SoS ble opprettet var at utfordringene med IKT-sikkerhet ble identifisert i et grunnleggende program om IKT (IKT 2010). Signaler fra NFR om utfordringene vedrørende IKT-sikkerhet resulterte i at temaet ble fanget opp i Regjeringens e-handlingsplan for deretter å lede til en anmodning fra NHD om å utvikle et eget program om IKT-sikkerhet og sårbarhet [72].

Målsettingen med IKT SoS var "å bygge opp kompetanse på spørsmål rundt IKT sikkerhet og sårbarhet på områder som er viktige for Norge og hvor det er behov for å styrke tilgangen på kunnskap og kompetanse for næringsliv og offentlige virksomheter" [73]. Regjeringens begrunnelse for å starte et slikt program var at de ville "bidra til tilliten i elektronisk samhandling og til å utvikle en sikkerhetskultur i samfunnet" [73]. Ønsket om å starte et forskningsprogram for IKT-sikkerhet stammet blant annet fra Sårbarhetsutvalgets anbefalinger, Sårbarhetsmeldingen (St.meld. 17 (2001–2002)) og Nasjonal strategi for informasjonssikkerhet [73].

Alle økonomiske midler bevilget til programmet ble i løpet av 2003 og 2004 fordelt på innvilgede prosjekter. Totalt fikk 22 prosjekter innvilget støtte under programmet: ti prosjekter i 2003, seks prosjekter i 2004 og nye seks prosjekter i 2005 [73]. Etter 2005 ble ingen nye utlysninger foretatt, men arbeid pågikk i flere av prosjektene til utgangen av 2007. Faktisk er et antall prosjekter fortsatt ikke ferdigstilte per dags dato, men de forventes å være ferdige i løpet av 2008 [47].

Totalt ble 15 PhD stipendiater og 2 post doc stipendiater finansiert av programmet. I tillegg ble det finansiert utenlandsopphold for 3 forskere [73].

Blant prosjektene som ble finansiert av IKT SoS, var følgende [73]:

BAS5 Metodikk for risiko- og sårbarhetsanalyse av IKT-infrastruktur (FFI)

SWAP Sikkerhet i nettbanker (UiB)

ENFORCE Administrasjon og etablering av policy for tillit mellom systemer (SINTEF/UiO)

AMBASEC og IRMA Tallfeste virkningen av forbedrede rutiner for hendelseshåndtering (HiA/SINTEF)

Noen prosjekter, herunder BAS5, mottok også midler fra andre aktører enn NFR.

Kjernekompetanse og verdiskaping i IKT (VERDIKT) 2005–2014

VERDIKT ble etablert i 2005 og skal avsluttes i 2014. Et av hovedmålene med prosjektet er å "skape innovasjon og økt verdiskaping i norsk IKT-næring samt nærings- og samfunnsliv forøvrig" [74]. VERDIKT hadde i 2006 et budsjett på 50 millioner kroner. Budsjettet for 2007 er på 150 millioner kroner og VERDIKT jobber for en opptrapping av budsjettet til 500 millioner kroner årlig (for 2011-2014). Hvis dette skulle gå igjennom vil programmet disponere i overkant av 3,1 milliarder i sin levetid. Det gjenstår likevel å se om en så drastisk økning vil få gjennomslag. Et argument for å trappe opp satsingen på VERDIKT

er at andelen av NFRs samlede IKT-bevilgninger, selv med den foreslåtte økningen for budsjettet i VERDIKT, fortsatt vil ligge under den tilsvarende andelen for IKT i EUs 7. rammeprogram for forsknings [74].

VERDIKT programmet skal ha prosjekter innen 4 fagområder [74]:

- Brukergrensesnitt, informasjonsforvaltning og programvareteknologi
- Kommunikasjonsteknologi og infrastruktur
- Sikkerhet, personvern og sårbarhet
- Samfunnsmessige, økonomiske og kulturelle utfordringer og muligheter

Informasjonssikkerhet utgjør altså bare en liten del av programmets fokus. I 2005 innvilget VERDIKT støtte til 7 prosjekter, og disse hadde oppstart i begynnelsen av 2006 [74]. Ett av disse prosjektene var relatert til informasjonssikkerhet og hadde tittelen SWACOM – Secure and reliable Wireless and Ad-hoc COMmunications. Ifølge prosjektplanen for SWACAOM vil tre PhD stipendiater og én annen forskerstilling bli finansiert gjennom VERDIKT. Det gjenstår å se hvor mange andre prosjekter relatert til informasjonssikkerhet vil bli finansiert gjennom forskningsprogrammet.

Samfunnssikkerhet og risiko (SAMRISK) **2006–2010**

SAMRISK programmet ble etablert i 2006 og er således fortsatt i en innledende fase. Programmet er planlagt avsluttet i 2010. Programplanen refererer til Sårbarhetsutvalget og Infrastrukturutvalget i sin argumentasjon for opprettelsen av SAMRISK. Samlet budsjett for programmets periode er ca. 50 millioner kroner, altså omtrent 10 mill. kr. årlig. Styret arbeider med å øke midlene til programmet.

Hovedmålet for SAMRISK er tredelt [75]:

- Øke kunnskap om trusler, farer eller sårbarhet
- Forebygge uønskede hendelser
- Styrke krisehåndtering

Programplanen angir enkelte generiske problemstillinger som ønskes belyst [75]:

- Teknologier i samspill med samfunn, organisasjon og mennesket
- Risikobildet, sårbarhet og samfunnets risikotoleranse
- Politikk, styring og reguleringer
- Sikkerhet og samfunn
- Krisehåndtering og risikokommunikasjon

Programstyret anså visse forskningsprogrammer å være relevante for SAMRISK. Et av disse relevante programmene var IKT SoS, og programstyret mente derfor at gjensidige oppdateringer og koordinering burde finne sted mellom programmene for å unngå overlapping innen spesifikke forskningstemaer. BAS5 ble nevnt som et konkret eksempel på relevant forskning for SAMRISK.

Utifra de generelle problemstillingene og programstyrets kommentarer er det svært sannsynlig at prosjekter under SAMRISK vil røre ved problemstillinger som er relevante for informasjonssikkerhet, IKT-infrastruktur og sårbarhet. Det gjenstår å se i hvilket omfang SAMRISK vil ta opp slike problemstillinger.

5.5 Nasjonal sikkerhetsmyndighet (NSM)

5.5.1 Om organisasjonen

NSM er en forebyggende og defensiv sikkerhetstjeneste hvis primæransvar er å "koordinere forebyggende sikkerhetstiltak og kontrollere sikkerhetstilstanden i de virksomheter som omfattes av Sikkerhetsloven" [76]. Koordinering kan i hovedsak tolkes som å gi informasjon, råd og veiledning samt foreslå forbedrede tiltak, mens kontroll tilsvarer å drive tilsynsvirksomhet [18, kap. 7.1.1]. NSM har også andre oppgaver som følger av Sikkerhetsloven og dens forskrifter. Å utføre sikkerhetsklareringer, godkjenninger og sertifiseringer er eksempler på slike oppgaver [18, kap. 7.1.1]. Hovedoppgavene til NSM reguleres gjennom Sikkerhetsloven.

NSM ble opprettet som eget direktorat i 1. januar 2003 etter å ha fungert som stab i Forsvarets FO/S (Forsvarets overkommando/ Sikkerhetsstaben). Direktoratet er underlagt Forsvarsdepartementet administrativt og faglig sett. Forsvarsdepartementet er eneste oppdragsgiver og direktoratet rapporterer dit for alt som angår militær sektor. Direktoratet har også en faglig rapporteringslinje til Justisdepartementet for saker i sivil sektor [76]. Viktige samarbeidspartnere er Politiets sikkerhetstjeneste (PST), Etterretningstjenesten og Direktoratet for samfunnssikkerhet og beredskap (DSB). NSM holder til på Kolsås.

Saldert budsjett for NSM var i 2005 nesten 96 mill. kr. og forslaget for budsjett for 2006 var på nesten 94 mill. kr [55, Kap. 4723]. Totalt har NSM ca. 130 ansatte [76].

Viktige sikkerhetsrelaterte virksomheter som sorterer under NSM er NorCERT og VDI: Norwegian Computer Emergency Response Team og Varslingssystem for Digital Infrastruktur. SERTIT-ordningen faller også innunder NSM sitt ansvarsområde.

Sikkerhetsloven

Sikkerhetsloven, eller "Lov om om forebyggende sikkerhetstjeneste" ble vedtatt i 1998 og trådde i kraft 1. juli 2001 [26, kap. 5.1]. Loven kom på bakgrunn av av ønske om en egen lov for EOS-tjenestene. Målet med loven er å gi etterretningstjenestene en bedre organisering, skille mellom de ulike EOS-tjenestenes oppgaver og tydeliggjøre hjemler i lovverket.

En rapport ble avgitt av en interdepartemental arbeidsgruppe i mai 2002 vedrørende forslag til forskrifter om objektsikkerhet til loven. Rapporten anbefalte at Sikkerhetsloven burde endres for å inkludere de mest sentrale forskriftene i Sikkerhetsloven. En ny arbeidsgruppe ble nedsatt for å følge opp saken, men arbeidet ble stilt i bero for å avvente Infrastrukturutvalgets rapport og rapportens høring. Etter at rapporten ble avlevert til JD 5. april 2006 og den etterfølgende høringen ble avsluttet, er arbeidet med lovendringen nå gjenopptatt og forventes avsluttet i løpet av 2007 [32].

Som forvalter av Sikkerhetsloven har NSM i oppgave å identifisere og klassifisere nasjonale objekter med behov for skjerming. Formålet med loven er tredelt:

- Legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser.
- Ivareta den enkeltes rettssikkerhet.
- Trygge tilliten til og forenkle grunnlaget for kontroll med forebyggende sikkerhetstjeneste.

Det viktigste formålet med loven er å verne skjermingsverdig informasjon og objekter. Sikkerhetsloven gjelder for forvaltningsorganer i stat og kommune. Det er gjort visse unntak slik at loven også omfatter visse privatrettsligevirksomheter som ikke er forvaltningsorganer men likevel er i besittelse av skjermingsverdig informasjon eller objekter. Blant disse virksomhetene er NorSIS, Posten Norge og Telenor ASA [18, kap. 7.2.2].

Det er viktig å påpeke at Sikkerhetsloven er en sektorovergripende lov, og at sektorlovgivning presiserer nærmere de krav som skal oppfylles vedrørende beskyttelse av skjermingsverdige objekter i den enkelte sektor. Sikkerhetsloven er altså subsidiær i forhold til sektorlovgivning. Sikkerhetsloven ble kritisert av Riksrevisjonen for ikke å være detaljert nok, og det ble etterlyst utfyllende forskrifter for loven som det nå arbeides med [26, kap. 5.1].

Nedfelt i Sikkerhetsloven finner man de oppgaver som er pålagt NSM. I hovedsak skal arbeidet til direktoratet konsentreres rundt fem primæroppgaver [77]:

- Innhente og vurdere informasjon av betydning for gjennomføringen av forebyggende sikkerhetstjeneste.
- Søke internasjonalt samarbeid, herunder med andre lands og organisasjoners tilsvarende tjenester, når dette tjener norske interesser.
- Føre tilsyn med sikkerhetstilstanden i virksomheter, herunder kontrollere at den enkeltes plikter i eller i medhold av loven her overholdes, og eventuelt gi pålegg om forbedringer.
- Bidra til at sikkerhetstiltak utvikles, herunder iverksette forskning og utvikling på områder av betydning for forebyggende sikkerhetstjeneste.
- Gi informasjon, råd og veiledning til virksomheter.

Foruten å inneholde bestemmelser som definerer NSM sin rolle i sikkerhetsarbeid, inneholder loven også bestemmelser verdrørende informasjonssikkerhet, objektsikkerhet, personellsikkerhet, sikkerhetsgraderte anskaffelser og kontroll- og tilsynsordninger. Straffebestemmelser for Sikkerhetsloven er forøvrig også nedfelt i den samme loven.

5.5.2 Varslingssystem for Digital Infrastruktur (VDI)

VDI er ansvarlig for å drifte et nett av sensorer for innbruddsdeteksjon på Internett. Formålet med deteksjonssystemet er å automatisk avdekke pågående angrep på nasjonal kritisk infrastruktur og melde fra om dette til ansvarlig personell [78]. Systemet kom til på bakgrunn av erfaringer om at innmelding av hendelser fra brukere er lite effektive. Lav effektivitet skyldes blant annet at brukeren ikke alltid vet hvem han skal henvende seg og at brukeren ikke alltid vet at systemet hans er kompromittert [78].

VDI ble etablert høsten 2000 som et prøveprosjekt med forankring i EOS-tjenestene. Et nasjonalt inntrengningsdeteksjonssystem ble utviklet i samarbeid mellom private og offentlige aktører. Norges system var det første i sitt slag som ble til gjennom et samarbeid på tvers av privat og offentlig sektor. Det tverrsektorielle samarbeidet resulterte i flere responser fra utlandet hvor man vurderte å etablere slike deteksjonssystemer [78].

VDI viste seg under prøveperioden å være et nyttig verktøy, og vinteren 2003 ble det bestemt at systemet skulle opprettholdes på permanent basis. På samme tidspunkt ble det bestemt å legge VDI under NSM, og idag er VDI en seksjon i avdeling NorCERT [78].

Ansvarsområdene til staben i VDI er følgende [78]:

- Drive og videreutvikle et inntrengningsdeteksjonssystem for nasjonal kritisk infrastruktur.
- Utvikle analyseverktøy for nettverksdata.
- Utvikle rapporteringsrutiner ved detekterte hendelser.
- Oppfølging av deltagere i VDI-systemet.
- Analysere angrep og ondsinnet kode.
- Bidra til at avdelingen til enhver tid har et oppdatert IKT-trusselbilde.

For tilfredsstillende å kunne utføre oppgaver innen ansvarsområdet så har seksjonen VDI spesialkompetanse innen følgende områder [78]: inntrengingsdeteksjonssystemer, nettverksprotokoller, analyse av nettverkstrafikk, internett infrastruktur, honeypot-teknologi [7], sårbarheter og ondsinnet kode (malware).

5.5.3 Norwegian Computer Emergency Response Team (NorCERT)

NorCERT er en avdeling i NSM ansvarlig for å "forebygge alvorlige angrep mot samfunnskritisk infrastruktur og informasjon på IT siden, varsle om alvorlige angrep, trusler og sårbarheter, og koordinere responsen i forbindelse med alvorlige sikkerhetsangrep" [20].

Bakgrunnen til opprettelsen av NorCERT var erfaringer som ble gjort med VDI [20]. VDI avdekket et behov for et nasjonalt responssenter ved angrep, slik at angrepsdeteksjon kunne bli knyttet opp mot hendelseshåndtering. Prosjekt NorCERT ble følgelig startet i februar 2004, og i april 2006 ble NorCERT offentlig åpnet av Forsvarsministeren og etablert som en permanent avdeling under NSM [20]. Avdeling NorCERT holder til på Akershus festning i Oslo sentrum.

NorCERT består av to seksjoner: VDI og seksjon for hendelseshåndtering. Mens VDI identifiserer trusler og sender varsel om dataangrep, er NorCERT ansvarlig for å koordinere hendelseshåndtering av angrep mot nasjonal kritisk IKT-infrastruktur. De to seksjonene bemanner sammen Operasjonssenteret. I senteret er det til enhver minst tid tre personer. Disse personene er hendelseskoordinator, analytiker og vakthavende. Koordinatoren er hovedansvarlig og koordinerer hendelser internt og eksternt. Analytikeren gjør analyse av tekniske data med fokus på data fra interne kilder slik som VDI-sensorene. Vakthavende

[7] En honeypot er en datamaskin som er satt opp for å levere visse tjenester i den hensikt å trekke til seg hackere. Datamaskinen overvåkes med spesiell programvare slik at en angripers fremgangsmåte detaljert kan kartlegges.

foretar også analyse av kildemateriell i likhet med analytikeren, men fokuserer på eksterne kilder [20].

NorCERT/VDI har en stab på tilsammen 17 IT-sikkerhetsspesialister. I tillegg har staben et antall datakyndige vernepliktige til sin disposisjon. I alvorlige krisesituasjoner kan NorCERT forsterkes ytterligere av personer med ekspertise i IT-sikkerhet fra NSM [20]. NorCERT sine driftsutgifter er på ca. 8 mill. kr. årlig, og privat og offentlig sektor samfinansierer avdelingen. Fornyings- og administrasjonsdepartementet dekker ca. 5 mill. kr. av utgiftene, mens de resterende 3 mill. kr. dekkes av privat sektor [55, Kap. 1723]. I privat sektor er det særlig større aktører innen olje- og gass, telekom samt bank- og finansnæringen som er bidragsytere [53]. Alle virksomheter som representerer en samfunnskritisk funksjon eller har ansvar for kritisk infrastruktur får hjelp av NorCERT i en krisesituasjon, selv om de ikke er tilkoblet VDI [53].

Det er nå foreslått å flytte budsjettansvaret til FD idet FAD sitt samordningansvar kun skal gjelde *forebyggende*, tverrsektorielle tiltak [79, kap. 1.9].

NorCERTs oppgaver er følgende [20]:

- Koordinere respons på alvorlige IT- sikkerhetsangrep mot viktig infrastruktur og informasjon.
- Innhente informasjon om alvorlige sikkerhetstruende hendelser på Internett.
- Koordinere tidlig sikkerhetsoppdatering av samfunnskritiske datasystemer.
- Fokusere på deling av informasjon.
- Til enhver tid ha et oppdatert teknisk trusselbilde.
- Hjelpe frem responsmiljøer i Norge.
- Gi innspill til nasjonale beredskapssystemer og bistår beredskapsarbeidet.
- Være Norges kontaktpunkt mot tilsvarende organisasjoner i utlandet.

NorCERT samarbeider tett med NorSIS, og de to organisasjonene planlegger å gjennomføre et seminar i 2007 beregnet på IKT-sikkerhetsledere for departementer og tilsyn.

5.5.4 SERTIT

SERTIT er en offentlig sertifiseringsmyndighet for IT-sikkerhet i produkter og systemer. Eksempler på produkter som blir sertifisert er brannmurer og operativsystemer. SERTIT ble opprettet på bakgrunn av en anbefaling fra Rådet for IT-sikkerhet i 1997 [28]. Hovedhensikten med sertifiseringsmyndigheten beskrives slik: "... å dekke myndighetenes og industriens behov for en kostnadseffektiv og rasjonell sikkerhetsmessig evaluering og sertifisering av IT produkter og systemer" [15].

