FFI RAPPORT

STRATEGIER FOR INFORMASJONSSIKKERHET - En komparativ studie av strategiarbeidet i Norge, USA, Australia og EU

GULICHSEN Steinar, HOFF Erlend, SØRLI Kjetil, HAGEN Janne, NYSTUEN Kjell Olav

FFI/RAPPORT-2003/00271-1

FFISYS/416401/044

Godkjent
Kjeller 21. januar 2004

Jan Erik Torp
Forskningssjef

STRATEGIER FOR INFORMASJONSSIKKERHET
- En komparativ studie av strategiarbeidet i Norge, USA, Australia og EU

GULICHSEN Steinar, HOFF Erlend, SØRLI Kjetil,
HAGEN Janne, NYSTUEN Kjell Olav

FFI/RAPPORT-2003/00271-1

FORSVARETS FORSKNINGSINSTITUTT
Norwegian Defence Research Establishment
Postboks 25, 2027 Kjeller, Norge

FORSVARETS FORSKNINGSINSTITUTT (FFI)
Norwegian Defence Research Establishment

P O BOX 25
NO-2027 KJELLER, NORWAY

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

REPORT DOCUMENTATION PAGE

1) PUBL/REPORT NUMBER	2) SECURITY CLASSIFICATION	3) NUMBER OF PAGES
FFI/RAPPORT-2003/00271-1	UNCLASSIFIED	69
1a) PROJECT REFERENCE	**2a) DECLASSIFICATION/DOWNGRADING SCHEDULE**	
FFISYS/416401/044	-	

4) TITLE

STRATEGIER FOR INFORMASJONSSIKKERHET - En komparativ studie av strategiarbeidet i Norge, USA, Australia og EU

STRATEGIES FOR INFORMATION SECURITY - A comparative study of the strategy work in Norway, US, Australia and EU

5) NAMES OF AUTHOR(S) IN FULL (surname first)

GULICHSEN Steinar, HOFF Erlend, SØRLI Kjetil, HAGEN Janne, NYSTUEN Kjell Olav

6) DISTRIBUTION STATEMENT

Approved for public release. Distribution unlimited. (Offentlig tilgjengelig)

7) INDEXING TERMS

IN ENGLISH:	IN NORWEGIAN:
a) Information security	a) Informasjonssikkerhet
b) Vulnerability	b) Sårbarhet
c) Strategy	c) Strategi
d) Information technology	d) Informasjonsteknologi
e)	e)

THESAURUS REFERENCE:

8) ABSTRACT

This report documents a brief comparative study on work and strategies in different countries in the field of national cyberspace security. These countries are Norway, Australia and USA. In addition the EU is included. This work has been done in connection with the pre-project 416401, BAS5.

9) DATE	AUTHORIZED BY	POSITION
	This page only	
2004-03-11	Jan Erik Torp	Director of Research

ISBN 82-464-0818-6

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

INNHOLD

STRATEGIER FOR INFORMASJONSSIKKERHET - En komparativ studie av strategiarbeidet i Norge, USA, Australia og EU

1 INNLEDNING

Gjennom forskningsprogrammet "Beskyttelse av samfunnet" (BAS) har Forsvarets forskningsinstitutt (FFI) siden 1994 hatt i fokus samfunnets sårbarhet og hvordan samfunnet kan bli mer motstandsdyktig mot et bredt spekter av trusler, i potensielle krise- og krigssituasjoner. Denne rapporten oppsummerer arbeidet utført i oppdrag nr 416401 "Beskyttelse av samfunnet 5 (BAS5) Forprosjekt". Forprosjektet ble etablert som en forberedelse til det planlagte BAS5-prosjektet med fokus på IKT-sårbarhet[1].

Fra før er det gjort én tverrsektoriell studie av samfunnets sårbarhet og flere dybdestudier, deriblant av sårbarheten i telenettet, kraftforsyningen og transportsektoren. FFI har også i samarbeid med Scandpower gjort en studie av sårbarheten i vannforsyningen. Sårbarhet i nettede informasjonssystemer og samfunnets avhengighet av disse har vært analysert gjennom utvalgte casestudier.