Forsvarets overkommando/Sikkerhetsstaben (FO/S) fikk gjennom St.prp. nr. 1 (1998–99) bevilget midler av NHD til opprettelsen [28]. NSM, tidligere kjent som Forsvarets overkommando/Sikkerhetsstaben (FO/S), har hatt ansvaret for SERTIT siden høsten 2000 [80]. Driftsutgifter har siden 2000 også blitt dekket gjennom Forsvarsdepartements budsjett. Enheten var ikke operativ før høsten 2002 og ble da etablert som sertifiseringsordning under Nasjonal sikkerhetsmyndighet [26, kap. 5.2.2].

Primæroppgaven til SERTIT er å utstede sertifikater og sertifiseringsrapporter. Videre har SERTIT disse oppgavene [15]:

- Utforme rammevilkår og regler for sertifisering av IT-sikkerhet i Norge, og påse at reglene følges av alle parter.
- Godkjenne private firma som evalueringsinstanser og føre tilsyn med disse.
- Føre tilsyn med evalueringsprosessene.

Viktige målsetninger for SERTIT er [15]:

- Styrke IT-sikkerheten i offentlig sektor.
- Skape tillit til e-handelsløsninger og annen kommunikasjon nasjonalt og internasjonalt.
- Bidra til å gjøre Norsk IT-industri mer konkurransedyktig overfor utlandet.
- Gjøre det enklere for anskaffer gjennom tillit til at forhåndsdefinerte sikkerhetskrav er tilfredsstilt.

SERTIT representerer Norge internasjonalt ved deltagelse i forumet "Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security (CCRA)". CCRA arbeider for at internasjonale sertifikater skal følge standarder som spesifisert i Common Criteria (CC, ISO 15408). Kun elleve land, inkludert USA, Storbritannia, Frankrike og Tyskland, har rett til å utstede slike sertifikater per idag [15].

Sertifiseringsmyndigheten har 4 ansatte og er underlagt en styringskomité som fører tilsyn med SERTIT. Styringskomitéen består av representanter fra både offentlig og privat sektor. Blant representantene er Forsvarsdepartementet, Justis- og politidepartementet, Nærings- og handelsdepartementet, Datatilsynet og NSM. Det er også etablert et fagråd i tilknytning til SERTIT med representanter fra en rekke bedrifter.

5.6 Norsk senter for informasjonssikring (NorSIS)

5.6.1 Om organisasjonen

Senter for informasjonssikring (SIS) ble etablert etter oppfølging av et konkret tiltak i Sårbarhetsutvalgets rapport. Senteret ble etablert som et prøveprosjekt i 2004 i regi av NHD og lagt til SINTEF i Trondheim. Prøvetiden ble forlenget ut 2005 og senteret ble permanent etablert 01.01.2006 under navnet NorSIS. Senteret befinner seg nå ved Gjøvik kunnskapspark.

Det opprinnelige mandatet til SIS var å "framskaffe et helhetlig bilde av truslene mot norske IT-systemer basert på innrapportering av hendelser fra norske virksomheter" [26, kap. 5.1.3]. Denne oppgaven var tenkt å relateres til VDI sin automatiske innsamling av overvåkningsdata fra IKT-infrastruktur. Mandatet til NorSIS ble etterhvert endret og fikk fokus på bevisstgjøring rundt informasjonssikkerhet i samfunnet generelt. Senteret skal bevisstgjøre om trusler, opplyse om tiltak og drive holdningskapende arbeid vedrørende informasjonssikkerhet.

Som målgruppe fokuserer NorSIS spesielt på små og mellomstore bedrifter i privat sektor og offentlig sektor, herunder kommunesektoren. Forøvrig er senterets mål at også allmennheten skal ha nytte av det i så stor grad som mulig.

NorSIS har et årlig budsjett på 6 mill. kr. og en bemanning på fire personer. Senteret mottar rundt 4 mill. kr. årlig gjennom FAD sitt budsjett, mens de resterende 2 millionene dekkes gjennom bidrag fra private aktører.

Av viktige samarbeidspartnere nevnes KiNS og NorCERT/VDI.

5.6.2 Arbeid

NorSIS arbeider for bevisstgjøring rundt informasjonssikkerhet mot et generelt publikum. Dette inkluderer offentlig og privat sektor såvel som privatpersoner. For eksempel samarbeider NorSIS med finansnæringen om holdningsskapende arbeid, men senteret arbeider også mot forbrukerne, for eksempel bankkunder, slik at de bedrer sine rutiner. Innen offentlig sektor jobber NorSIS mye mot kommunesektoren, herunder rådmenn i kommuneadministrasjonen [9]. NorSIS og Datatilsynet besøkte et stort antall kommuner sammen i 2006 for å undersøke samt bidra til kommunesektorens arbeid med informasjonssikkerhet [9].

NorSIS har gjennomført flere tiltak for å øke bevisstgjøringen rundt informasjonssikkerhet i samfunnet generelt. Blant annet har senteret gjennomført flere informasjonskampanjer. Sammen med Post- og teletilsynet og andre private aktører har senteret gjennomført Nasjonal sikkerhetsdag tre ganger siden 2005.

NorSIS lanserte en sikkerhetsskole på Internett i samarbeid med VG, og har også rettet fokus mot barn og ungdom gjennom programmet Pysj Pop Baluba på NRK. Tilsammen er det her laget åtte ulike innslag om forskjellige temaer som er blitt sendt lørdager på NRK. NorSIS har også bidratt til et innslag i Forbrukerinspektørene vedrørende sikkerhet og nettbanker [9].

TV og Internett er de to viktigste mediene for å nå allmennheten, og informasjon gjennom disse kanalene er derfor et viktig tiltak i å drive bevisstgjøring mot allmennheten.

En undersøkelse gjort av Symantec i perioden juli 2006 til desember 2006 viste at Norge er blant de fremste angrepsplattformene i verden [38]. Det at Norge havnet så høyt oppe på listen kan delvis tilskrives at antallet datamaskiner i Norge er svært høy og at mange har bredbånd, men en stor del kan høyst sannsynlig tilskrives manglende bevissthet rundt informasjonssikkerhet. Denne undersøkelsen understreker viktigheten av å gjennomføre tiltak som effektivt kan øke bevisstheten rundt informasjonssikkerhet hos allmennheten.

5.7 Utdannings- og forskningsinstitusjoner

I dette delkapittelet presenteres enkelte utdannings- og forskningsinstitusjoner med aktiviteter innen informasjonssikkerhet. Det er forsøkt å gi en viss oversikt over primært universiteter og høyskoler i Norge som arbeider med informasjonssikkerhet. Denne oversikten over utdannings- og forskningsinstitusjoner er på ingen måte detaljert og komplett, men gir et grovt bilde over noen sentrale aktører på området.

Per idag eksisterer det utdanning i informasjonssikkerhet på bachelor og masternivå på to ulike utdanningsinstitusjoner i Norge. Disse er Norges teknisk-naturvitenskapelige universitet (NTNU) og Høgskolen i Gjøvik (HiG). Det ses da bort fra ulike studier relatert

til mer matematiske og tradisjonelle fag som kryptografi, samt studier som inkluderer informasjonssikkerhet som et sideordnet emne men som ikke fokuserer på det.

Tabell 5.3 gir en oversikt over institusjonene som tilbyr utdanning i informasjonssikkerhet på bachelor- eller masternivå.

Utdanningsinstitusjon	Grad	Varighet	Etablert
NTNU	Master/Siv.ing. i kommunikasjonsteknologi med spesialisering i informasjonssikkerhet	5 år	–
NTNU	Nordisk master i informasjonssikkerhet (NordSecMob)	2 år	2006
HiG	Bachelor i informasjonssikkerhet	3 år	2005
HiG	Master i informasjonssikkerhet	2 år	2002

Tabell 5.3: *Utdanningsinstitusjoner som tilbyr studier i informasjonssikkerhet på bachelor- eller masternivå.*

NTNU

NTNU tilbyr utdanning i informasjonssikkerhet på master- og doktorgradsnivå. Mer presist tilbys mastergrad i kommunikasjonsteknologi (eller datateknikk) med spesialisering/fordypning i informasjonssikkerhet.

To mastergrader finnes ved universitet som er relevant for informasjonssikkerhet. Den første er master i kommunikasjonsteknologi med spesialisering i informasjonssikkerhet. Dette er et femårig studium, men toårig påbygning kan også gjennomføres for ingeniører som søker om opptak. Det har ikke lyktes å få tak i årstallet for opprettelsen av denne spesialiseringen. Det som derimot er sikkert er at de første prosjekt- og hovedoppgavene innen sikkerhet ved NTNU ble skrevet ved Institutt for teleteknikk, faggruppe Telematikk midt på 1980-tallet [81]. Videre er det klart at PhD undervisning og -forskning innen sikkerhet ble etablert tidlig på 1990-tallet [81].

Det siste tilskuddet ved NTNU innen informasjonssikkerhet, Master's Programme in Security and Mobile Computing (NordSecMob), er et studium over 2 år og et supplement til den første mastergraden. NordSecMob er et samarbeid mellom følgende fem nordiske institusjoner [82]: Helsinki University of Technology (TKK) i Finland, Danmarks Tekniske Universitet (DTU), Kungliga Tekniska högskolan (KTH) i Sverige, NTNU og University of Tartu (UT) i Estland.

Man kan få støtte gjennom Erasmus Mundus programmet når man tar mastergraden NordSecMob. Det kreves at man tilbringer minimum ett av de to årene på et annet universitet enn universitet i hjemlandet. Programmet startet høsten 2006 og skal opprettholdes i minst 5 år [82].

NTNU har et eget program for utdanning og forskning for informasjonssikkerhet. Programmet er et samarbeid mellom instituttene for telematikk, datateknikk, matematikk, elektroteknikk og industriell økonomi og teknologiledelse. Målet med programmet er å avdekke IKT-sårbarhet på et strategisk nivå [83]. I 2005 hadde programmet totalt 13 PhD stipendiater, hvorav 7 var fra Institutt for telematikk. I årsmeldingen for 2006 var antallet

PhD stipendiater og andre forskere totalt rundt 26 stykker. Det er 2 professorater knyttet til informasjonssikkerhet ved NTNU [16].

HiG

Masterstudiet ved HiG utføres ved gruppen for informasjonssikkerhet NISlab (Norwegian Information Security laboratory). NISlab er en del av Bluelightnettverket og samarbeider også med Universitet i Oslo. Opprettelsen av bachelor- og mastergraden i informasjonssikkerhet har primært vært et resultat av mangel på kompetanse på området, samt at næringslivet har etterspurt denne type utdanning [23].

NISlab mottok i perioden 2003–2007 ca. 10 mill. kr. fra Norges forskningsråd (NFR), altså rundt 2,5 mill. per år [23]. Rundt 2 av disse 10 millionene kom gjennom forskningsprogrammet IKT SoS og NFR. Alle 10 millionene er indirekte eller direkte gitt gjennom NFR [23]. NISlab mottar i dag ingen midler fra næringslivet, men mottok flere millioner kroner fra blant annet Telenor under etableringen av mastergraden for informasjonssikkerhet [9]. Bidragene kom som et resultat av at næringslivet etterspurte og hadde et stort behov for kompetanse på området.

I mars 2007 hadde NISlab 4 PhD stipendiater og 1 post doc stilling besatt. Tilsammen disponerer NISlab 15 årsverk, hvorav 10 er avsatt innen ordinært budsjett for forskning [23]. Det er 4 professorater knyttet til informasjonssikkerhet ved NISlab/HiG [16].

Det er verdt å kommentere en forskjell mellom den førstnevnte (femårige) mastergraden ved NTNU og mastergraden ved HiG. Sivilingeniørstudiet ved NTNU har tradisjonelt hatt en bred fagprofil med vekt på realfag som matematikk de to første årene. I de siste årene på studiet er det også lagt opp til at studentene skal tilegne seg bredde i sin kompetanse, selv om det blir et økt fokus på spesialisering. Denne brede fagsammensetningen er bevisst og i tråd med ånden bak sivilingeniørstudiet. I mastergraden på HiG handler tilnærmet alle emnene om ulike fordypninger i informasjonssikkerhet. En viktig forskjell mellom NTNU og HiG sin mastergrad er derfor at graden ved NTNU fokuserer på bredde og inkluderer mange andre emner enn informasjonssikkerhet de to siste årene, mens graden ved HiG er meget spesialisert og gir dertil en bedre dybde i informasjonssikkerhet på grunn av en annen sammensetning av emnene.

Andre relevante utdanningsinstitusjoner

Høgskolen i Agder (HiA)

HiA tilbyr femårig og toårig master i informasjons- og kommunikasjonsteknologi (IKT) med spesialisering i blant annet sikkerhet. Temaer i denne spesialiseringen inkluderer informasjonssikkerhet, SMART-Card-teknologi og sikkerhet i organisasjoner [84]. Kandidaten har under tvil valgt å ekskludere denne utdanningen fra tabell 5.3 fordi spesialiseringen primært omhandler *sikkerhet* og ikke bare informasjonssikkerhet.

Det finnes 2 professorater innen informasjonssikkerhet tilknyttet HiA [85]. Videre er det 4 PhD stipendiater og 2 post doc stipendiater ved høyskolen som arbeider med informasjonssikkerhet. Sivilingeniør-/mastergraden ble opprettet i 2005 og da først og fremst som et ledd i høyskolens søknad om akkreditering for doktorgrad [85].

Universitetet i Tromsø

I Tromsø tilbys det en bachelorgrad i datasikkerhet. Graden fikk dette navnet i 2004 [24]. Før den tid eksisterte et bachelorstudium som het Matematikk med informatikk og som kom med Kvalitetsreformen i 2003 [24]. Før Kvalitetsreformen inngikk forøvrig mange av emnene i de mulighetene den gamle cand.mag. graden ga [24].

Bachelorstudiet i datasikkerhet fører fram til en bachelorgrad i realfag. Studentene kan etter bachelorgraden ta videre utdanning med 2-årig masterstudium i matematikk, studieretning datasikkerhet eller masterstudium i informatikk [86]. Både bachelorgraden i datasikkerhet og mastergraden i informatikk med spesialisering datasikkerhet fokuserer på de matematiske emner som danner grunnlaget for kryptografi [86,87].

Det var ikke mulig å få tak i informasjon om antall forskere med informasjonssikkerhet som fagfelt da kandidaten var i kontakt med UiT.

Universitetet i Bergen (UiB)

Ved UiB tilbys det mastergrad i informatikk med studieretning kodeteori og kryptografi. Universitetet har også en sterk forskningsgruppe for fagfeltet kodeteori og kryptografi som består av 3–4 professorer med permanent tilknytning til universitetet, 2 andre professorer (adjunkt), 1 post doc samt 4 PhD stipendiater [88].

Kodeteori har vært et forskningsemne ved UiB siden 1970-tallet [88]. Gjennom en evaluering igangsatt av NFR i 1992 ble det konkludert med at faggruppen for kodeteori og kryptografi ved UiB hadde publisert flest artikler (27) i internasjonale tidsskrifter av alle informatikkgruppene ved Norges universiteter i perioden 1988–1992 [88].

Universitetsstudiene på Kjeller (UniK)

Universitetsstudiene på Kjeller tilbyr master- og doktorgradsstudier i samarbeid med blant annet UiO og NTNU. Det tilbys ingen bachelor- eller mastergrad i informasjonssikkerhet ved UniK, men det undervises i enkelte sikkerhetsrelaterte emner på mastergradsnivå, herunder kryptografi, sikkerhet i distribuerte systemer samt sikkerhet i operativsystemer og programvare [89].

Forskningsinstituttene FFI og Telenor Forskning og Utvikling (TFoU) er to viktige samarbeidspartnere for UniK, og forskere fra disse instituttene veileder de fleste studentene ved UniK. I tillegg foreleser forskere ved disse instituttene mange av emnene [89].

UNIK har en forskningsgruppe ved navnet "Communication group" for IKT som blant annet består av en gruppe innenfor informasjonssikkerhet. Denne gruppen dekker ulike interesseområder, deriblant grunnleggende kommunikasjonssikkerhet, kryptografi, autentisering og sikkerhet i ad-hoc nettverk [89].

Et større prosjekt innen informasjonssikkerhet som UniK er involvert i er SWACOM. Prosjektet omhandler sikkerhet i trådløse ad-hoc nettverk og er et samarbeid mellom flere aktører, deriblant Telenor FoU, FFI, og Kongsberg gruppen [89]. Prosjektet har fått støtte fra Norges forskningsråd.

Det var ikke mulig å få tak i informasjon om antall forskere med informasjonssikkerhet som fagfelt da kandidaten var i kontakt med UniK.

Andre forskningsinstitusjoner

FFI er, som omtalt i kapittel 5.1, en viktig aktør for forskning for IKT og samfunnets sårbarhet. Spesielt har forskningen gjennom BAS prosjektene vært av stor betydning for sivil såvel som militær sektor.

Stiftelsen for industriell og teknisk forskning (SINTEF) er Skandinavias største uavhengige forskningsorganisasjon. SINTEF er organisert i konsernområder hvorav ett av disse er SINTEF IKT. Under SINTEF IKT finnes avdeling for systemutvikling og sikkerhet med faggruppene for informasjonssikkerhet og systemsikkerhet [90].

Det er kjent at også Norsk Regnesentral har sterk kompetanse innen IKT-sikkerhet.

Omfanget av kompetansen hos disse tre forskningsinstitusjonene har ikke vært kartlagt.

Foruten disse tre relativt store miljøene finnes det sannsynligvis også en rekke andre aktører involvert i større eller mindre grad med forskning på informasjonssikkerhet i Norge. Å kartlegge disse har ikke vært en prioritet i denne oppgaven.

Kapittel 6

Private institusjoner og informasjonssikkerhetsarbeid

I dette kapittelet gis en kortfattet oversikt over følgende organisasjoner: Kommunal Informasjonssikkerhet (KInS), Næringslivets sikkerhetsråd (NSR) og Gjøvik kunnskapspark. NSR og Mørketallsundersøkelsene er viet mest plass. Kapittelet er kort fordi denne oppgavens fokus ligger på offentlig sektor og myndighetenes satsing på informasjonssikkerhet. Likevel er det interessant å betrakte enkelte virksomheter i privat sektor siden flere av disse i varierende grad samarbeider med offentlig sektor.

6.1 Kommunal Informasjonssikkerhet (KInS)

6.1.1 Om organisasjonen

KInS ble stiftet stiftet i april 2003 på bakgrunn av et samlet initiativ fra Oppland fylkeskommune, Gjøvik Kunnskapspark og Datatilsynet [91]. Foreningens formål er å "bidra til økt informasjonssikkerheten i kommuner og fylkeskommuner" [92]. Strategien for å realisere dette målet er å "få til samhandling med aktuelle fagmiljøer, etablering av arenaer for kompetanseheving og utvikling av standarder" [92].

Selve foreningen KInS har ingen ansatte, men gjennom Gjøvik Kunnskapspark (GKP) gis det støtte til en 50% stilling for å drive KInS. Styret til KInS består av tre kommune-/fylkesrepresentanter, en representant fra Bluelight nettverket samt en fra GEOLOK foreningen [92].

Inntektene til foreningen kommer primært fra medlemskontingenten som hver deltagerkommune må betale. Denne varierer på bakgrunn av innbyggertallet i kommunen, men nedre og øvre grense er henholdsvis 2 500 og 10 000 kroner. Ved siden av kontingenten genererer også medlemskonferansen et økonomisk bidrag. Staten bidrar økonomisk ved å lønne den ene halvtidsstillingen samt sekretariatstjenester. Foreningen slet økonomisk de første årene, men er nå kommet i balanse [91].

Samarbeidspartnere til KInS inkluderer KS [1], NorSIS, Bluelightnettverket, Datatilsynet og KUN (Kompetanse- og utviklingsnettverket). I motsetning til KInS er Bluelight

[1] KS er kommunenes, fylkeskommunenes og medlemsbedriftenes arbeidsgiverorganisasjon.

nettverket fullstendig kommersielt og et samarbeid mellom bedrifter som jobber med informasjonssikkerhet. NorSIS samarbeider tett med KInS, og målgruppene deres overlapper. NorSIS retter seg mot alle små og mellomstore bedrifter både i privat og offentlig sektor, herunder kommunesektoren. KInS sin målgruppe er de kommunene og fylkeskommunene som har medlemskap. Det finnes også (per februar 2007) rundt 20 kommersielle medlemmer (bedrifter) blant medlemmene til KInS [91]. Alle medlemmene til KInS får tilbud om medlemskap i Bluelight nettverket uten ekstra kostnad (hvertfall for det første året) [91].

Etter 1. april 2007 ble KInS en faggruppe under NorSIS [91], og halvtidsstillingen til lederen av KInS ble utvidet til heltid. KInS/NorSIS har etter dette hatt *alle* landets kommuner som målgruppe. Praksisen rundt medlemskontingenten vil endres da det ville være urettferdig om medlemmer skulle sponse ikke-medlemmer [91]. Et delmål ved sammenslåingen av KInS og NorSIS har vært at KInS skal bli fullt ut ikke-kommersiell. Det vil si at ingen kommersielle medlemmer lenger vil bli tillatt.

6.1.2 Arbeid

KInS primæroppgave er å skape arenaer for utveksling av informasjon og nettverksbygging [92], og den årlige sikker.info konferansen (tidligere KInS konferansen) er grunnsteinen i denne oppgaven [91]. I 2006 holdt KInS 8 lokale seminarer [91]. Tilsammen har representanter fra 100 kommuner deltatt på disse 8 seminarene. Siden antall kommuner i Norge er 431, betyr dette at 23% av landets kommuner deltok på minst én KInS konferanse i 2006 [93].

Et mål med disse konferansene er å bygge nettverk. KInS forsøker å komme i kontakt med personer som jobber med informasjonssikkerhet i kommune- og fylkesadminstrasjonen. Disse kontaktpersonene kan så arrangere konferanser i samarbeid med KInS . Kontaktpersonen (og kommunen) sørger da for å stille lokaler, mens KInS stiller med foredragsholdere. Samarbeidspartnere for konferansene er blant annet NorSIS og Bluelight nettverket.

KInS bygger nettverk av kontaktpersoner både med hensyn til kommunene og fylkeskommunene. Et mål for foreningen er å avholde et årlig seminar på fylkesnivå etter at nok fylker blir representert. I februar 2007 hadde KInS 10 kontaktpersoner i forskjellige fylker, og nettverksbyggingen pågår kontinuerlig [91].

6.2 Næringslivets sikkerhetsråd (NSR)

6.2.1 Om organisasjonen

NSR sin målsetning er å "være et rådgivende organ for næringslivet i spørsmål om kriminalitet og dermed bidra til å forebygge tap" [94]. Organisasjonen gir råd om sikkerhetstiltak mot alt fra industrispionasje til terrorisme, deriblant datakriminalitet.

NSR er resultatet et samarbeid mellom næringslivets tyngste aktører, inkludert NHO, Rederiforbundet, Bedriftsforbundet, Telenor, Statoil, Finansnæringens Hovedorganisasjon og Sparebankforeningen. Organisasjonen består av et styre, et sekretariat og et fagråd. Fagrådet i NSR bidrar til å utarbeide trusselvurderinger og tiltak mot kriminelle handlinger som er rettet mot næringslivet. Rådet har faste representanter fra blant annet PST, NSM, DSB, Kripos og Økokrim [94].

NSR har også sju regionale kontakter med den hensikt å drive nettverksbygging på lokalt plan mellom sikkerhetsmyndigheter og de som arbeider med sikkerhet. Å skape møteplasser for ledere og ansatte i bedrifter om sikkerhetstemaer er også et mål med den regionale virksomheten [94]. NSR holder årlig flere konferanser og kurs på regionalt nivå.

6.2.2 Arbeid

For spesielle problemområder har NSR opprettet et antall ekspertutvalg for avdekking av trusler og rådgivning om mottiltak. Datakriminalitet er et av disse områdene hvor NSR har satt ned et eget utvalg for nærmere granskning. Datakrimutvalget i NSR (må ikke forveksles med Datakrimutvalget som er nedsatt av regjeringen) har gitt ut tilsammen fem mørketallsundersøkelser. Resultatene av disse ble publisert i 1993, 1997, 2001, 2003 og 2006. Målet med undersøkelsene er å kartlegge omfanget av datakriminalitet og andre uønskede hendelser i norske virksomheter.

NSR har samarbeidet med mange ulike institusjoner om mørketallsundersøkelsene. I 2003 eller 2006 har blant annet KRIPOS, Økokrim, NorSIS, NorCERT, Statoil, Hydro og SINTEF vært involverte. Foruten mørketallsundersøkelsene har NSR også gitt ut faghefter vedrørende risikoanalyse, dokumentsikkerhet og kommunikasjonssikkerhet.

Mørketallsundersøkelsen har primært vært utført som et samarbeid av organisasjoner i næringslivet, men også myndighetene har hatt nytte av materialet. Det er verdt å nevne at FAD ga økonomisk støtte til Mørketallsundersøkelsen 2006. Et eksempel på at myndighetene også nyttiggjør seg av materialet fra undersøkelsene finnes i St.meld. nr. 17 (2006–2007) – "Eit informasjonssamfunn for alle". I denne meldingen beskrives hovedfunnene fra Mørketallsundersøkelsen 2006. Et annet tilfelle hvor myndighetene kan ha nyttegjort seg av Mørketallsundersøkelsen er statistikken vedrørende sikring av trådløse nettverk. I undersøkelsen fra 2003 ble det slått fast at mer enn 30% ikke sikret egne trådløse nettverk ved å bruke kryptering. Infrastrukturutvalget anbefalte i sin rapport anno 2006 å pålegge alle utstyrsleverandører å levere trådløse nettverkskomponenter med en sikker konfigurasjon.

Det er positivt at myndighetene kan bidra til og dra nytte av slike undersøkelser siden de tegner et bilde av tilstanden i offentlig såvel som privat sektor. Ikke minst er undersøkelsen viktig fordi den anonymiserer og aggregerer resultatene fra spørreundersøkelsen, noe som gjør at flere virksomheter gir sitt samtykke til å delta i den. Større deltagelse gir igjen et mer korrekt bilde av tilstanden i sektorene.

Mørketallsundersøkelsen danner et viktig informasjonsgrunnlag med tanke på å utarbeide sikringstiltak for samfunnskritisk infrastruktur. 11% av de spurte virksomhetene i Mørketallsundersøkelsen 2006 oppfattet seg selv som en del av samfunnskritisk infrastruktur. 40% av disse anså seg selv som en del av samfunnskritisk infrastruktur og uttalte at de ville få alvorlige problemer innen én time dersom viktige IKT-systemer skulle være ute av drift. Dette utsagnet burde være god motivasjon for myndighetene til å investere midler i informasjonssikkerhet. Styrket informasjonssikkerhet i kritisk IKT-infrastruktur tilsvarer redusert sårbarhet i samfunnet.

Mørketallsundersøkelsen 2003

Undersøkelsen viste at 60% av norske virksomheter i 2003 ble rammet av enten datakriminalitet eller andre uønskede IT-hendelser [95]. Allikevel ble bare 187 tilfeller av datakri-

minalitet, herunder 50 tilfeller av datainnbrudd, anmeldt til politiet [95]. Av ulike grunner unnlot majoriteten av bedriftene å anmelde datainnbrudd og annen datakriminalitet til politet.

Norske bedrifter ble i 2003 utsatt for [95]:

- 5200 datainnbrudd
- 2,7 millioner forsøk på datainnbrudd
- 150 000 virus infeksjoner
- 50 millioner forsøk på virus infeksjoner

Undersøkelsen viste at over 50% av organisasjonene i 2003 ikke hadde rutiner for rapportering av sikkerhetsrelaterte hendelser. En annen undersøkelse utført i en masteroppgave fra 2005 ved HiG viste derimot at 80% hadde rutiner for rapportering av slike hendelser [52]. Denne masteroppgaven var i samsvar med Mørketallsundersøkelsen angående det at svært få bedrifter anmelder datakriminalitet til politiet.

Andre viktige momenter i Mørketallsundersøkelsen 2003 var [95]:

- To av tre virksomheter ville få vesentlige problemer allerede etter én dag dersom de viktigste IT-systemene er ute av drift.
- Åtte av ti virksomheter hadde lagret verdifull informasjon elektronisk og ni av ti ville få vesentlige problemer hvis informasjonen skulle være upålitelig eller gal.
- Kun hver fjerde virksomhet som ble rammet, kunne anslå hvor mye de hadde tapt økonomisk. 12% hadde rutiner for å beregne slike tap.
- Det samlede tapet for norske virksomheter grunnet datakriminalitet og andre uønskede hendelser ble anslått til 5 milliarder kroner.
- 70% av virksomhetene fikk ekstra arbeid på grunn av uønskede hendelser.
- Bare hver femte virksomhet som hadde vært utsatt for datakriminalitet, greide å identifisere en gjerningsmann. De fleste manglet rutiner for rapportering dersom de skulle avdekke en uønsket hendelse.
- Trådløse nettverk ble brukt av stadig flere, men mer enn 30% unnlot å sikre disse dataene med kryptering.
- Hver tredje virksomhet var treg med å oppdatere sin antivirus programvare, og like mange slurvet med sikkerhetsoppdatering av annen programvare.
- Virksomheter i helse- og sosialsektoren har lagret store mengder personopplysninger, men halvparten av dem visste ikke om de hadde vært utsatt for datainnbrudd eller datatyveri. Sektoren brukte sikringsmekanismer som kryptering i langt mindre grad (13%) enn andre sektorer. Til sammenligning brukte 40% av virksomhetene innen bank- og finansnæringen kryptering.

Mørketallsundersøkelsen 2006

Oppfølgeren til Mørketallsundersøkelsen 2003 avdekket at de fleste rapporterte hendelsene omhandlet virusangrep, tyveri av utstyr og misbruk av IT-ressurser [96].

Viktige momenter fra undersøkelsen er:

- Nesten alle bedrifter som har opplevd uønskede hendelser har gjennomført tekniske tiltak slik som installering av antivirus programvare, brannmur og spamfilter.
- Kun 40% av alle bedriftene har gjennomført sikkerhetsopplæring av ansatte. Dette viser viktigheten av å gjennomføre andre tiltak enn de rent tekniske.
- Det er estimert at norske virksomheter ble utsatt for 3900 datainnbrudd over en periode på 12 måneder, men kun 61 av disse ble anmeldt til politiet.
- Antall misbruk av IT-ressurser estimeres til 8900 tilfeller, hvorav kun 11 er anmeldt. Viljen til å anmelde straffbare forhold varierer sterkt med typen kriminalitet.
- Omtrent hver tredje virksomhet vet ikke om de har vært gjenstand for uønskede hendelser. Mørketallene er derfor fortsatt store, noe som bekreftes av lignende undersøkelser på internasjonal basis.
- 64% av norske virksomheter gir ansatte tilgang hjemmefra, noe som er en økning fra 43% i 2003. Disse virksomhetene er også de som i størst mulig grad benytter ulike sikringstiltak.
- Store virksomheter er raskere til å ta i bruk ny teknologi enn små virksomheter. For eksempel bruker bare 5% av de små virksomhetene IP-telefoni, mens tilsvarende tall for de største er 27%.
- Flere små virksomheter benytter brannmur. I 2003 hadde 62% implementert dette, mens det for 2006 var 83%. Imidlertid har kun 15% innført rutiner for vedlikehold av regelsett for brannmur og gjennomgang av logger.
- Bruk av sikkerhetskopier har økt fra 73% til 83%.
- Andelen av virksomheter som selger varer og tjenester over Internett har økt fra 9% i 2003 til 25% i 2006. Disse virksomhetene har mer fokus på sikringstiltak, men er også mer utsatt for sikkerhetshendelser.

Den hyppigst oppgitte årsaken for unnlatelse av å anmelde et forhold var at saken ble ansett som ubetydelig. Videre unnlot man ofte å anmelde fordi man ikke trodde det var mulig å finne gjerningsmannen eller at man mente angrepet ikke var spesielt rettet mot virksomheten.

Datakrimutvalget konkluderte med at mørketallene fortsatt er store. Dette skyldes ikke bare mangelfull rapportering, men også at mange bedrifter ikke er klar over at de har blitt angrepet på grunn av mangelfull deteksjon.

6.3 Gjøvik kunnskapspark

6.3.1 Om organisasjonen

Gjøvik kunnskapspark A/S er et selskap med fokus på innovasjon og nyskapning, og har rundt ti ansatte som arbeider med å realisere innovasjonsprosjekter i regionen med internasjonalt potensiale. Et av satsingsområdene til selskapet er informasjonssikkerhet.

6.3.2 Arbeid

GKP har samlet flere ulike virksomheter med relevans for informasjonssikkerhet under seg. Både NorSIS og KInS er delvis finansiert gjennom GKP. Gjennom et samarbeid med Høgskolen i Gjøvik og andre aktører i næringslivet fikk GKP i 2002 opprettet et studieprogram på masternivå i informasjonssikkerhet ved høgskolen. Studiet utføres ved NISlab/HiG og i 2005 ble tilbudet komplementert med et studieprogram på bachelornivå. Flere PhD stipendiater er også tilknyttet NISlab/HiG.

Bluelight er en annen organisasjon opprettet i regi av GKP. Bluelight består av kommersielle aktører som arbeider med produkter og systemer med fokus på informasjonssikkerhet.

GKP har forøvrig også et inkubatorprogram som for å støtte entreprenørvirksomhet innen informasjonssikkerhet. Programmet kan gi gründere med sikkerhetsprosjekter verdifull støtte i etableringen av nye virksomheter.

Kapittel 7

Sveriges satsing på informasjonssikkerhet

Dette kapittelet tar sikte på å peke ut noen sentale aktiviteter som har foregått på myndighetsnivå i Sverige for å styrke landets informasjonssikkerhet. Tabell 7.1 gjengir de utredninger og aktiviteter som beskrives i kapittelet. For hver av utredningene i tabellen blir det i dette kapittelet gjengitt foreslåtte tiltak. Informasjon om oppfølgingen av tiltakene er gitt av Sitic [97]. Gjennomførte tiltak er merket ✓, tiltak som ikke er gjennomført er merket ✗, og for de tiltak der det ikke har blitt funnet informasjon om oppfølgingen er dette angitt med "Status ukjent". Tiltak som er delvis gjennomført er merket ✓ (delvis).

Utredning	**År**
Cabinet Working Group on Information Warfare (AgIW I&II)	1997–1998
Nationella strukturer för skydd mot informationsoperationer (Mandatorrapporten)	1999
Sårbarhetsutredningen	2001
Informationssäkerhetsutredningen	2003–2005
Strategi för ett säkrare Internet	2007

Tabell 7.1: *Svenske utredninger for styrking av nasjonal informasjonssikkerhet.*

Cabinet Working Group on Information Warfare 1997–1998

Bakgrunnen for nedsettelsen av arbeidsgruppen som skulle drøfte Information Warfare (AgIW) var to proposisjoner som kom i 1996. Den ene, 1996/97:11, omhandler store påkjennelser for samfunnet i fredstid, mens proposisjon 1996/97:4 drøfter totalforsvaret i fornyelse [98, kap. 1.1]. Arbeidsgruppens mål var å utrede utviklingen av trussel- og risikobildet innen informasjonskrigføring. Denne arbeidsgruppen var den første som utredet trusler innenfor informasjonssikkerhet i regi av den svenske staten [99, kap. 7.1.3]. Arbeidsgruppen fikk deretter i oppgave å anbefale en ansvarsfordeling samt retningslinjer for en strategi på området. Under dette arbeidet endret gruppen navn til AgIO (arbeidsgruppen for Information Operations).

Den første rapporten fra arbeidsgruppen beskriver historikken og bakgrunnen til informasjonskrigføring, tekniske metoder for krigføring og overordnede tiltak for beskyttelse. I

den andre rapporten beskrives mer detaljerte forslag til strategi for beskyttelse mot informasjonskrigføring.

Arbeidsgruppen foreslo følgende tiltak [100, kap. 6.1]:

Opprette samordningsgruppe — ✗ En samordningsgruppe opprettes på regjeringsnivå som starter arbeidet med en strategisk kartlegging av informasjonskrigføring. Gruppen bør også kunne fungere som en del av nasjonal krisehåndtering. Blant de foreslåtte aktørene i samordningsgruppen finnes Överstyrelsen för civil beredskap (nåværende KBM, ble foreslått som koordinator), Försvarsmakten (Försvarsmaktens Högkvarter og militära underrättelse- och säkerhetstjänsten), Totalförsvarets Chefsnämnd, Försvarets radioanstalt, Post- och telestyrelsen, StatsCERT og en statistikkenhet for datakriminalitet.

Opprette samordningsorgan — ✗ Et nytt interdepartementalt samordningsorgan opprettes innen Regeringskansliet [1] for å håndtere sektovergripende spørsmål knyttet til Information Warfare

StatsCERT — ✓ Opprettes og organiseres under ledelse av Post- och telestyrelsen med støtte fra Rikspolisstyrelsen (RPS). Får ansvar for å overvåke, beskytte og gjenopprette drift av kritisk infrastruktur ved dataangrep. Per idag ligger CERT funksjonen hos Sitic (Sveriges IT-incident centrum), og den er ikke støttet av RPS.

Statistikkenhet — ✓ En statistikkenhet ansvar for å samle inn statistikk om datakriminalitet opprettes og skal samarbeide med Näringslivets Säkerhetsdelegation. Per idag har Sitic mandat som statistikkenhet, men organisasjonen samarbeider ikke med Näringslivets Säkerhetsdelegation.