Det har vært en viktig målsetning i forprosjektet til BAS5 å skaffe oversikt over det internasjonale arbeidet innenfor informasjonssikkerhet, dog med vekt på å kartlegge de initiativer ulike stater har tatt i forhold til utfordringen som ligger i avhengigheten av åpne, verdensomspennende og sårbare informasjonsnettverk. Det er i denne sammenheng valgt å fokusere på Norge, USA, Australia og EU. USA er valgt fordi USA er ledende i bruk av ny forsvarsteknologi og i å tenke på nasjonal sikkerhet. Australia er valgt fordi Australia på mange måter har likheter med Norge i form av stor geografisk utbredelse og spredt bebyggelse. Det har også vært naturlig å skjele til hva EU gjør på dette området som en overbygning for flere europeiske stater og som en handelspolitisk premissgiver for Norge.

Rapporten belyser i hvilken grad arbeidet med informasjonssikkerhet, på nasjonalt nivå, har materialisert seg i strategier med avklart ansvarsområde og konkrete tiltak, og hvilket fokus strategiene har mht. trusler og innretning av sikkerhetsarbeidet.

2 METODE

Studien bygger på litteratur innhentet gjennom søk i databaser og på Internett. Det finnes mange ulike kilder med relevans for de spørsmål som søkes besvart i studien. Som følge av tidsmessige begrensninger har det ikke vært mulig å gå i detalj på alle relevante områder. Studien er derfor en forstudie som kan trekke linjer for det videre arbeidet.

[1] Nasjonal strategi for informasjonssikkerhet omtaler dette prosjektet som en planlagt aktivitet ved FFI.

Det er valgt å skille mellom telesikkerhet og –beredskap, og informasjonssikkerhet, der det første er innrettet mot å sikre innbyggerne tilgang på sikre teletjenester. Informasjonssikkerhet bygger allerede på en forutsetning om tilgjengelighet på teletjenester, og berører andre aspekter som konfidensialitet, integritet og autentisering i elektronisk kommunikasjon.

En strategi for informasjonssikkerhet på nasjonalt plan bør si noe om mål og virkemiddelbruk, hvem som skal ha ansvar for arbeidet og kostnader, og eventuelt hvordan tiltakene skal finansieres. Disse variablene har også vært gjenstand for oppmerksomhet når informasjon om nasjonale strategier for informasjonssikkerhet er innhentet. I tillegg er det pågående strategiarbeidet kartlagt, samt hvilken formell status denne strategien har (utkast eller godkjent offentlig dokument).

3 NORGE

3.1 En historisk oversikt over arbeidet med informasjonssikkerhet i Norge

3.1.1 Verdiskapning i fokus og Norge som IT-nasjon

I Regjeringens langtidsprogram fra 1996 ble det lagt opp til en politikk som skulle gi økt verdiskapning, sikre en rettferdig fordeling og fremme den enkeltes mulighet til å bruke sine evner og kunnskaper gjennom aktiv deltakelse i samfunnet. Ifølge Statssekretærutvalget for IT var utnyttelse av informasjonsteknologi et ledd i å nå målsettingen om økt verdiskapning. Denne tanken ble fulgt opp gjennom St.meld. nr. 41 (1998-99). Med denne meldingen ønsket Regjeringen å gi impulser til næringsutvikling, og elektronisk handel ble her betraktet som et vekstområde der Norge skulle ligge i front.

Elektronisk handel krever en relativt robust informasjonsinfrastruktur med god kapasitet og evne til å formidle store datamengder raskt. Regjeringen la frem sin handlingsplan for bredbåndskommunikasjon 11. oktober 2000. Den ønsket en rask og bred geografisk utbygging av bredbåndsnett i regi av markedsaktørene. Det var viktig å få til en mer fleksibel lovgivning og forutsigbarhet for markedsaktørene. Konkurransen skulle styrkes, og det skulle legges til rette for økt offentlig etterspørsel etter bredbånd. Liberalisering av telemarkedet var ett viktig tiltak for å fremme konkurransen. For å fremme etterspørselen etter bredbånd i offentlig og privat sektor, ble tilskuddsordningen for høyhastighetskommunikasjon (HØYKOM) etablert. Denne tilskuddsordningen viste at offentlige tilskudd kunne utløse investeringer fra andre offentlige og private virksomheter, og dermed stimulere til å ta i bruk bredbånd.