Rapporteringsplikt — ✗ Innføres for IT-relaterte hendelser innen statsforvaltningen.

Försvarsmaktens mandat utvides — ✗ Den delen av mandatet som omfatter sikring av kommunikasjon i totalforsvaret utvides til å omfatte sivile informasjonssystemer med betydning for totalforsvaret.

IT-kontrollfunksjon — ✓ En samordnet IT-kontrollfunksjon opprettes for å drive aktiv kontroll av totalforsvarets datasystemer. Med aktiv kontroll menes det å utsette systemene for kontrollerte angrep slik at sårbarheter kan avdekkes. Funksjonen er opprettet og lagt til Försvarets radioanstalt.

Lovendringer i dataloven — ✗ De nødvendige endringer i dataloven gjennomføres snarest.

Operativ overvåkning — ✗ SPF (Styrelsen för psykologiskt försvar) etablerer en analysegruppe for medieovervåkning av Internett. Slik overvåkning innebærer at man prøver å følge informasjonsflyten på Internett og sile ut det som har interesse for myndighetene. Tanken er at man skal skaffe til veie et overblikk over det som skjer på Internett og som er i myndighetenes interesse å vite. Et eksempel er å registrere unormale aktiviteter som kan indikere angrep på IKT-infrastruktur.

[1] Regeringskansliet bistår regjeringen i sitt arbeid. Det ledes av Statsrådsberedningen og består forøvrig av departementene og forvaltningsavdelingen.

Etteretning — ✓ (delvis) Nye samarbeidsrutiner og ny arbeidsfordeling gjennomføres for å effektivisere og kvalitetssikre behandling av etteretningsdata.

Som det fremgår av oversikten ble omtrent halvparten av de foreslåtte tiltakene gjennomført. Det er verdt å bemerke at av de gjennomførte tiltakene var tre relativt store og ressurskrevende: CERT, statistikkfunksjon og IT-kontrollfunksjon.

Nationella strukturer för skydd mot informationsoperationer (Mandatorrapporten) 1999

Mandator er et IT-konsulent selskap i Sverige som på våren i 1999 mottok forespørsler fra Försvarsdepartementet og den svenske etterretningstjenesten om å bidra til "ökade förståelse för informations-operationer och strategiskt nationellt IT-säkerhetsskydd" [101]. 14. desember samme året var rapporten ferdig.

Rapporten beskriver en helhetlig løsning for å takle angrep på nasjonale datasystemer og -nettverk. Prosjektgruppen benyttet en metodikk som gikk ut på å identifisere nøkkelfunksjoner og deretter gruppere disse i organisasjoner etter grad av kobling mellom funksjonene.

Hovedpunktene i forslaget om organisasjonsstruktur er opprettelsen av tre virksomheter [101, kap. 6]:

CERT — ✓ Har to hovedoppgaver. Den første er å fungere som helpdesk døgnet rundt hele året. Den andre oppgaven er å drive hendelsesrapportering. Det foreslås at systemeiere leverer beskrivelse av systemene sine til CERT slik at man lettere kan gi hjelp ved uforutsette hendelser. Personalet oppfordres også til å sertifisere seg for eksempel gjennom CISSP (Certified Information Systems Security Professional). Ved alvorlige hendelser er det en spesiell krisehåndteringsgruppe som har ansvaret. Medlemmer av gruppen er lederen for CERT, lederen for analysegruppen, lederen for IT-sikkerhetsgruppen samt representanter fra Justitie, Försvars-, Finans- och Näringsdepartementene. CERT foreslås underlagt Överstyrelsen för civil beredskap (ÖCB, nåværende KBM) på bakgrunn av det spesielle ansvaret organisasjonen har for samordning samt at den har god kontakt med næringslivet. CERT funksjonen er opprettet og ligger i dag hos Sitic som er underlagt PTS.

IT-sikkerhetsgruppen — ✗ Ansvarlig for å teste og evaluere teknikker, metoder og verktøy for forsvarssektoren. Nye laboratoriemiljøer må etableres slik at denne forskningen kan utføres tilfredsstillende. I denne gruppen etableres et såkalt Red Team som har i oppgave å avdekke sårbarheter og utføre penetreringstester. Red Team skal primært evaluere systemer i militær sektor, men kan også nyttes for systemer i den sivile delen av statsforvaltningen. Administrativt underlegges sikkerhetsgruppen Försvaret og blir videre en del av etterretningstjenesten.

Analysegruppen — ✗ Får ansvar for å evaluere strategiske trusler og risikoer. Analysene skal brukes som grunnlag for å utarbeide retningslinjer innen sårbarhet og beredskap. Gruppen får også i ansvar å samordne forskning på informasjonsoperasjoner. Gruppen anbefales også å etablere kontakt med lignende virksomheter i andre land slik som Critical Infrastructure Coordination Group (CICG) i USA.

Rapporten peker på at det er foretatt en oppdeling av hvilke ansvarsmyndigheter som er hensiktsmessige å ha i sivil og militær sektor basert på type aktivitet som skal utføres. Et viktig argument i denne sammenheng er at man bør skille mellom kunnskap for å bryte seg inn i systemer (såkalt Red Team aktiviteter) og kunnskap vedrørende sivile virksomheters sensitive systemer. Sivil og militær sektor skal derfor ifølge forslaget ha et ikke-overlappende ansvar for henholdsvis sivile systemer og Red Team aktivitet. For et konkret eksempel om hensikten bak dette argumentet nevnes det at sivile systemeiere neppe er interessert i at militæret skal være i besittelse av informasjon om sårbarheter i deres systemer slik at sårbarhetene kan utnyttes militært [101, kap. 6].

Som det fremgår av oversikten har bare det første tiltaket vedrørende opprettelsen av en CERT blitt gjennomført. Tiltaket vedrørende IT-sikkerhetsgruppen overlapper noe med tiltaket om en IT-kontrollfunksjon og etablering av et Red Team som foreslått av AgIW/AgIO, men tiltaket om IT-sikkerhetsgruppen er langt mer omfattende siden tiltaket også inkluderer etablering av nye laboratoriemiljøer. Det siste foreslåtte tiltaket som omhandlet opprettelsen av en analysegruppe ble ikke foreslått av AgIW/AgIO.

Sårbarhetsutredningen (SOU 2001:41) **2001**

"Sårbarhets- och säkerhetsutredningen" hadde i oppdrag å foreslå forslag for å oppnå en bedre helhetlig planlegging for det sivile forsvaret og beredskapen under store påkjennelser i fredstid. Utredningsgruppen skulle også bedømme organisatorisk eller strukturell inndeling og avdekke mulig forbedringspotensiale. Utredningen skulle videre omfatte forslag til å forbedre IT-sikkerhet samt bedre beskyttelsen mot informasjonsoperasjoner.

Det er to kapitler i rapporten som særskilt drøfter IT og sikkerhet: Kapittel 6 – "Strategi för ökad robusthet i den tekniska infrastrukturen" og kapittel 7 – "Strategi för ökad IT-säkerhet och skydd mot informationsoperationer".

Tiltakene foreslått i begge disse kapitlene gjengis i det følgende.

Strategitiltak for å forbedre sikkerheten i teknisk infrastruktur [99, kap. 6.6]:

- ➢ Utrede lovgivningen vedrørende sikkerhetskrav til teknisk infrastruktur slik at eventuelle nødvendige skjerpelser og presiseringer kan skje — ✗
- ➢ Tilsynene av ulike virksomheter innenfor den tekniske infrastrukturen bør effektiviseres — ✗
- ➢ Brukere som har svært høye krav til sikkerhet i den tekniske infrastrukturen bør ha skjerpede krav om at de skal gå til anskaffelse av reserveløsninger — ✗
- ➢ Planleggingen av sikkerhets- og beredskapsarbeidet som gjelder den tekniske infrastrukturen bør samordnes bedre — ✗
- ➢ Det bør satses flere ressurser på sikkerhets- og beredskapsarbeid på den tekniske infrastrukturen — ✗
- ➢ Elektrisitetsforsyningen bør gis høyeste prioritet i samfunnets satsing på sikkerhets- og beredskapsarbeid — ✗

Strategitiltakene som ble foreslått for økt IT-sikkerhet og beskyttelse mot informasjonsoperasjoner [99, kap. 7.8]:

- ➢ En sektoroverlappende strategi for samfunnets håndtering av IT-sikkerhet og beskyttelse mot informasjonsoperasjoner — ✓ KBM har fått i oppdrag å utarbeide en nasjonal handlingsplan, det vil si en mindre delmengde av en strategi, for informasjonssikkerhet.
- ➢ Et tverrsektorielt koordineringsorgan for IT-sikkerhet og beskyttelse mot informasjonsoperasjoner opprettes i Regeringskansliet — ✗
- ➢ Planleggingsmyndigheten [2] opprettes og får et overordnet ansvar for samfunnets IT-sikkerhet — ✗ Planleggingsmyndigheten er ikke opprettet.
- ➢ En funksjon for teknisk kompetanse innen IT-sikkerhet opprettes i Försvarets radioanstalt (FRA) som en egen myndighet underlagt FRA — ✗ FRA har oppdraget med å ivareta denne kompetansen og er således ansvarlig. Det er derimot ikke opprettet en egen myndighet innen FRA.
- ➢ En funksjon for hendelseshåndtering i IT opprettes i høyskolemiljøet som en egen myndighet underlagt PTS (Post- och telestyrelsen) — ✓
- ➢ Funksjonen for analyse av omverdenen, som opprettes som en del av planleggingsmyndigheten, skal ha kapasitet til å drive analyse også innen IT-sikkerhet og informasjonsoperasjoner — ✗
- ➢ Det utredes og foreslås endringer i reguleringer for å kunne garantere hemmelighold samt pålegge taushetsplikt innen funksjonen for teknisk kompetanse og hendelseshåndteringsfunksjonen for IT. Obligatorisk hendelsesrapportering innføres for statsforvaltningen — ✗
- ➢ Det utredes og foreslås endringer i lover eller forskrifter for å klargjøre forutsetningene for aktiv IT-kontroll — ✗
- ➢ Försvarsmakten får i oppgave å bygge opp et svensk system for evaluering og sertifisering innen IT — ✓
- ➢ Regjeringen undertegner Recognition Arrangement for IT Security Certificates — ✓

De organisatoriske konsekvensene av forslaget innebærer å danne to nye organer innen Regeringskansliet: et nasjonalt krisehåndteringsorgan og et koordineringsorgan for IT-sikkerhet. Videre medfører forslaget at man oppretter en planleggingsmyndighet og IT-sikkerhetsorganer som omfatter funksjoner for IT-hendelseshåndtering, teknisk kompetanse og et system for evaluering og sertifisering av sikkerhet i produkter og systemer [99, Sammanfattning].

Utredningen ble behandlet i regjeringens proposisjon 2001/02:158 – "Samhällets säkerhet och beredskap" og denne proposisjonen fremmet i hovedsak de samme synspunktene som utvalget vedrørende etablering av IT-sikkerhetsorganene. Som det går frem av oversikten er det gjort svært lite for å følge opp forslagene til tiltak.

[2] Planleggingsmyndigheten er tenkt å påta seg oppgaver som hører til på høyt myndighetsnivå men som ikke bør belaste Regeringskansliet. Disse oppgavene er å skaffe et godt informasjonsgrunnlag for regjeringens beslutninger, samle informasjon fra omverdenen og foreta og analyser (inkludert ROS-analyser på nasjonalt og internasjonalt nivå) samt koordinere forskningsinstitusjoner innen fagområdet krisehåndtering.

Informationssäkerhetsutredningen **2003–2005**

InfoSäkutredningen består av fire delutredninger utført i perioden 2003–2005. Disse delutredningene er:

- SOU 2003:27 Signalskydd [3]
- SOU 2004:32 Informationssäkerhet i Sverige och internationellt – en översikt
- SOU 2005:42 Säker information – förslag till informationssäkerhetspolitik
- SOU 2005:71 Informationssäkerhetspolitik – Organisatoriska konsekvenser

Av disse fire delutredningene gjengis tiltakene fra de to siste utredningene i denne oppgaven. I SOU 2005:42 presenteres et forslag til nasjonal strategi for informasjonssikkerhet, mens SOU 2005:71 tar for seg organisatoriske konsekvenser som følge av denne strategien.

SOU 2005:42 Säker information – förslag till informationssäkerhetspolitik

Forslaget til strategi for informasjonssikkerhet var i denne utredningen av svært overordnet karakter. Innholdet i forslaget gjengis her [102, kap. 9]:

1. Utvikle Sveriges posisjon innen EU og i internasjonale sammenhenger
2. Skape tillit, trygghet, sikkerhet og øke integritetsbeskyttelsen
3. Fremme økt bruk av IT
4. Forebygge og kunne håndtere forstyrrelser i informasjons- og kommunikasjonssystemer
5. Styrke etterretnings- og sikkerhetstjenestenes arbeid
6. Styrke evnen innen området nasjonal sikkerhet

   Det ble også kommentert at strategien burde inneholde følgende momenter:
7. Utnytte samfunnets samlede kapasitet
8. Fokusere på samfunnskritisk virksomhet
9. Øke bevisstheten rundt sikkerhetsrisikoer og muligheter til beskyttelse
10. Sikre at kompetansen blir ivaretatt

SOU 2005:71 Informationssäkerhetspolitik – Organisatoriska konsekvenser

I oppfølgeren til SOU 2005:42, SOU 2005:71, utredes organisatoriske forhold på bakgrunn av den anbefalte strategien.

Følgende anbefalinger vedrørende organisatoriske endringer ble gitt i SOU 2005:71 [103, Sammanfattning]:

Samarbeid med næringslivet — Status ukjent Det ble anbefalt å kontakte næringslivets nystartede organisasjon på området.

[3] Det nærmeste man kommer dette ordet på norsk er kommunikasjonsbeskyttelse.

Målsetninger for arbeidet — ✗ Utvalget anbefalte å utarbeide en målstruktur med målsetninger for arbeidet med informasjonssikkerhet.

Flytte samordningsansvar til IST — ✗ Det ble anbefalt å legge samordningsansvaret for teknisk informasjonssikkerhet til en ny institusjon med navnet IST – Institutet för signalunderrättelsetjänst och teknisk informationssäkerhet. Myndigheten skulle ha høy teknisk kompetanse, og kompetansen skulle i hovedsak overføres fra Försvarets radioanstalt.

Flytte ansvar for policy og administrativ koordinering til KBM — ✗ Utvalget foreslo å legge disse ansvarsområdene til KBM. Dette har ikke skjedd. En nyere utredning har foreslått å slå sammen KBM med Räddningsverket og å nedlegge informasjonssikkerhetsavdelingen i KBM [97].

Flytte teknisk samordningsansvar til IST — ✗ Utvalget anbefalte å flytte ansvaret for kommunikasjonssikkerhet fra etterretningstjenesten under Försvarsmakten til den nye institusjonen IST. KBM sitt ansvar for nøkkeldistribusjon ble også foreslått overført til IST.

Opprette organisasjoner for utenlandsk samarbeid — ✗ Det ble foreslått å opprette to organisasjoner: National Communications Security Agency (NCSA) og National Distribution Agency (NDA). Førstnevnte organisasjon skulle ha ansvaret for spørsmål knyttet til kommunikasjonssikkerhet, mens sistnevnte skulle ha ansvar for nøkkeldistribusjon. Det ble foreslått å legge NCSA og NDA under IST.

Sitic og samarbeidspartnere — ✓ Utvalget understreket viktigheten av et nært og tillitsfullt samarbeid mellom aktører innen informasjonssikkerhetsområdet og Sitic som er ansvarlig for hendelsesrapporteringsfunksjonen. Spesielt KBM og FRA ble fremhevet som viktige samarbeidspartnere for Sitic. Sitic har kontakt med KBM og FRA gjennom Samverkansgruppen för informationssäkerhet (SAMFI), og ifølge Sitic fungerer samarbeidet mellom organisasjonene godt [97].

Etablering av frivillig kriseressurser — ✗ Det ble anbefalt å opprette en kompetansebank av frivillige ressurser. KBM ble foreslått som ansvarlig for ordningen. Oppgaven bestod i å vedlikeholde kontaktnettverk, inngå avtaler med enkeltpersoner og virksomheter samt sørge for at det ble gjennomført øvelser.

Det er angitt nåværende status for de tiltakene som her ble gjengitt. Det vites ikke om tiltakene vil bli implementert i fremtiden. I delutredning III, SOU 2005:42, ble det presentert en strategi bestående av meget overordnede tiltak. KBM jobber per idag med å utarbeide en delmengde av denne gjennom en nasjonal handlingsplan for informasjonssikkerhet. Denne handlingsplanen skal presenteres sammen med organisasjonens årsrapport for 2008 [97].

Som oversikten viser er det i praksis ikke gjennomført et eneste foreslått tiltak fra delutredning IV, SOU 2005:71. Det kan nevnes at Försvarsmakten hadde store innsigelser mot å flytte sin kompetanse fra Försvarets radioanstalt over til det foreslåtte Institutet för signalunderrättelsetjänst. Denne innsigelsen ble synliggjort allerede i utredningens rapport [103, s. 115]. Det vites ikke hva myndighetenes begrunnelse er for å ikke gjennomføre de andre tiltakene.

Strategi för ett säkrare Internet **2006**

Etter at PTS fikk i oppdrag fra regjeringen å fremme forslag for en strategi til et sikrere Internet i Sverige, foretok organisasjonen en utredning hvilket resulterte i rapporten "Strategi för ett säkrare Internet i Sverige". Denne var ferdigstilt 4. juli 2006. Denne strategien må ikke forveksles med den nasjonale strategien for informasjonssikkerhet. Krisberedskapsmyndigheten holder på å utvikle denne nasjonale strategien [97].

I strategien for et sikrere Internett pekes det på en rekke tiltak som er foreslåtte, planlagte og pågående. Disse er gjengitt i tabell 7.2. PTS er ansvarlig utførelsen av de aller fleste tiltakene som er i tabellen. Visse tiltak er ment å gjennomføres av Sitic eller den svenske regjeringen. Majoriteten av tiltakene er planlagt utført innen 2008, mens visse andre tiltak er løpende.

Tiltak for å beskytte Internetts fysiske og logiske struktur

- ➢ Vurdere anbefalinger til leverandører av innholdstjenester for økt tilgjengelighet.
- ➢ Fremme bruk av DNSSEC [4] i navnetjenere.
- ➢ Vurdere anbefalinger om sikrere trafikkutveksling mellom Internettilbydere.

Tiltak for informasjon til brukere

- ➢ Informere om sårbarheter
- ➢ Utvikle råd for bestilling av internettjenester
- ➢ Samordne og intensivere informasjonsinnsats mot brukere
- ➢ Utdanne kommende lærere i informasjonssikkerhet
- ➢ Videreutvikle PTS sin nettside angående Internett og sikkerhet

Tiltak for økt ansvarstagning for brukernes sikkerhet

- ➢ Arbeide med spesifiserte krav på god funksjon og teknisk sikkerhet
- ➢ Følge opp Internettilbydernes funksjonsevne.
- ➢ Gi Internettilbyderne mulighet til å forhindre spredning av skadelig trafikk
- ➢ Utrede krav om økt ansvar for leverandører av programvare og annet utstyr

Tiltak for å fremme kunnskapsutvikling

- ➢ Informere aktører om de finansieringsmuligheter som finnes
- ➢ Arbeide for at det settes av midler innen rammen for EUs forskningsprogram vedrørende Internetts infrastruktur

Tiltak for å øke svensk deltagelse i internasjonalt arbeid

- ➢ Øke svensk samordning og deltagelse i internasjonale fora
- ➢ Tydeliggjøre svensk ansvarsfordeling i forbindelse med internasjonale kontakter om sikkerhet i Internetts infrastruktur
- ➢ Videreutvikle det operative internasjonale nettverket for hendelseshåndtering
- ➢ Fortsette med aktiv deltagelse i vurdering av EU direktiver

Tabell 7.2: *PTS sine strategitiltak i 2006 for et sikrere Internett i Sverige.*

Kapittel 8

Diskusjon

Innledningsvis i oppgaven ble det stilt et antall forskningsspørsmål i forbindelse med nasjonal satsing på informasjonssikkerhet. Disse spørsmålene var følgende:

1. Hvilke tiltak er foreslått i forskjellige utvalg nedsatt av regjeringen?
2. Hvilke av de foreslåtte tiltakene er blitt implementert?
3. Hva har graden av fremgang vært mellom de ulike utvalgene?
4. Hva gjør offentlig sektor for å styrke informasjonssikkerheten i samfunnet?
5. Hva gjør privat sektor for å styrke informasjonssikkerheten i samfunnet?

   Videre ble det stilt spørsmål om hvordan Norges satsing står i forhold til satsing i Sverige. Oppgaven skulle gi svar på følgende spørsmål i denne sammenheng:
6. Hvilke hvilke er foreslått og implementert i Sverige for å bedre informasjonssikkerheten?
7. Hvordan skiller arbeidet med informasjonssikkerhet seg i Sverige fra det som skjer i Norge?

For å gi svar på spørsmål 1 og 2 har oppgaven tatt for seg Sårbarhetsutvalget, Infrastrukturutvalget og Datakrimutvalget. I tillegg har oppgaven tatt for seg Nasjonal strategi for informasjonssikkerhet siden denne må regnes som svært relevant for myndighetenes satsing på nasjonal informasjonssikkerhet. Riksrevisjonens undersøkelse er også diskutert i sammenheng med oppfølgingen av Nasjonal strategi for informasjonssikkerhet.

Spørsmål 1 og 2 er besvart i delkapitlene om Sårbarhetsutvalget, Infrastrukturutvalget, Datakrimutvalget og Nasjonal strategi for informasjonssikkerhet (jf. hhv. kap. 3.2, 3.3, 3.4, 4.1). Det har dessverre ikke vært mulig å vurdere oppfølgingen av anbefalingene fra Infrastrukturutvalget og Datakrimutvalget (delutredning II) siden begge utvalgene avleverte rapport nylig (april 2006 og februar 2007). Utvalgenes anbefalinger har i stedet vært drøftet.

Hva har graden av fremgang vært mellom de ulike utvalgene?

Infrastrukturvalget kan ses på som en delvis oppfølging av Sårbarhetsutvalgets arbeid. Nasjonal strategi for informasjonssikkerhet er også å betrakte som en delvis oppfølging

av Sårbarhetsutvalget. Infrastrukturutvalget avleverte ikke sin rapport før i 2006 og har således ikke hatt noen innvirkning på Nasjonal strategi for informasjonssikkerhet ennå. Den vil sannsynligvis ha en viss innvirkning på den reviderte strategien for perioden 2007–2010.

Sårbarhetsutvalgets rapport har blitt stående som et referansedokument om samfunnets sårbarhet, herunder sårbarhet som følge av avhengighet til IKT. Selv om det ble fokusert i overkant mye på fysiske sikringstiltak av IKT-infrastrukturen, anbefalte utvalget tiltak på en rekke områder for å oppnå styrket informasjonssikkerhet i samfunnet. Rapporten som ble avlevert i juli 2000 var tydelig på at det måtte etableres en nasjonal strategi for informasjonssikkerhet, og av de seks punktene som utvalget foreslo i en slik strategi, handlet fire av de om å tilegne seg kunnskap om samfunnets sårbarhet og informasjonssikkerhet (jf. kap. 3.2.2, side 14). At kunnskap og læring hadde et så stort fokus understreker at man på den tiden hadde svært begrensede kunnskaper om informasjonssikkerhetens rolle for å skape robuste IKT-infrastrukturer i samfunnet, til tross for samfunnets totale avhengighet til de samme infrastrukturene.

Utvalget anbefalte en helhetlig tilnærming til problemstillingen med opprettelsen av en nasjonal strategi for informasjonssikkerhet, etableringen av et senter for informasjonssikring og et varslingssenter for trusler mot IKT-tjenester i offentlig virksomhet. SIS og VDI ble senere innlemmet som en del av Nasjonal strategi for informasjonssikkerhet og ble dermed sikret fokus videre i myndighetens arbeid.

Mandatet til SIS virket opprinnelig noe omfattende. En mer passende helhetlig løsning kom ved etableringen av NorCERT i tilknytning til VDI. Dette har gitt klarere grenselinjer i og med at én organisasjon er blitt primæransvarlig for forebyggende arbeid, mens en annen primært er ansvarlig for å gjenopprette normal drift ved sikkerhetshendelser. En slik deling og spesialisering i å gjennomføre proaktive og reaktive tiltak synes mer hensiktsmessig. Denne nye fordelingen av arbeidsoppgaver kan blant annet tillegges arbeidet med Nasjonal strategi for informasjonssikkerhet.

Infrastrukturutvalget har skiftet nokså mye fokus i forhold til Sårbarhetsutvalget. Sistnevnte var opptatt av å finne ut mer om informasjonssikkerhetstrusselen i samfunnet og etablere et apparat for å redusere sårbarheten. Da Infrastrukturutvalget avleverte rapport var det gått nesten seks år siden Sårbarhetsutvalget avleverte sin rapport. Førstnevnte utvalg har, i likhet med Riksrevisjonens rapport, viet mye oppmerksomhet til organiseringen av informasjonssikkerhetsarbeidet. Utvalget har videre anbefalt flere administrative og økonomiske tiltak for å sikre bedre oppfølging av arbeidet i fremtiden. Det er også flere foreslåtte tiltak rettet mot privatpersoner, slik som at Internettilbydere bør forpliktes til å levere sikkerhetsprogramvare til sine kunder. Tiltak av denne typen var ikke med i Sårbarhetsutvalgets rapport.

Det nasjonale og helhetlige apparatet som trengs for å kunne forebygge informasjonssikkerhetstrusselen ser i stor grad ut til å være på plass. Det som nå er problemet er å organisere arbeidet på en koordinert og effektiv måte. Dette innebærer ifølge Infrastrukturutvalget blant annet en tydeliggjøring av ansvarsfordeling på departementnivå, enklere finansiering av tverrsektorielle tiltak og entydige regelverk som etterleves, herunder en sektorovergripende lov om beredskap og sikring av kritisk infrastruktur.

Sårbarhetsutvalget var inne på problemstillingen med et utdatert lovverk i forhold til datakriminalitet. Temaet ble derimot ikke godt nok dekket til å kunne danne grunnlag for lovendringer. Infrastrukturutvalget har ikke vært inne på lovgivning i tilknytning til data-

kriminalitet. I januar 2002 ble Datakrimutvalget opprettet, men oppgaven var ikke å alene vurdere nasjonal lovgivning på området, men vurdere hva som måtte endres i norsk lov for å kunne godkjenne datakrimkonvensjonen til EU. Få endringer ble gjort i den norske lovgivningen, og utvalget konkluderte i hovedsak med at det fantes hjemmelgrunnlag for at Norge skulle kunne godkjenne majoriteten av artiklene i konvensjonen uten nasjonale lovendringer. Først i 2007, ytterligere 5 år etter opprettelsen av Datakrimutvalget, foreligger det en vurdering og forslag til en eksplisitt regulering av datakriminalitet. Denne utredningen, delutredning II, baserer seg i en viss grad på arbeidet fra delutredning I.

Det er på høy tid at de juridiske aspektene IKT-utviklingen har bragt frem også blir viet oppmerksomhet. Et internasjonalt samarbeid for felles regulering er viktig i denne sammenheng, siden datakriminalitet svært ofte foregår på tvers av landegrenser.

Hva gjør offentlig sektor for å styrke informasjonssikkerheten i samfunnet?

Kapittel 5 omhandler sentrale offentlige institusjoner samt deres rolle og viktige arbeider med å bedre informasjonssikkerheten i samfunnet. I det følgende beskrives utviklingen med informasjonssikkerhetsarbeid som foregikk på 1990-tallet og som har ledet til den nåværende og bedre tilpassede organisasjonsstrukturen.

Arbeidet med å styrke informasjonssikkerheten på 1990-tallet bar preg av mangel på kontinuitet og mangel på forståelse av informasjonssikkerhet og den logiske trusselen. FFI var en viktig aktør som bidro med informasjon om samfunnets sårbarhet i sivil såvel som militær sektor. Dette bidraget kom i form av prosjektserien BAS – Beskyttelse av samfunnet, som i varierende grad drøftet informasjonssikkerhet i samfunnet. Hoveddelen av innholdet i disse prosjektene drøftet sikring av samfunnskritisk infrastruktur, herunder IKT-infrastruktur. Resultatene fra prosjektene resulterte i mange foreslåtte tiltak i ulike Stortingsmeldinger. Arbeidet med prosjektene var forøvrig en viktig faktor for opprettelsen av Sårbarhetsutvalget [104, kap. 12.1]. Det ble fokusert på fysisk sikring slik som samlokalisering av infrastruktur i fjellhaller, noe som kan tilskrives mangel på forståelse av det nye kommunikasjonsparadigmet IKT hadde gitt samfunnet.

Oppfølgingen av de foreslåtte tiltakene i forskjellige Stortingsmeldinger har vært svært varierende. Rapporten fra BAS5 trekker frem BAS2 prosjektet som et eksempel på mangelfull oppfølging. Mange av tiltakene i BAS2 prosjektet ble ikke gjennomført på grunn av at de ble foreldet grunnet hurtig teknologisk utvikling, men også fordi oppfølgingen skjedde i et altfor langsomt tempo. I rapporten til BAS5 ble det også kommentert at departementene etterspurte tiltakslister, til tross for at prosjektet hadde fokus på metodikk. Dette med informasjonssikkerhet som en prosess kontra tiltakslister er et viktig moment. Først når arbeidet med informasjonssikkerhet settes i et system blir resultatene gode. For at arbeidet skal kunne gjøres systematisk forutsettes det en metodisk fremgangsmåte, langsiktig tenkning samt kontinuerlig evaluering og revidering av arbeidet og målsetningene. Først når disse faktorene er på plass kan man snakke om arbeidet med informasjonssikkerhet som en prosess. Den nasjonale strategien for informasjonssikkerhet har lagt premissene for at at arbeidet med informasjonssikkerhet ikke skal preges av ujevn og noe vilkårlig oppfølging av tiltak. Arbeidet nærmer seg i stedet en prosess hvor de strategiske målsetningene er knyttet opp mot tiltak.

Koordineringsutvalget for informasjonssikkerhet (KIS, opprettet 2004) har en sentral oppgave i å koordinere arbeidet med oppfølgingen av den nasjonale strategien selv om

utvalget ikke har myndighet til å fatte vedtak. Oppfølgingen av Nasjonal strategi for informasjonssikkerhet har fått mye kritikk av Riksrevisjonen, men selve strategien virker samlet sett god, til tross for at det er behov for enkelte endringer. Blant annet må strategien endres slik at det er mulig å evaluere graden av måloppnåelse for målsetningene ved å koble disse mot tiltakene. En revidert strategi vil foreligge i nær fremtid. Forhåpentligvis vil ansvarsfordelingen være bedre bedre avklart slik at den reviderte strategien vil få bedre oppfølging enn den nåværende. Det er viktig å påpeke at Riksrevisjonens undersøkelse har fokusert mye på koordinering og samordning av arbeidet på departementnivå, og lite på arbeidet som skjer i den enkelte sektor. Det kan derfor være at det totale bildet av tilstanden for informasjonssikkerhet i det norske samfunn ikke nødvendigvis er så dårlig som Riksrevisjonens rapport gir inntrykk av [79, kap. 9.4.1].

En presisering av ansvarsfordelingen er nylig kommet i St.meld. nr. 17 (2006–2007). To viktige avklaringer gjelder FAD og JD. Stortingsmeldingen presiserer at FAD er ansvarlig for *forebyggende, tverrsektorielt arbeid* med IKT-sikkerhet, mens JD har et koordinering- og tilsynsansvar for sikkerhet i samfunnets sivile sektor. Som følge av denne avklaringen er det foreslått å flytte budsjettansvaret for NorCERT over til FD. Videre heter det i meldingen at primæransvar for sikring av informasjonssystemer ligger hos eier eller operatør, og at fagdepartementene har et overordnet sektoransvar for å ivareta sikringen av sektorens IKT-infrastruktur [79, kap. 9.4.1].

Post- og teletilsynet ble opprettet i 1987 og har som hovedoppgave å regulere og overvåke post- og telekommunikasjonssektoren. PT er også en sentral aktør i arbeidet med informasjonssikkerhet på nasjonalt nivå. Som forvalter av ekomloven har tilsynet et spesielt ansvar for sikkerhet- og beredskap i ekomnett og er ansvarlig for oppfølgingen av flere tiltak i Nasjonal strategi for informasjonssikkerhet. PT har et ansvar for sikring av kritisk infrastruktur, men er også ansvarlig for å arbeide med bevisstgjøring og kompetanseheving overfor Internettleverandører og deres brukere. Nettstedet nettvett.no er et eksempel på et tiltak innen veiledning som PT etablerte i samarbeid med andre aktører. Vedrørende sikring av kritisk infrastruktur har PT arbeidet for sikring av NIXene samt etablering av flere IXer på regionalt nivå. PT driver også kontinuerlig kartlegging av den samlede infrastrukturen, herunder transportnettet, som den enkelte markedsaktør er en del av. Videre utarbeider tilsynet ROS-analyser basert på informasjon fra aktørene og fra kartleggingen av infrastrukturen. I denne sammenheng er det verdt å bemerke at metodikken utviklet gjennom BAS5 prosjektet kan være nyttig for tilsynet, og at det derfor bør undersøkes i hvilket omfang metodikken kan nyttiggjøres.

I St.meld. nr. 17 (2006–2007) uttaler PT at organisasjonen i fremtiden bør rette et økt fokus mot sikring av IP-baserte nettverk siden disse nettverkene blir stadig mer utbredt på grunn av konvergensen mellom ulike teknologier. Det kommenteres videre at redundansen i telenettene er blitt god på grunn av økt konkurranse mellom aktørene, hvorav flere har etablert egne nett. PT nevner også at erfaringer organisasjonen har gjort tilsier at de store tilbyderne tar sikring av IKT-produksjonssystemene alvorlig, og at de bruker red teams for å avdekke sikkerhetshull i egne systemer gjennom aktive penetreringsforsøk.

I BAS2 (1997–1999) ble det konkludert med at myndighetene måtte sette premisser for utviklingen av telenettet for å begrense sårbarheten. Ifølge PT har mange ulike aktører i markedet ført til god redundans i telenettet, noe som er et tegn på at et fritt marked og konkurranseutsetting også kan bidra til økt sikkerhet.

I nevnte Stortingsmelding kommenterer PT at viktige fremtidige sikringstiltak inkluderer sikring av tjenester for elektronisk kommunikasjon i henhold til ekomloven, bransjenormer for håndtering av spam og andre trusler ved bruk av epost samt sikring av domenenavnsystemet [79, kap. 9.4.4].

De siste årene har det vært etablert flere institusjoner med ulike oppgaver innenfor informasjonssikkerhet. Disse er VDI, NorCERT, NorSIS og SERTIT. Institusjonene har blitt tildelt oppgaver innenfor sine respektive mandater. Det er viktig at helheten i satsingen på informasjonssikkerhet og samarbeidet mellom institusjonene ikke svekkes selv om det er foretatt en oppdeling av arbeidsoppgaver på ulike institusjoner. Myndighetene har lagt opp til at institusjonene skal samarbeide med hverandre, noe som ser ut til å bli gjort. For eksempel er NorCERT/VDI og NorSIS i jevnlig kontakt med hverandre for utveksling av informasjon og erfaringer.

Det er verdt å påpeke at NorCERT/VDI og NorSIS ikke er fullfinansiert over statsbudsjettet, men at næringslivet i stor grad også bidrar årlig med midler til disse institusjonene.

NorSIS ble etablert som et prøveprosjekt i 2004. Riksrevisjonen stilte spørsmål ved nytten av senteret idet det ble innrapportert mindre enn fem sikkerhetshendelser fra målgruppen samme året. Senteret ble permanent etablert i 2006, og etter en endring i mandatet har senterets fokus blitt vridd mer mot bevisstgjøring og rådgivning. Målgruppen er i hovedsak små og mellomstore bedrifter samt kommunesektoren, men også privatpersoner er ment å kunne nyttiggjøre seg av NorSIS. Bevisstgjøring og holdningsskapende arbeid rundt informasjonssikkerhet er viktig, men dette arbeidet er en langsiktig prosess. Det tar tid å endre holdninger, og følgelig tar det tid før man ser effekten av det holdningsskapende arbeidet. Arbeidet medinformasjonssikkerhett i mange kommuner går fortsatt svært sakte fremover, mens tilstanden for større virksomheter i næringslivet ser ut til å være endel bedre. Mindre bedrifter har derimot også et stykke igjen å gå før de kan sies å være på et tilfredsstillende nivå [9]. Dette bekreftes også av Mørketallsundersøkelsen 2003/2006.

Nettvett.no er et informasjons- og veiledningstiltak som ble opprettet i 2005 av PT på forespørsel fra SD. En rekke aktører, herunder NorSIS, Telenor og NSR, er bidragsytere til nettstedet og kvalitetssikrer informasjonen som publiseres [64]. Nettstedet retter seg mot private samt små og mellomstore bedrifter, og dekker viktige temaer innenfor hver av målgruppene. Som eksempler på relevante temaer for privatpersoner nevnes nettbank og e-handel, mens det for bedrifter nevnes risikovurdering og hjemmekontor. Temaene er presentert på en kortfattet og oversiktlig måte som også personer med ikke-teknisk bakgrunn burde kunne forstå. Nettstedet hadde i 2006 ca. 222 900 besøkende [45].