I strategien for eksport og internasjonalisering av IKT-næringen 2002-2003, som ble lagt frem av Nærings- og handelsministeren i desember 2001, ble næringslivets satsing på IKT-sikkerhetsprodukter nevnt som et mulig vekstområde der Norge ville kunne hevde seg internasjonalt. Det var nå blitt økt oppmerksomhet i samfunnet på informasjonssikkerhet. Dette gjenspeilet seg også i Nærings- og handelsdepartementet. Under Nærings- og

handelsministerens IT-politiske redegjørelse i Stortinget 14. mai 2002, ble denne dreiningen tydeliggjort ved at tilgjengelighet og sikkerhet ble nevnt spesielt. Elektronisk signatur ble for eksempel nevnt som en forutsetning for sikker bruk av elektronisk kommunikasjon. Fortsatt var hovedparolen utvikling, effektivitet og verdiskapning, men nå ble det understreket at sikre og tilgjengelige informasjonssystemer og -tjenester var en forutsetning.[2]

3.1.2 Sårbarhet i fokus

Den store endringen i internasjonal sikkerhet på begynnelsen av 90-tallet da Sovjetunionen gikk i oppløsning, gjorde det nødvendig å omstille både det militære Forsvaret og den sivile beredskapen. I 1994 startet derfor FFI sin forskning på samfunnets sårbarhet og behov for omlegging av den sivile beredskapen. Den første sluttrapporten, som kom i 1997, markerte startpunktet for flere sektorstudier om sårbarhet, utført ved FFI, der kritisk informasjonsinfrastruktur også ble behandlet. I rekkefølge ble telekommunikasjon, kraftforsyning, transport og vannforsyning analysert. I tråd med den økte digitaliseringen av Forsvaret og samfunnet for øvrig, iverksatte FFI også etter hvert forskning på internettkrigføring og studier av hvordan man kan forsvare seg mot denne type trusler.

IT-sikkerhet ble satt på den politiske dagsorden da "Rådet for IT-sikkerhet" (RITS) ble opprettet våren 1996. Rådet var et forum for erfaringsutveksling, med en rådgivende funksjon overfor departementene. Rådet skulle ta opp saker av tverrsektoriell interesse. Det ble etablert under Arbeids- og administrasjonsdepartementet, og flyttet til Nærings- og Handelsdepartementet i januar 1998. Det ble etablert flere arbeidsgrupper i denne sammenheng, som blant annet tok for seg digitale signaturer, sertifisering av IT-sikkerhet i produkter, systemer og organisasjoner, og vurdering av behovet for en kryptopolitikk[3].

I 1998 tok Statssekretærutvalget for IT (SSIT) initiativ til et underutvalg som skulle lage en rapport om status for IT-sårbarheten i Norge.[4] Dette IT-sårbarhetsprosjektet ble igangsatt i 1999 i samarbeid med flere departementer under ledelse av NHD. Prosjektet ble ferdigstilt i oktober 2000.

År 2000 (Y2K)-problemene og resultatene fra BAS-programmet, var begge sterke drivere for at Sårbarhetsutvalget ble etablert, med tidligere statsminister Kåre Willoch som leder. I 2000, parallelt og med nær tilknytning til arbeidet med IT-sårbarhetsprosjektet, kom utvalget med sin innstilling om samfunnets sårbarhet. Nå var hele samfunnets sårbarhet satt på den politiske dagsorden.

3.2 Teleberedskap

Konklusjonene fra BAS2, som hadde sårbarhet i det offentlige telenettet som fokus, ble fulgt

[2] Allerede året før kom et utvalg som skulle utrede elektronisk signatur med sin rapport, NOU 2000:10. Utvalgets arbeidet pågikk fra februar 2000 til mars 2001, og forskrifter basert på dette kom i perioden 2001-2002.
[3] Arbeids- og administrasjonsdepartementet (2001): AAD:NOU 2001:10, Uten penn og blekk. Bruk av digitale signaturer i elektronisk samhandling og i forvaltningen
[4] eNorge - Samfunnets sårbarhet som følge av avhengighet til IT, oktober 2000

opp av ytterligere utredninger, deriblant TIFKOM-prosjektet. Dette arbeidet endte i St.meld. nr. 47 (2000-2001), om Teleberedskap, som ble godkjent 11. mai 2001.[5] Sammen gir stortingsmeldingen og innstillingen innblikk i Norges mål og strategi for telesikkerhet og beredskap. Tiltakene tar høyde for hele spekteret av trusler mot telenettet, fra trusler i fred til trusler i krig, og de anbefalinger som ble gitt i BAS2-prosjektet ved FFI er i stor grad inkludert. Eksempler på tiltak er prioriteringsordning, samlokalisering, redundans i nettene og nasjonal autonomi.

3.3 Strategi for informasjonssikkerhet

Arbeidet med en nasjonal strategi for informasjonssikkerhet startet våren 2002 etter initiativ fra Justisdepartementet (JD), Forsvarsdepartementet (FD) og Nærings- og handelsdepartementet (NHD). Høsten 2002 ble et grunnlagsdokument sendt ut på høring med høringsfrist 25 november. [6] Den 8. juli 2003 ble den norske nasjonale strategien for informasjonssikkerhet offentliggjort. Strategien har et perspektiv på 2-3 år, og har følgende formål (10):

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

Regjeringen ønsket å legge til rette for trygg elektronisk forretningsdrift og sikre og pålitelige nettjenester fra det offentlige ved å redusere sårbarheten ved alminnelig bruk av IT og i kritisk IT-infrastruktur. Den nasjonale strategien for informasjonssikkerhet bygger på OECDs retningslinjer.[7,8,9]

Den stadig sterkere avhengigheten av IKT i dagens samfunn har gjort at man i dag er utsatt for en rekke nye trusler som har gjort samfunnet sårbart på mange områder. Samtidig muliggjør den nye teknologien at man kan utveksle informasjon og gjøre forretninger mer effektivt enn tidligere. Dette gjør at man må fokusere enda sterkere på sikkerhet i IKT-systemer for å unngå at tapene blir for store ved forstyrrelser i den daglige driften. Den nasjonale strategien for informasjonssikkerhet fremhever fire overordnede mål for å bedre sikkerheten i nasjonalt kritiske IKT-systemer. Disse er (10):

- **Robusthet:** 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.

[5] Se Ins.S.nr.329 (2000-2001) – telesikkerhet og beredskap i et telemarked med fri konkurranse
[6] http://odin.dep.no/nhd/norsk/aktuelt/hoeringssaker/paa_hoering/024101-080002/index-dok000-b-n-a.html#inn
[7] Se appendiks A.
[8] http://www.enorge.org/modules/module_111/news_item_view.asp?iResponse=3 &iNewsId=1449&iCategoryId=153
[9] http://www.digi.no/dtno.nsf/pub/dd20020926151643_ero_80736552

- **Sikkerhetskultur:** 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.
- **Elektronisk signatur:** Norge skal ha en allment tilgjengelig samfunnsinfrastruktur for elektronisk signatur, autentisering av kommunikasjonspartere, samt sikker overføring av sensitiv informasjon.
- **Utvikle lovgivningen:** Regelverk som berører informasjonssikkerhet skal håndheves og videreutvikles på en samordnet, og for brukerne, enkel og oversiktlig måte.

Ett av de viktigste målene blir i følge strategien utvikling av en "sikkerhetskultur" i samfunnet. Strategien henvender seg til myndigheter, næringsliv og organisasjoner, men det påpekes at strategiens innhold er av interesse for alle brukere av informasjonssystemer, og at alle aktører har et felles ansvar for å øke bevisstheten om og forståelsen av IKT-sikkerhet.