VDI ble etablert som et prøveprosjekt i 2000 med forankring i EOS-tjenestene.Inntrengningsdeteksjon har et begrenset antall tilkoblede virksomheter som anses å være en del av nasjonal kritisk infrastruktur eller kritiske samfunnsfunksjoner. Rundt 10–15 virksomheter var tilkoblet systemet ved oppstart, og det etterstrebes at de tilkoblede virksomhetene skal være representativt for nasjonale, kritiske virksomheter. Frem til idag har det sannsynligvis vært en liten økning i antall deltagere. Det begrensede antallet tilkoblede deltagere skyldes primært tekniske begrensninger. Det er uheldig hvis begrensningen i antall deltagere går på bekostning av nøyaktigheten av representasjonen i utvalget.

Nytteverdien av å ha et system som VDI ble raskt lagt merke til, og etter prøveperioden ble VDI permanent etablert i 2003. På bakgrunn av erfaringene fra VDI, ble prosjekt NorCERT opprettet ikke lenge etter i 2004 og VDI ble innlemmet som en seksjon

i NorCERT. NorCERT fikk ansvar for analyse og trusselvurdering, rådgivning og assistanse ved håndtering av større sikkerhetshendelser i tilknytning til Internett [79, kap. 9.4.3]. VDI overvåker kun et begrenset antall kritiske systemer, men alle virksomheter som er å regne for samfunnskritisk infrastruktur eller samfunnskritiske funksjoner kan få hjelp fra NorCERT ved alvorlige sikkerhetshendelser. Det er uklart i hvor stor grad NorCERT/VDI har nådd målene sine, da mye av denne informasjonen er gradert konfidensiell. Det er derimot lite tvilsomt at NorCERT/VDI har, er og vil fortsette å være et viktig redskap ved alvorlige sikkerhetshendelser i tilknytning til nasjonal kritisk infrastruktur.

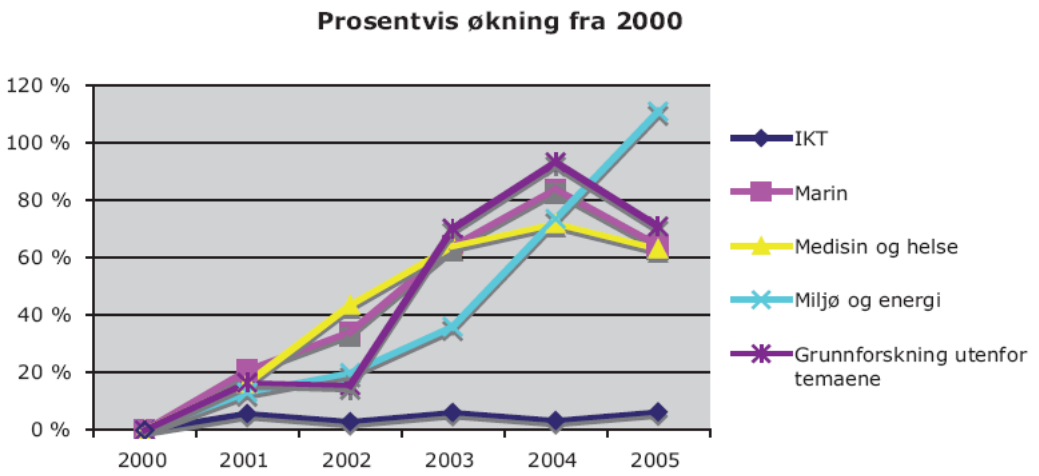
NorCERT/VDI sin moderorganisasjon, NSM, har også en relevant rolle i myndighetenes satsing på informasjonssikkerhet. I tillegg til NorCERT/VDI, er også sertifiseringsordningen SERTIT underlagt NSM. NSM ble opprettet i 2003 etter tidligere å ha fungert som stab i Forsvarets overkommando. Direktoratet er finansiert over budsjettet til FD, og har naturlig nok størst fokus på militær sektor. Samtidig rapporterer direktoratet også til JD for sivile anliggender. NSM sin primæroppgave er å koordinere forebyggende sikkerhetstiltak og kontrollere sikkerhetstilstanden i virksomheter som omfattes av Sikkerhetsloven. Viktige samarbeidspartnere for NSM er PST og DSB.

SERTIT er en sertifiseringsordning underlagt NSM. Ordningen ble opprettet gjennom bevilgninger i St.prp.nr. 1 (1998–1999), men først fra høsten 2002 var SERTIT operativ og ble etablert under NSM [26, kap. 5.2.2]. I Nasjonal strategi for informasjonssikkerhet oppfordres norske virksomheter til å ta i bruk etablerte standarder for IT-sikkerhet og sertifisere produkter og systemer. Ordningen er relativt lite kjent i næringslivet, spesielt blant små og mellomstore bedrifter. Det er heller ikke økonomisk lønnsomt for bedrifter flest (og særlig de mindre) å sertifisere produktene eller systemene sine, siden sertifisering er en tidkrevende og kostbar prosess. NSM har uttalt at de ønsker at offentlig sektor bør gå foran med et godt eksempel og selv kjøpe inn sertifiserte produkter og systemer, men FAD har kommentert at de ikke har noen planer for å fremme ordningen idet den må anses å være markedsbasert. Bransjeorganisasjonen IKT-Norge mener at offentlig sektor ofte har et stort fokus på pris som gjør at den velger bort sertifiserte produkter og systemer [26, kap. 5.2.3].

Forskning på informasjonssikkerhet har de senere årene har fått et løft takket være forskningsprogrammet IKT SoS i regi av NFR og BAS5 prosjektet ved FFI. IKT SoS er nå avsluttet, og programmet finansierte blant annet 15 PhD stipendiater og 2 post doc stipendiater. Forskningsprogrammet SAMRISK vil sannsynligvis inkludere informasjonssikkerhet, men i et begrenset omfang. Det er også mulig at VERDIKT vil gi enkelte midler til forskning hvor informasjonssikkerhet er involvert som tema. I St.meld. nr. 17 (2006–2007) gis det uttrykk for at Norges satsing på forskning innen informasjonssikkerhet er lav i internasjonal sammenheng. Figur 8.1 illustrerer stagneringen i økte bevilgninger til IKT-forskning fra 2000 til 2005.

Kun 0,24% av BNP ble benyttet til IKT-forskning i 2003, et tall som plasserer Norge i nedre halvdel av OECD landene. Finland topper listen med 1,27%, mens tilsvarende tall for Sverige er ca. 1%. Den lave andelen for Norge kan dels tilskrives et høyt BNP og relativt lav samlet forskningsinnsats i næringslivet. Vurderer man IKT-forskning i næringslivet opp mot den totale forskningsinnsatsen i næringslivet, kommer Norge bedre ut og havner i samme kategori som Danmark og Frankrike [79, kap. 5.3].

BAS5 prosjektet ble formelt avsluttet i 2007. NSM og DSB hadde vanskeligheter med å samle inn midler for å starte opp prosjektet, og prosjektet mottok halvparten av sine



Figur 8.1: *Prosentvis utvikling av Forskningsrådetstildelingerr til de fem prioriterte områdene i forskningsmeldingen fra 1999 [79, kap. 5.3].*

midler gjennom IKT SoS. Det er bekymringsfullt at det var vanskelig å samle inn nok midler, siden BAS5 var viktig for sikkerhet- og beredskapsarbeid på tvers av sektorene. Sannsynligvis var finansieringen vanskelig nettopp fordi prosjektet hadde nytteverdi på tvers av sektorene samtidig som det ikke fantes én hovedinteressent blant disse sektorene.

Prosjektene i BAS-serien har vært organisert ad-hoc og som spleiselag mellom ulike aktører. Et noe annet mandat og en annerledes finansieringsmodell kunne gitt bedre kontinuitet i fremgangen og økt forutsigbarhet for de involverte. Samtidig ville man forhindret at den kompetansen som FFI har opparbeidet seg på området kritisk infrastruktur og informasjonssikkerhet ikke svekkes. Det er per idag ikke planlagt noen arvtager til BAS5 [22].

Offentlig sektor har et overordnet ansvar for å sikre informasjonssikkerheten i samfunnet. Ansvarsområdene inkluderer blant annet sikring av kritisk infrastruktur, bevisstgjøring og veiledning, hendelseshåndtering samt utdanning og forskning. Det er i myndighetenes egeninteresse at informasjonssikkerheten er på et tilstrekkelig nivå i samfunnet. Med sårbar IKT-infrastruktur og lite sikre IKT-tjenester vil det fort oppstå problemer av stort omfang. Problemene kan resultere i forbigående driftsforstyrrelser eller lengre driftsavbrudd for kritiske samfunnsfunksjoner og infrastruktur slik som kraftforsyning og sykehus. Upålitelig kritisk IKT-infrastruktur og usikre IKT-tjenester kan i siste instans føre til at brukerne slutter å bruke infrastrukturen og tjenestene. Målet med å bruke IKT i offentlig sektor er først og fremst å effektivisere sektoren, og da må myndighetene sikre sikkerheten rundt bruken og den kritiske infrastrukturen. Hvis ikke sikringen er god nok, kan i beste fall effektiviteten gå ned på grunn av økt ressursbruk når sikkerhetshendelser oppstår. Utilstrekkelig sikring kan dog få langt større konsekvenser enn dette. I 2006 ble for eksempel flere nettbanker og halvparten av alle landets minibanker utilgjengelige i to timer på grunn av en feil hos EDB fellesdata [105].

En tilstrekkelig grad av informasjonssikkerhet er nødvendig i samfunnet for å ivareta brukernes tillit. Uten denne tilliten forsvinner brukerne tjenestene er ment for. Majoriteten av tiltakene myndighetene har iverksatt er forebyggende eller proaktive. Denne typen tiltak

er nødvendig for i størst mulig grad forhindre at uønskede hendelser oppstår. Reaktive tiltak er viktige for å håndtere uønsket hendelse som allerede har oppstått. NorCERT er et eksempel på en avdeling som arbeider både proaktivt og reaktivt. NorCERT driver med analyse og utarbeider trusselvurderinger, men samtidig er enheten også ansvarlig for hendelseshåndtering. NorSIS arbeider på sin side med forebyggende problemstillinger. Det er verdt å nevne at tiltak også kan deles inn i andre kategorier, for eksempel organisatoriske, tekniske og økonomiske.

Hva gjør privat sektor for å styrke informasjonssikkerheten i samfunnet?

Før dette spørsmålet besvares er det interessant å betrakte i hvilken grad privat sektor *bør* være ansvarlig for informasjonssikkerhet i samfunnet. Da staten hadde monopol i telesektoren, var naturligvis myndighetene ansvarlige for sikkerhet- og beredskap for sektoren. Med avviklingen av monopolet kom det etterhvert flere private aktører som konkurrerte seg imellom. Fri markedsøkonomi leder til økt konkurranse og effektivisering i den aktuelle sektoren. Samtidig settes det et større fokus på fortjeneste som offentlig sektor ikke har. Når private aktører overtar ansvar for kritisk infrastruktur og andre kritiske samfunnsfunksjoner, må de også ta sin del av ansvaret som staten har hatt før overtakelsen. Staten har etter en slik overdragelse til privat sektor en langt mindre økonomisk og organisatorisk kontroll, og kan bare øve innflytelse gjennom regulering av offentlig lovverk og tilsynsvirksomhet. Dersom staten finner det nødvendig, kan det utstedes pålegg. Til tross for de relativt begrensede virkemidler staten har til rådighet, forventer likevel innbyggerne at staten ivaretar sikkerheten og beredskapen i samfunnet med disse virkemidlene [79, kap. 5.3].

Sikkerhet og beredskap er godt regulert gjennom i offentlig lovverk, og et antall tilsyn har ansvar for å følge opp de aktuelle virksomhetene og at disse overholder bestemmelsene i lovverket. Likevel kan det være forholdsvis lett å skjule manglende sikkerhet- og beredskapsarbeid [79, kap. 5.3]. For et mest mulig effektivt samarbeid er det viktig å bygge opp en gjensidig tillit mellom offentlige tilsyn og private aktører på området.

Det finnes flere aktører i privat sektor som er involvert i arbeid med å styrke informasjonssikkerhet. Bransjeorganisasjonene IKT-Norge og Abelia har for eksempel vært i kontakt med departementene vedrørende utforming og oppfølging av Nasjonal strategi for informasjonssikkerhet i næringslivet.

Foreningen for Kommunal informasjonssikkerhet (KInS) ble stiftet i 2003. Siden 1. april 2007 har KInS vært organisert som en faggruppe under NorSIS. KInS arbeider med å styrke informasjonssikkerheten i kommunesektoren (kommuner og fylkeskommuner), en målgruppe som også NorSIS sikter mot. KInS har arbeidet med å bygge opp et nettverk av kontakter innen kommune- og fylkessektoren, og har videre arrangert konferanser i ulike kommuner. Det arbeides også for å holde konferanser på fylkesnivå. I 2006 deltok 23% av Norges kommuner på minst én konferanse arrangert av KInS. Kommunesektoren er en viktig målgruppe for styrking av informasjonssikkerhet i offentlig sektor. Ofte har kommunene begrensede midler og ressurser og velger derfor å nedprioritere sikkerhet- og beredskapsarbeid. En økt bevisstgjøring rundt temaet er derfor viktig for å få det på dagsordenen.

Næringslivets sikkerhetsråd (NSR) er et rådgivende organ for næringslivet vedrørende spørsmål om kriminalitet. Målet er å forebygge tap i private virksomheter som følge av kriminelle handlinger. Et viktig arbeid som NSR gjør er å kartlegge datakriminalitet og

andre uønskede hendelser gjennom mørketallsundersøkelser. Dette gir grunnlag for å vurdere sikkerhetstilstanden i virksomhetene samt avdekke typiske sårbarheter. Den siste undersøkelsen ble utført i 2006 i samarbeid med blant annet KRIPOS, NorSIS og NorCERT. Undersøkelsen brukes av offentlig såvel som privat sektor, og har blant annet blitt brukt i St.meld. nr. 17 (2006–2007) for å tegne et bilde av tilstanden i norske virksomheter.

Skillelinjene mellom private og offentlige organisasjoner kan av og til være noe utydelige. NorCERT/VDI og NorSIS er eksempler på institusjoner som samfinansieres av offentlig og privat sektor. Myndighetene har det overordnede ansvaret for NorCERT/VDI og NorSIS, men brukergruppene består av virksomheter fra privat såvel som offentlig sektor. NorCERT/VDI mottar 3 av 8 mill. kr. i sitt budsjett fra privat sektor, mens NorSIS får 2 av totalt 6 mill. kr. fra privat sektor.

Gjøvik kunnskapspark (GKP) har gjort en god jobb i å samle virksomheter med informasjonssikkerhet som hovedområde. Både NorSIS, KInS, NISlab (HiG) og Bluelightnettverket ligger under GKP. I tillegg eksisterer det også et inkubatorprogram innen informasjonssikkerhet i regi av GKP. Her kan gründere med sikkerhetsprosjekter få verdifull støtte i etableringen av nye virksomheter.

I Nasjonal strategi for informasjonssikkerhet rettes det et økt fokus mot tiltak i privat sektor. Det er naturlig at en stor del av strategien involverer næringslivet siden det er ansvarlig for kritisk infrastruktur og kritiske samfunnsfunksjoner. Det er positivt at privat sektor kan ha deler av ansvaret for slik infrastruktur og slike funksjoner, men det er likevel viktig at det blir ført grunding tilsyn fra myndighetens side for å kontrollere at lovgivning om sikkerhet og beredskap følges.

Hvordan skiller arbeidet med informasjonssikkerhet seg i Sverige fra det som skjer i Norge?

Denne oppgaven har også tatt for seg svenske myndigheters satsing informasjonssikkerhet. I denne sammenheng er det stilt følgende spørsmål:

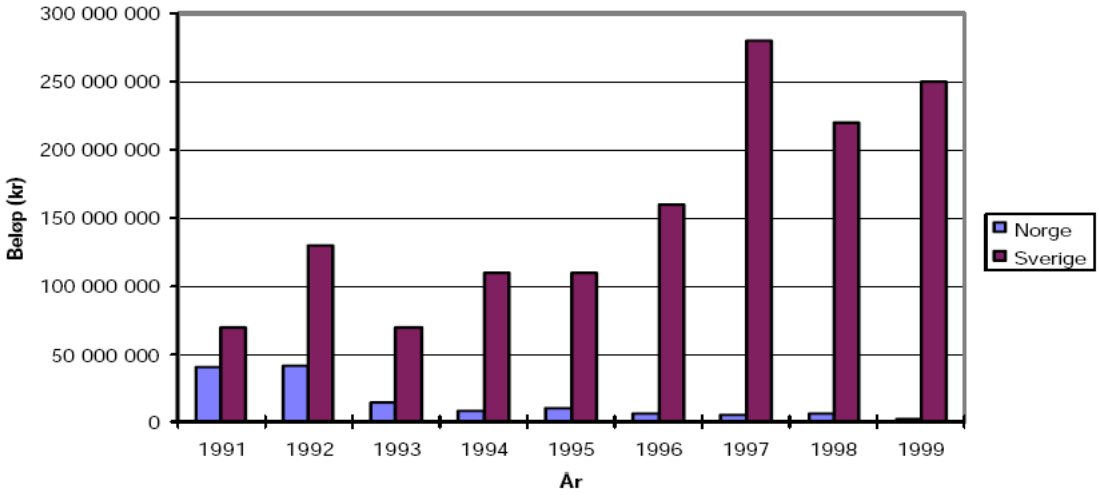
- Hvilke tiltak er foreslått og implementert i Sverige for å bedre informasjonssikkerheten?
- Hvordan skiller arbeidet med informasjonssikkerhet seg i Sverige fra det som skjer i Norge?

Det første spørsmålet vedrørende foreslåtte og implementerte tiltak, er besvart i kapittel 7.

Det andre spørsmålet er ikke besvart tidligere i oppgaven.