For å oppfylle målsetningene foreslår strategien en rekke tiltak, 40 i alt, fordelt på forskjellige fokusområder. Noen av disse er: Samordne regelverk, koordinering, risko- og sårbarhetsanalyser, bevisstgjøring, varsling, sertifisering, PKI-strategi, kompetansebygging og samarbeid (10).

En gjennomgang av de viktigste fokusområdene er gitt i appendiks B, men følgende tre punkter trekkes frem:

Risiko- og sårbarhetsanalyser: Regjeringens ønsker et felles sett med kriterier for "hvor man bør legge lista", for deretter å gjennomføre ROS-analyser. Ansvaret for dette er spredt på blant annet JD, FD, DSB og NSM.

Samordnet lovgivning: Håndhevingen av regelverket innen IKT-sikkerhet er delt mellom en rekke offentlige etater og organisasjoner. Derfor ønsker Regjeringen, gjennom den nasjonale strategien, både å foreta en gjennomgang av eksisterende regelverk og å samordne tilsynsmyndigheten. Et permanent koordineringsutvalg er tenkt å kunne ivareta det felles overordnede hensynet.

VDI: Et annet viktig punkt i strategien er det foreslåtte varslingssystemet for digital infrastruktur (VDI). VDI har vært organisert som et prøveprosjekt, men er vedtatt etablert permanent fra 1. januar 2004. VDIs oppgave vil i hovedsak bestå i å fange opp trusler mot nasjonalt viktige IKT-systemer. I denne sammenheng kan også nevnes Senter for informasjonssikring (SIS), som har fått i oppgave å være rapporteringspunkt og rådgiver for næringslivet ved datainnbrudd, virusangrep og lignende.[10]

3.4 Avslutning

"Nasjonal strategi for informasjonssikkerhet", som ble offentliggjort sommeren 2003 gir

[10] Se appendiks B.

sammen med sikkerhetsloven, innstillingen til og St.meld. nr. 47 (2000-2001) innsikt i Norges håndtering av sårbarhet og sikkerhet i nettede informasjonssystemer og IKT.

St.meld. nr. 47 (2000-2001) med innstilling har fokus på bredden i trusselspekteret, dog med en viss nedprioritering av den nedre og øvre del av trusselspekteret, dvs de dagligdagse truslene og de tradisjonelle krigstruslene. Den nylig utgitte strategiens trusselfokus er mer vagt, og slik vi tolker den, innrettet mot i hovedsak dagligdagse hendelser og trusler. Mulige fremtidige trusler mot nasjonal sikkerhet synes ikke behandlet på en hensiktsmessig måte.

I sikkerhetsloven med tilhørende forskrifter som gjelder for militære informasjonssystemer har man et regime for håndtering og spredning av informasjon avhengig av informasjonens kritikalitet med hensyn til skadepotensiale for rikets sikkerhet dersom informasjonen kommer på avveie. I den totale sammenheng kan det hevdes at det er et fåtall systemer dette gjelder. I dagens nettverkssamfunn der små og store datanettverk blir koplet sammen, der det er stor dynamikk i utviklingen og skillet mellom militære og sivile systemer gradvis viskes ut, blir denne tenkemåten utfordret mht sin relevans og sin praktiske anvendbarhet.

Strategien for informasjonssikkerhet er slik vi forstår den, tenkt å dekke aktører opp til og med kritisk infrastruktur, dvs. samfunnet i stort. Skillet ved kritisk infrastruktur/systemer av betydning for rikets sikkerhet er imidlertid ikke klart – særlig ikke når man ser nærmere etter hvilke datasystemer som henger sammen og hvordan disse henger sammen.

Det fragmenterte ansvaret for informasjonssikkerhet kombinert med sektor- og nivåtekning gjør at det etter FFIs vurdering fremdeles er langt frem til at Norge har kommet i mål når det gjelder en helhetlig nasjonal politikk for informasjonssikkerhet der ansvar er avklart og alle aspekter er ivaretatt. Det må i den sammenheng nevnes at det er under utarbeidelse en ny forskrift om objektsikkerhet som er utformet for å møte en del av disse utfordringene. Forskriften er for tiden ute til høring.