Avmonopoliseringen av telemarkedet i Sverige har foregått noe raskere enn i Norge og de fleste andre europeiske land [58, kap. 4.3]. Den raskere utviklingen i Sverige var sannsynligvis en medvirkende faktor til at landet var tidligere ute enn Norge i arbeidet med å utrede IKT og samfunnets sårbarhet. I BAS2 prosjektet ble det pekt på at Sverige investerte mer enn Norge i sikringstiltak på 1990-tallet [58, kap. 4.3]. Argumentet med en tidligere avmonopolisering kan likevel ikke brukes til å forsvare utviklingen som foregikk på 1990-tallet. Figur 8.2 sammenligner ressursbruk i Norge og Sverige med hensyn på nye sikringstiltak implementert på 1990-tallet. Selv omsammenligningenn er gjort direkte og uten korrigeringer, gir den allikevel et entydig bilde av hvordan landene prioriterte på 1990-tallet. Sverige sine investeringer i sikringstiltak økte stort sett jevnt utover hele

perioden, mens det i Norge var en motsatt utvikling. I rapporten til BAS2 prosjektet ble det sagt at "statlig finansiering av sårbarhetsreduserende tiltak i en eller annen form vil være nødvendig. I stort handler dette om å få politisk forståelse for konsekvenser og behov" [58, kap. 4.3]. Det vites ikke hvordan de tilsvarende tallene mellom Norge og Sverige har vært fra 2000 og frem til idag.



Figur 8.2: *Sammenligning av investeringer i "friske" sikringstiltak i Norge og i Sverige i perioden 1991–1999 (tall for 1999 er anslag) [58]*

Begge landene har i senere tid utført flere utredninger og prosjekter knyttet til informasjonssikkerhet. Tabell 8.1 angir tidsløpet for Norge og Sverige sine utredninger om samfunnets sårbarhet og informasjonssikkerhet. Utredninger av noenlunde samme karakter er plassert ved siden av hverandre.

Norge		**Sverige**	
TIFKOM [a]	1997–1999	AgIW/AgIO [b]	1997–1998
IT-sårbarhetsprosjektet [c]	1999–2000	Mandatorraporten	1999
Sårbarhetsutvalget	1999–2000	Sårbarhetsutredningen	1999–2001
Infrastrukturutvalget	2006	InfoSäkutredningen	2003–2005

[a] Teleberedskap i fritt konkurransemarked.
[b] Arbeidsgruppen for Information Warfare/Information Operations.
[c] Utført under Nærings- og handelsdepartementet. Samarbeidet med Sårbarhetsutvalget.

Tabell 8.1: *Sammenligning av relevante norske og svenske utredninger og tidsperioder for disse.*

I Sverige avleverte arbeidsgruppen for Information Warfare (AgIW) rapport i august 1997, og videreføringen av denne rapporten kom i august 1998 med arbeidsgruppen for Information Operations (AgIO).

I Norge gjennomførte FFI prosjektet "Teleberedskap i fritt konkurransemarked" (TIFKOM) i perioden september 1997 – februar 1999. TIFKOM utredet sårbarhet og sårbarhetsreduserende tiltak innen offentlig telekommunikasjon. Det norske IT-sårbarhetsprosjektet ble påbegynt i november 1999 på oppdrag fra NHD. Samme året avleverte det svenske IT-konsulent selskapet Mandator den såkalte Mandatorrapporten (desember 1999). Rapporten fra det norske prosjektet om IT-sårbarhet ble avlevert oktober 2000, og prosjektgruppen samarbeidet med Sårbarhetsutvalget som utførte sitt arbeid i perioden september 1999 – juli 2000. IT-sårbarhetsprosjektet viste til USA som et foregangsland på området, og deres arbeid "Critical Foundations – Protecting Americas Infrastructures" som ble offentliggjort i 1997. Sverige ble nevnt som et land som hadde "kommet et godt stykke på vei" med dette arbeidet [106, kap. 1.1].

I Sverige ble det i juni 1999 besluttet å utrede samfunnets sårbarhet. Sårbarhets- og säkerhetsutredningen avla sin rapport i mai 2001, etter å ha fått mandatet sitt utvidet på bakgrunn av direktiver vedtatt i juni og desember 2000 [99].

I Norge ble Sårbarhetsutvalgets anbefalinger fulgt opp hovedsaklig gjennom Nasjonal strategi for informasjonssikkerhet fra 2003. En nasjonal handlingsplan for informasjonssikkerhet i Sverige holder på å utarbeides avKrisberedskapsmyndighetenn og skal presenteres i 2008 [97]. Svenske PTS følger en annen strategi i sitt arbeide, nemlig "Strategi för ett säkrare Internet i Sverige" som var ferdigstilt juli 2006.

I Sverige ble det utført fire delutredninger i forbindelse med Informationssäkerhetsutredningen som fulgte opp Sårbarhets- og säkerhetsutredningen. Delutredningene ble utført i perioden 2003–2005 og omhandlet kommunikasjonsbeskyttelse (signalskydd), informasjonssikkerhet i Sverige kontra andre land, forslag til informasjonssikkerhetspolitikk og organisatoriske konsekvenser av denne politikken. I Norge har for eksempel informasjonssikkerhetspolitikken og organisatoriske konsekvenser kommet til syne gjennom arbeidet med Nasjonal strategi for informasjonssikkerhet. Norge har i motsetning til Sverige ikke hatt nasjonale utredninger som har fokusert utelukkende på informasjonssikkerhet. Det norske Sårbarhetsutvalget drøftet informasjonssikkerhet i sammenheng med kritisk infrastrukturer generelt. Det samme gjorde Infrastrukturutvalget som utførte sitt arbeid i perioden oktober 2004 – april 2006.

Begge lands myndigheter har fått en ekstern vurdering av arbeidet med nasjonal informasjonssikkerhet. I november 2005 presenterte den norske Riksrevisjonen sin rapport, og svenske Riksrevisionen avla sin rapport nå nylig 1. juni 2007. Begge rapportene har en rekke punkter med kritikk mot de respektive myndigheters arbeid med informasjonssikkerhet. Et fellestrekk er at det pekes på dårlig oppfølging og kontroll av arbeidet.

Infrastrukturutvalget spiller en sentral rolle i oppfølgingen av Sårbarhetsutvalget. Begge disse utvalgene har prøvd å favne så bredt som mulig og har tatt for seg alle samfunnets sektorer. En slik bred innfallsvinkel til problemstillingen er god nok til å gi et overordnet, om enn noe grovt, bilde av situasjonen. Problemet er at antallet utvalgsmedlemmer er begrenset, og at det derfor blir relativt lite ekspertise og kompetanse som er representert fra den enkelte sektor i utvalget. Sårbarhetsutvalgets IKT-underutvalg og dets fokus på den logiske trusselen ble viet mindre oppmerksomhet i sluttrapporten enn BAS2 prosjektet som hadde hovedvekt på fysisk sikring [16]. Det er enormt viktig at det finnes tilstrekkelig kompetanse i utvalgene innen det fagområdet de utreder, idet det kan være vanskelig for underutvalg, referansegrupper eller andre rådgivende organer å formidle informasjon

av meget teknisk eller på annen måte komplisert karakter på en tilstrekkelig klar og god måte. I de tre utvalgene som har vært drøftet i denne rapporten har den teknisk kompetansen vært underrepresentert. Det er forståelig at myndighetene ønsker å favne så bredt som mulig når den nasjonale sikkerhetstilstanden skal analyseres, men man må være veldig forsiktig når man prioriterer bredde fremfor dybde med hensyn på den kompetansen utvalgsmedlemmene har. Feil prioritering kan lede til et feilaktig bilde av den tilstanden man ønsker å kartlegge.

I Sverige har man fulgt opp Sårbarhetsutredningen med en egen utredning innen informasjonssikkerhet, InfoSäkutredningen. Utredningen har foregått i perioden 2003–2005 og fire delrapporter har vært avlevert. En egen utredning viet til informasjonssikkerhet gir en dypere forståelse av problemstillingene på myndighetsnivå. Samtidig oppnår man et bedre fokus på problemstillingene fra myndighetenes side, idet temaet er klart avgrenset og ikke omfatter problemstillinger i alle sektorer.

Det påpekes i SOU 2004:32 – "Informationssäkerhet i Sverige och internationellt" at det er vanskelig å direkte sammenligne organisasjonsmodeller mellom ulike land. Selv om landene ofte står overfor de sammen problemstillingene i informasjonssikkerhet, spiller eksisterende organisasjonsstruktur en stor rolle for organiseringen av arbeidet. Sveriges IT-incident centrum (Sitic), Post- og telestyrelsen (PTS), Försvarets radioanstalt (FRA), Totalförsvarets signalskyddsavdelning (TSA) og Krisberedskapsmyndigheten (KBM) er sentrale organisasjoner i Sveriges arbeid med informasjonssikkerhet. PTS har tilsvarende funksjon som norske PT. KBM minner om norske DSB og Sitic ligner delvis på NorSIS. FRA er enetterretningstjenestee spesialisert på kommunikasjonsteknologi, mens TSA er ansvarlig for beskyttelse av totalforsvarets kommunikasjon. Institusjoner i Norge som dekker noenlunde de samme ansvarsområdene som disse to er PST og NSM.

Sitic ble opprettet 1. januar 2003 og mandatet ligner som sagt på NorSIS sitt. Det er likevel flere organisatoriske forskjeller. Sitic er underlagt PTS, mens NorSIS ikke er underlagt tilsvarende norske PT. Den nasjonale CERT funksjonen i Sverige ligger hos Sitic, mens den i Norge ligger hos NorCERT. Sitic er fullfinansiert gjennom Näringsdepartementet, mens NorSIS og NorCERT er delvis finansiert av næringslivet [97]. Sitic har ikke et særskilt ansvar for overvåking av kritisk infrastruktur, men har sensorer innen flere sektorer, herunder Internettilbydere [97]. NorSIS er på sin side ikke involvert i overvåkning av kritisk infrastruktur, men det er derimot NorCERT. Det er verdt å nevne at Mørketallsundersøkelsen 2005 for Sverige ble gjennomført av Sitic. Sitic samarbeidet ikke med Näringslivets Säkerhetsdelegation om undersøkelsen. I Norge bidro SIS/NorSIS sammen med NSR og andre aktører til gjennomføringen av Mørketallsundersøkelsen 2003/2006.

Sitic har et årlig budsjett på 15 MSEK (fullfinansiert gjennom staten), og dette budsjettet vil antageligvis øke til 20 MSEK [97]. Til sammenligning har NorCERT og NorSIS tilsammen et budsjett på totalt 14 MNOK. Det er vanskelig å si nøyaktig hva forskjellen i økonomiske bevilgninger er på, siden organisasjonene ikke har et likt mandat. En nøyaktig sammenligning krever korrigering for ulike funksjoner som dekkes av organisasjonene, samt korrigering for antall innbyggere og virksomheter som organisasjonene har som målgruppe.

Kapittel 9

Konklusjon

Denne oppgaven har evaluert myndighetenes nasjonale satsing på informasjonssikkerhet. En del av denne evalueringen har foregått gjennom en vurdering av tiltakene som ble anbefalt av tre sentrale utvalg vedrørende informasjonssikkerhet: Sårbarhetsutvalget, Infrastrukturutvalget og Datakrimutvalget.

Sårbarhetsutvalget avleverte rapport i 2001 og anbefalte å etablere et nasjonalt, helhetlig apparat rundt informasjonssikkerhet. De viktigste tiltakene som ble foreslått var etableringen av en nasjonal strategi for informasjonssikkerhet, VDI, SIS og et strategisk forskningsprogram for IKT-sårbarhet (BAS5). Alle tiltakene ble senere gjennomført, men den gode uttellingen på antall utførte tiltak må også tillegges den lange tiden som har gått siden utvalget leverte sin rapport. Det er grunn til å stille spørsmål om nøyaktig hva som ble gjort som et konkret resultat av utvalgets anbefalinger, siden andre prosesser også påvirket arbeidet underveis. Det tok forøvrig hele fire år før SIS ble opprettet som prøveprosjekt og BAS5 ble påbegynt, noe som indikerer treghet eller manglende vilje i forvaltningen.

Infrastrukturutvalget er ett av flere utvalg som har fulgt opp tiltakene fra Sårbarhetsutvalget. Utvalget avleverte rapport i 2006 og konkluderte med at ansvarsfordelingen for sikkerhet- og beredskapsarbeid burde tydeliggjøres, og at JD sin rolle som overordnet koordinator for sikkerhet- og beredskapsarbeid burde avklares formelt. Det ble anbefalt å samordne ansvaret for IT-sikkerhet hos JD, FAD og SD til ett departement med overordnet ansvar for IT-sikkerhet. Det ble videre foreslått å gjennomføre endringer i Sikkerhetsloven vedrørende objektsikring, utvide FFI sitt mandat til å omfatte sivil sektor, etablere et program for finansiering av tverrsektorielle tiltak uten hovedinteressent samt et program for å forplikte sektorene til jevnlig å utføre ROS-analyser. Utvalget anbefalte også å pålegge utstyrsleverandører å sikre trådløse nettverkskomponenter samt pålegge Internettilbyderne å legge ved sikkerhetsprogramvare til kundene sine.

Datakrimutvalget avleverte sin første utredning i 2003 i forbindelse med at Norge skulle ratifisere EUs datakrimkonvensjon som innehold et felles sett med straffebestemmelser, straffeprosessuelle forpliktelser og regler for internasjonalt samarbeid. Konvensjonen ble ratifisert, og det fantes allerede hjemmelgrunnlag i norsk lovgivning for å godkjenne majoriteten av artiklene med få eller ingen endringer. I 2007 avleverte utvalget delutredning II vedrørende nasjonale straffebestemmelser for datakriminalitet. Problemstillingene rundt datakriminalitet reiser så mange spørsmål at man er tjent med en særregulering, og derfor

laget utvalget et forslag til et eget kapittel i straffeloven om emnet. Kapittelet inneholder mange hensiktsmessige og gode bestemmelser, herunder kriminalisering av spam og spredning av tilgangsdata. På den andre siden kriminaliserer bestemmelsene i overkant mye ved å inkludere elektronisk kartlegging og befatning med skadelige dataprogrammer. Dette er såkalte forberedelseshandlinger som ifølge tradisjonell norsk rettspraksis er straffrie. Et mindretallsforslag om filtrering av Internett foreligger også i utvalgets rapport. Dersom alle bestemmelsene inkluderes i lovverket, vil Norge få en svært restriktiv lovgivning på området.

Sårbarhetsutvalget hadde i sin rapport et fokus på etablering av et helhetlig og nasjonalt apparat for informasjonssikkerhet. Infrastrukturutvalget (og Riksrevisjonen) har i sin rapport vektlagt organiseringen av det arbeidet apparatet utfører. Graden av fremgang mellom Sårbarhetsutvalget og Infrastrukturutvalget har naturligvis vært stor siden det er seks år mellom de, og i denne perioden har både VDI, NorSIS og NorCERT blitt opprettet. Infrastrukturutvalget er dog kun én av flere aktører som har fulgt opp arbeidet fra Sårbarhetsutvalget. Den viktigste drivkraften for informasjonssikkerhetsarbeid i perioden mellom disse to utvalgene har vært Nasjonal strategi for informasjonssikkerhet som kom i 2003. Denne strategien er viktig for å sikre et kontinuerlig fokus på informasjonssikkerhet fra myndighetenes side. Fremdriften med å nå de strategiske målene har dessverre ikke vært like høy som forventet, og ifølge Riksrevisjonen skyldes dette primært manglende ansvarsavklaring på departementnivå.

Sårbarhetsutvalget var inne på problemstillingen med datakriminalitet og et utdatert lovverk, men foretok ingen grundige drøftelser som kunne danne grunnlag for lovendringer. Dette temaet har nylig blitt behandlet av Datakrimutvalgets delutredning II. Det er ennå for tidlig å vurdere oppfølgingen av Datakrimutvalgets anbefalinger. Det samme er tilfellet for Infrastrukturutvalgets anbefalinger.

Offentlig sektor sitt arbeid med å styrke samfunnets informasjonssikkerhet skjer gjennom mange organisasjoner og organer. Arbeidet med å styrke informasjonssikkerhet inkluderer blant annet sikring av kritisk infrastruktur, bevisstgjøring og veiledning, analyse og hendelseshåndtering og forskning. Disse funksjonene dekkes delvis av henholdsvis PT, NorSIS, NorCERT/VDI og FFI. Andre aktører er også involvert i disse arbeidene, men de forutnevnte gir et godt bilde av ulike aspekter ved informasjonssikkerhet som offentlig sektor arbeider med.

Privat sektor har et ansvar for informasjonssikkerhet i samfunnet idet sektoren er eier/operatør av samfunnskritiske infrastrukturer. Offentlige organisasjoner som arbeider med informasjonssikkerhet har ofte deler av næringslivet som viktige samarbeidspartnere. For eksempel samarbeider PT med de private aktørene i telesektoren for å kartlegge infrastruktur og utføre ROS-analyser.

Privat sektor bidrar med en betydelig del av midlene for driften av NorSIS og NorCERT. Dette er naturlig siden disse organisasjonene har privat sektor som en av sine målgrupper. Ellers kan det nevnes at næringslivet bidro mye til opprettelsen av mastergradsstudiet i informasjonssikkerhet ved HiG, blant annet gjennom økonomiske tilskudd.

NSR arbeider med spørsmål om kriminalitet og forsøker å forebygge tap. Organisasjonens arbeid omfatter også datakriminalitet, og NSR har frem til idag utført fem mørketallsundersøkelser som tegner et bilde av tilstanden for informasjonssikkerhet i norske virksomheter. Denne informasjonen er nyttig for offentlig såvel som privat sektor.

Sverige var tidligere ute enn Norge på 1990-tallet med å kartlegge sårbarhet og informasjonssikkerhetstrusselen, men Norge har hatt Nasjonal strategi for informasjonssikkerhet siden 2003. I Sverige er det nærmeste man kommer en slik strategi den nasjonale handlingsplanen for informasjonssikkerhet som utarbeides av KBM og er forventet ferdig i 2008. På en annen side har Sverige utført en omfattende utredning i fire deler som utelukkende har fokusert på informasjonssikkerhet, nemlig Informationssäkerhetsutredningen (2003–2005). I Norge har det ikke vært foretatt en lignende utredning.

Både Norge og Sverige har fokus på en helhetlig tilnærming til informasjonssikkerhet i samfunnet. Det eksisterer naturlig nok forskjeller i organisasjonsstruktur som gjør at landene utfører oppgavene på ulik måte selv om problemstillingene er de samme. Likevel er det et tildels stort samsvar mellom organisasjoner i Norge og Sverige, eksempelvis mellom Sitic og NorSIS/NorCERT. En viktig forskjell er at Sitic i motsetning til NorCERT ikke har et særskilt ansvar for overvåking av kritisk infrastruktur, men Sitic har likevel sensorer innen flere sektorer for overvåkning. En annen viktig forskjell er at både NorSIS og NorCERT er delvis finansiert gjennom næringslivet, mens Sitic er fullfinansiert over statsbudsjettet.

Både Norge og Sverige har i flere omganger utredet samfunnets sårbarhet som følge av IKT-avhengighet. Undersøkelser som er gjort i denne rapporten viser at oppfølgingen av foreslåtte tiltak av ulike grunner har vært mangelfull i Sverige såvel som Norge. Dette bekreftes av de respektive riksrevisjonene som har kritisert myndighetenes oppfølging av satsingen på nasjonal informasjonssikkerhet.

Referanser

[1] Jan A. Audestad. Internet as a Multiple Graph Structure: The Role of the Transport Layer. *Information Security Technical Report*, 12(1), 2007.

[2] Jan A. Audestad. E-bomber og e-granater: Om IKT og sårbarhet, FFI/NOTAT-2005/00938.

[3] Wikipedia. Dot-com bubble. http://en.wikipedia.org/wiki/Dot-com_bubble. Sist aksessert: 17.05.2007.

[4] Ericsson. Managing network security. http://www.ericsson.com/technology/whitepapers/3075_Network_Security_A.pdf, 2006.

[5] Gerd Lilledahl og Atle Wehn Hegnes. Kvalitativ metode. http://www.giaever.com/sosiologi/KM.htm. Sist oppdatert: 22.10.2000.

[6] Wikipedia. Scale-free network. http://en.wikipedia.org/wiki/Scale-free_network, mars 2007.

[7] NorCERT – Månedsrapport: April – 2007.

[8] NorCERT. IKT-trusselbildet. http://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/IKT-trusselbildet2/. Sist aksessert: 24.05.2007.

[9] Personlig meddelelse: samtale med Tore Orderløkken ved NorSIS. 21.05.2007.

[10] Craig A. Schiller og Jim Binkley. *Botnets – The Killer Web App*. Syngress Publishing Inc., 2007.

[11] Ken Baylor og Chris Brown. Killing botnets – a view from the trenches. http://www.mcafee.com/us/local_content/white_papers/wp_botnet.pdf, oktober 2006.

[12] Stortinget. Saksgangen mellom regjeringen og Stortinget. http://www.stortinget.no/om_stortinget/saksgangen.html, 2007. Sist aksessert: 20.03.2007.

[13] Håvard Fridheim og Janne Hagen. BAS5 sluttrapport. Personlig meddelelse: epost fra Håvard Fridheim ved Forsvarets forskningsinstitutt. 12.04.2007.

[14] Justis og politidepartementet. NOU 2000: 24 - Et sårbart samfunn. http://odin.dep.no/detalj/NOU200020000024000NORHTMO/bn!15900031.html, juli 2000.

[15] SERTIT. Om SERTIT. http://sertit.no/. Sist aksessert: 17.03.2007.

[16] Personlig meddelelse: epost fra Jan A. Audestad. Audestad var medlem av IKT-underutvalget og referansegruppen til Sårbarhetsutvalget. 12.03.2007.

[17] Jan A. Audestad og Svein E. Pettersen. Telektronikk. http://www.telenor.com/telektronikk/volumes/index.php?page=ing&id1=65&id2=162&id3=832&select=05-09, 2005.

[18] Justis og politidepartementet. NOU 2006: 6 - Når sikkerheten er viktigst. http://www.regjeringen.no/en/ministries/jd/Documents-and-publications/NOUer/2006/NOU-2006-6.html?id=157408, april 2006.

[19] Nærings og handelsdepartementet. Senter for informasjonssikring: Rapport fra forprosjekt. http://www.regjeringen.no/en/ministries/nhd/Documents/Reports-and-plans/Reports/2001/Senter-for-informasjonssikring.html?id=105666, juni 2001.

[20] NorCERT. Om NorCERT. http://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/Om-NorCERT/, 2007.

[21] Forsvarets Forskningsinstitutt. BAS5 – Critical Information Infrastructure Protection. http://www.mil.no/felles/ffi/start/FFI-prosjekter/Alfover/_1014/, mars 2007.

[22] Personlig meddelelse: epost fra Håvard Fridheim, prosjektleder for BAS5 ved Forsvarets forskningsinstitutt. 16.03.2007.

[23] Personlig meddelelse: epost fra Erik Hjelmås ved NISlab (Høgskolen i Gjøvik). 24.05.2007.

[24] Personlig meddelelse: telefonsamtale med Svein Tore Jensen, kontorsjef ved Institutt for informatikk ved Universitetet i Tromsø. 24.05.2007.

[25] Koordineringsutvalget for forebyggende informasjonssikkerhet. Gjennomførte tiltak i Nasjonal strategi for informasjonssikkerhet 2003. http://www.nsm.stat.no/Documents/KIS/Publikasjoner/Utkvittering%20av%20tiltak%20nasjonal%20strategi%202003.pdf. 20.03.2007.

[26] Riksrevisjonen. Dokument nr. 3:4 (2005–2006): Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur. http://www.riksrevisjonen.no/NR/rdonlyres/1B1ECB4D-BDCD-489B-83B5-DE6B630E42BA/0/Dok_3_4_2005_2006.pdf.

[27] Norsk Akkreditering. Hva ER akkreditering? http://na.imaker.no/cgi-bin/na/imaker?id=1343. Sist aksessert: 16.03.2007.

[28] SERTIT. Om sertifiseringsordningen. http://sertit.no/Publikasjoner/Sd_001_v5_0_rev.pdf. Sist aksessert: 17.03.2007.

[29] Personlig meddelelse: epost fra Anette Kræmer ved Lovavdelingen for Justis- og politidepartementet. 02.05.2007.

[30] Personlig meddelelse: epost fra Cort Archer Dreyer ved Fornyings- og administrasjonsdepartementet. 22.05.2007.

[31] Koordineringsutvalget for informasjonssikkerhet. Notat: Vurdering av Nasjonal strategi for informasjonssikkerhet og forslag til endringer. http://www.nsm.stat.no/Documents/KIS/Arbeidsgrupper/Sluttrapport%20-%20arbeidsgruppe%20for%20videref\T1\oring%20av%20nasjonal%20strategi%20for%20informasjonssikkerhet.pdf. 15.05.2006.

[32] Personlig meddelelse: epost fra Severin Vikanes, avdelingsdirektør ved Forsvarsdepartementet. 08.06.2007.

[33] Datakrimutvalget. NOU 2003:27 - Lovtiltak mot datakriminalitet: Delutredning I, november 2003.

[34] Datakrimutvalget. NOU 2007: 2 - Lovtiltak mot datakriminalitet: Delutredning II, februar 2007.

[35] Computer Crime Research Center. The Council of Europe Cybercrime Convention. http://www.crime-research.org/articles/CoE_Cybercrime/, 2000.

[36] Wikipedia. Convention on Cybercrime. http://en.wikipedia.org/wiki/Convention_on_Cybercrime, april 2007.

[37] The World ISPA Forum og European Telecommunications Networks Operators Association (ETNO). Letter to Professor Kaspersen on Draft COE Convention, 18 April 2001. http://www.privacyinternational.org/issues/cybercrime/coe/wispa401.pdf.

[38] digi.no. Norge helt på topp i Internett-angrep. http://www.digi.no/php/art.php?id=373688, mars 2007.

[39] Forbruker.no. – Dette er sensur! http://forbruker.no/digital/nyheter/data/article1639559.ece, februar 2007.

[40] Stortinget. Innst.O. nr. 17 (2001-2002): Innstilling fra familie-, kultur- og administrasjonskomiteen om lov om endringer i markedsføringsloven. Innstillingfrafamilie-, kultur-ogadministrasjonskomiteenomlovomendringerimarkedsf\T1\oringsloven.

[41] E24.no. Oljefondet satser milliarder på kasino. http://e24.no/naeringsliv/article1746572.ece, april 2007.

[42] Kultur og kirkedepartementet. Ot.prp. nr. 44 (2002-2003). http://aad.dep.no/nn/dep/kkd/Dokument/Proposisjonar-og-meldingar/Odelstingsproposisjonar/20022003/Otprp-nr-44-2002-2003-/6/5.html?id=313926&epslanguage=NO-NY,NO-NY,NO-NY, mars 2003.

[43] Wikipedia. Internet censorship. http://en.wikipedia.org/wiki/Internet_censorship, mai 2007.

[44] Forsvarsdepartementet og Nærings-og handelsdepartementet og Justis-og politidepartementet. Nasjonal strategi for informasjonssikkerhet. http://www.nsm.stat.no/Documents/KIS/Publikasjoner/Nasjonal_strategi_for_informasjonssikkerhet.pdf, juni 2003.

[45] Post- og teletilsynet. Årsrapport 2006 fra Post- og teletilsynet. http://www.npt.no/iKnowBase/Content/101215/aarsmelding_pt_2006.pdf.

[46] Koordineringsutvalget for forebyggende informasjonssikkerhet (KIS). http://www.nsm.stat.no/kis. Sist aksessert: 21.05.2007.

[47] Personlig meddelelse: telefonsamtale med Morten Ween, programkoordinator for IKT SoS under Norges forskningsråd. 16.03.2007.

[48] Koordineringsutvalget for informasjonssikkerhet. Mandat for arbeidsgruppe for utarbeidelse av Nasjonal Strategi for Informasjonssikkerhet 2007. http://www.nsm.stat.no/Documents/KIS/Mandat%20for%20arb.gruppe%20nasjonal%20strategi.pdf, juli 2006.

[49] NorSIS. Gjør PC-en klar for Internet. http://www.norsis.no/veiledninger/teknisk/Gjxr_PC-en_klar_for_Internet.html.

[50] IDG.no. IT-budsjettene maner til forsiktighet.
http://www.idg.no/computerworld/article55017.ece.

[51] Årsrapport om betalingssystemer fra Norges bank for 2005.

[52] Tore Orderløkken. Security Incident handling og reporting – a study of the difference between theory og practice. Hovedfagsoppgave, Høgskolen i Gjøvik, 2005.

[53] Personlig meddelelse: telefonsamtale med Cristophe Birkeland. 04.06.2007.

[54] Personlig meddelelse: epost fra Per K. Brekke ved DSB. 28.05.2007.

[55] St.prp. nr. 1 (2005–2006).
http://aad.dep.no/nn/dep/fd/Dokument/Proposisjonar-og-meldingar/Stortingsproposisjonar/20052006/Stprp-nr-1-2005-2006-/6/1/9.html?id=297647.

[56] Håvard Fridheim ved Forsvarets Forskninsinstitutt. Sårbarhet i kritisk infrastruktur – Ikke minst IKT-systemer.
http://www.sikkerhetsdagene.no/Tidligere%20konferanser/2005/Fridheim.pdf.

[57] Thor Gunnar Olsen og Håvard Fridheim Ole Morten Hæsken. BAS1, Rapportnr.: 97/01459. http://rapporter.ffi.no/rapporter/97/01459.pdf.

[58] Janne Merete Hagen og Kjell Olav Nystuen. BAS2, Rapportnr.:99/00240. Personlig meddelelse: epost fra Jan Erik Torp ved FFI. 16.03.2007.

[59] Håvard Fridheim og Janne Hagen og Stein Henriksen. BAS3, Rapportnr.: 2001/02381.
http://rapporter.ffi.no/rapporter/2001/02381.pdf.

[60] Janne Hagen og Gry Hege Rodal og Erlend Hoff og Brynjar Lia og Jan Erik Torp og Steinar Gulichsen. BAS4, Rapportnr.: 2003/00929. Personlig meddelelse: epost fra Håvard Fridheim ved Forsvarets forskningsinstitutt. 16.03.2007.

[61] Post- og teletilsynet. http://www.npt.no. Sist aksessert: 10.05.2007.

[62] Lovdata. Forskrift om gebyr til Post- og teletilsynet.
http://www.lovdata.no/for/sf/sd/sd-20050221-0168.html.

[63] Samferdselsdepartementet. Ot.prp. nr. 58 (2002–2003): Lov om elektronisk kommunikasjon (ekomloven).

[64] Post- og teletilsynet med flere. Nettvett. http://www.nettvett.no.

[65] digi.no. Nå skal Norge endelig få et ekte internett.
http://www.digi.no/php/art.php?id=376607.

[66] Post- og teletilsynet. Referat fra møte i Internettgruppen.
http://www.npt.no/iKnowBase/Content/referat_mote7.pdf?documentID=49829.

[67] Personlig meddelelse: epost fra Kjetil Otter Olsen, seksjonssjef ved USIT/UiO. 14.05.2007.

[68] Post- og teletilsynet. Pts arbeid med sikkerhet og beredskap i nett.
http://www.npt.no/portal/page/portal/PG_NPT_NO_NO/PAG_NPT_NO_HOME/PAG_SIKKERHET_TEKST?p_d_i=-121&p_d_c=&p_d_v=48554.

[69] Post- og teletilsynet. Hva er kvalifiserte sertifikater?
http://www.npt.no/portal/page/portal/PG_NPT_NO_NO/PAG_NPT_NO_HOME/PAG_SIKKERHET_TEKST?p_d_i=-121&p_d_c=&p_d_v=49876.

[70] Post- og teletilsynet. Hva er SEID prosjektet? http://www.npt.no/portal/page/portal/PG_NPT_NO_NO/PAG_NPT_NO_HOME/PAG_SIKKERHET_TEKST?p_d_i=-121&p_d_c=&p_d_v=49874.

[71] Norges forskningsråd. Dette er Norges forskningsråd. http://www.forskningsradet.no/servlet/Satellite?c=Page&cid=1138650413071&pagename=ForskningsradetNorsk%2FPage%2FStandardSidemal. Sist aksessert: 09.05.2007.

[72] Personlig meddelelse: epost fra Eirik Normann, avdelingsdirektør i Norges forskningsråd ved Divisjon for innovasjon. 09.05.2007.

[73] IKT sikkerhet og sårbarhet (IKTSOS). http://www.forskningsradet.no/iktsos. Sist aksessert: 09.05.2007.

[74] Kjernekompetanse og verdiskaping i IKT (VERDIKT). http://www.forskningsradet.no/verdikt. Sist aksessert: 09.05.2007.

[75] Samfunnssikkerhet og risiko (SAMRISK). www.forskningsradet.no/servlet/Satellite?cid=1150814040080&pagename=samrisk%2FPage%2FHovedSide. Sist aksessert: 09.05.2007.

[76] NSM. Om NSM. http://nsm.stat.no/Om-NSM. Sist aksessert: 16.05.2007.

[77] Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven). http://www.lovdata.no/all/nl-19980320-010.html. Sist oppdatert: 11.05.2007.

[78] Nasjonal sikkerhetsmyndighet. VDI. http://nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/VDI/. Sist aksessert: 18.05.2007.

[79] Fornyings og administrasjonsdepartementet. St.meld. nr. 17 (2006–2007): Eit informasjonssamfunn for alle.

[80] Innst.S. nr. 49 (2004-2005): Innstilling fra forsvarskomiteen om samfunnssikkerhet og sivilt-militært samarbeid. http://www.stortinget.no/inns/inns-200405-049.html.

[81] Personlig meddelelse: epost fra Svein J. Knapskog, professor ved Institutt for telematikk ved NTNU. 10.06.2007.

[82] Institutt for telematikk ved NTNU. The NordSecMob MSc study. http://www.item.ntnu.no/acm_msc_nordsec.php. Sist aksessert: 24.05.2007.

[83] Stig Frode Mjølsnes. NTNU - Information Security Research Program. http://www.item.ntnu.no/infosik. Sist oppdatert: 02.02.2005.

[84] Høgskolen i Agder. Informasjons- og kommunikasjonsteknologi (ikt) – sivilingeniør, 5-årig master. http://hia.no/no/portaler/student_og_studier/studietilbud/informasjons_og_kommunikasjonsteknologi_ikt_sivilingenioer.

[85] Personlig meddelelse: telefonsamtale med Jose J. Gonzalez, professor ved Høgskolen i Agder. 16.03.2007.

[86] Universitetet i Tromsø. Bachelorgradsprogram i datasikkerhet. http://uit.no/matstat/datasikkerhet/17. Sist oppdatert: 24.01.2007.

[87] Universitetet i Tromsø. Mastergradsprogram i matematikk – datasikkerhet. http://uit.no/matstat/master/26. Sist oppdatert: 08.10.2004.

[88] Coding theory og cryptography group. Coding theory and cryptography research group at UiB: People. http://www.ii.uib.no/forskningsgrupper/kode/personer/index-eng.shtml#staff.

[89] Universitetsstudiene på Kjeller. http://www.unik.no.

[90] SINTEF. Konsernområdet SINTEF IKT. http://sintef.no/content/page3____6430.aspx.

[91] Personlig meddelelse: samtale med Jan Erik Østvang, styreleder i foreningen KiNS. 19.02.2007.

[92] Foreningen KInS: Om foreningen. http://www.kommunesiden.no/index.gan?id=147&subid=0. Sist aksessert: 08.03.2007.

[93] Norges kommuner pr. 01.01.2006. http://www.ssb.no/kommuner/komkat.html, februar 2007.

[94] Næringslivets sikkerhetsråd. http://www.nsr-org.no. Sist aksessert: 19.05.2007.

[95] NorSIS. Mørketallsundersøkelsen 2003 tilgjengelig. http://www.norsis.no/nyheter/337.html. Sist oppdatert: 24.11.2004.

[96] NorSIS. Mørketallsundersøkelsen 2006. http://www.norsis.no/nyheter/755.html.

[97] Personlig meddelelse: epost fra Peter Wallström ved Sveriges IT-incident centrum (Sitic). 02.05.2007.

[98] Arbetsgruppen om informationskrigföring. Åtgärder och skydd mot informationskrigföring. 15.08.1997.

[99] Sårbarhets och säkerhetsutredningen. SOU 2001:41 – Säkerhet i en ny tid.

[100] Arbetsgruppen om informationskrigföring. Åtgärder och skydd mot informationskrigföring - förslag till ansvarsfördelning m m. Personlig meddelelse: epost fra Peter Wallström ved Sitic. 02.05.2007.

[101] Mikael Lindén og Rickard Posacki og Peter Wallström. Nationella strukturer för skydd mot informationsoperationer (Mandatorrapporten). Personlig meddelelse: epost fra Peter Wallström ved Sitic. 02.05.2007.

[102] InfoSäkutredningen. SOU 2005:42 – Säker information - Förslag till informationssäkerhetspolitik.

[103] InfoSäkutredningen. SOU 2005:71 – Säker information - Förslag till informationssäkerhetspolitik.

[104] Fornyings og administrasjonsdepartementet. St.meld. nr. 17 (2001–2002): Eit informasjonssamfunn for alle.

[105] Nettavisen. Bank-kaos rammet Norge. http://www.nettavisen.no/okonomi/privat/article780880.ece. 24.10.06.

[106] Nærings og handelsdepartementet. Samfunnets sårbarhet som følge av avhengighet til IT. http://www.regjeringen.no/en/ministries/nhd/Documents/Reports-and-plans/Reports/2000/Samfunnets-sarbarhet-som-folge-av-avhengighet-til-IT.html?id=277328, oktober 2000.