Også positive trekk i tiden må fremheves. Blant annet har Norges forskningsråd 59 mill kroner til forskning på IKT-sikkerhet.

4 USA

4.1 Et nytt sikkerhetsfokus

USA var allerede på 90-tallet opptatt av hvordan sårbarheter i kritiske IKT-systemer kunne påvirke nasjonal sikkerhet. Siden da har det vært gjennomført utredningsarbeider på området kritisk infrastruktur (CIP) og kritiske informasjonsinfrastrukturer (CIIP).
Myndighetene har også utarbeidet en rekke nasjonale strategier for å styrke den nasjonale sikkerheten. Beskyttelse av nasjonal kritisk infrastruktur kom ennå høyere opp på den politiske agenda etter terroraksjonene 11 september (1).

De to strategiene ”The National Security Strategy of the United States of America” og ”The National Strategy for Homeland Security” er overordnede strategier som etablerer et rammeverk, og som gir føringer for de andre mer underordede strategiene (2). Siden forstudien omhandler arbeidet med informasjonssikkerhet i ulike land, er det derfor kun ”The National Strategy to Secure Cyberspace” som vil bli omtalt her.

4.2 En historisk oversikt over arbeidet med beskyttelse av kritisk infrastruktur i USA

Arbeidet med å analysere kritisk infrastruktur startet for alvor med at Presiden Bill Clinton i 1996 undertegnet ”Executive Order 13010”. Dette dokumentet godkjente opprettelsen av presidentens kommisjon for beskyttelse av kritisk infrastruktur (PCCIP) (3). Denne kommisjonen fikk i oppgave å studere omfanget av trusler mot, og sårbarheten i, kritisk infrastruktur. Kritisk infrastruktur blir i det samme dokumentet definert til å omfatte:

- Telekommunikasjon
- Kraftforsyning
- Bank og finans
- Transport
- Vannforsyning
- Nødetatene

Kommisjonen analyserte både fysiske og IKT-baserte trusler mot kritisk amerikansk infrastruktur. Sluttrapporten fra dens arbeid, som kom i 1997 (4), dannet grunnlaget for President Clintons ”Decision Directive 63” (PDD-63) i 1998.[11] I sin tur banet PDD-63 vei for utarbeidelsen av en nasjonal plan for beskyttelse av informasjonssystemer som ble utgitt i januar 2000 (1).

Mesteparten av den kritiske infrastrukturen i USA er eid av private aktører, noe som gjorde et samarbeid mellom føderale, statlige og private aktører nødvendig, også kalt PPP (Public-Private-Partnership). Tanken var samarbeid og minimal bruk av lovregulering, og PDD-63 foreslår opprettelse av følgende organisasjoner for å møte den utfordringen (5):

- **The Critical Infrastructure Assurance Office (CIAO)**: Et kontor med fokus på å koordinere de føderale myndighetenes initiativ knyttet til beskyttelse av kritisk infrastruktur, lokalisert under handelsdepartementet. CIAO fikk også i oppgave å bistå ulike byråer i oppgaven med å identifisere deres egen avhengighet av kritisk infrastruktur og å koordinere utarbeidelsen av et nasjonalt utdannings- og bevisstgjøringsprogram innen CIP.

- **The National Infrastructure Protection Center (NIPC)**: Et kontor lokalisert under

[11] Finnes på http://www.fedcirc.gov/library/legislation/presDecDirective63.html

FBI med fokus på trusselvurderinger, sårbarheter og etterforskning.

I tillegg til disse organisasjonene beordret PDD-63 opprettelsen av såkalte ISACs (Information Sharing and Analysis Centers), som er sektorvise informasjonsdelings- og analysesentre.[12]

Allerede før angrepene på World Trade Center 11. september 2001, ble en gjennomgang av PDD-63-rammeverket igangsatt, og resultatet av gjennomgangen som ble igangsatt i mars 2001 av presiden George W. Bush, kom i oktober det året. Det bestod av to bekjentgjørelser: (6) (7)

- Executive Order 13228, om opprettelsen av Office of Homeland Security (OHS)
- Executive Order 13231, om CIP i informasjonstidsalderen.

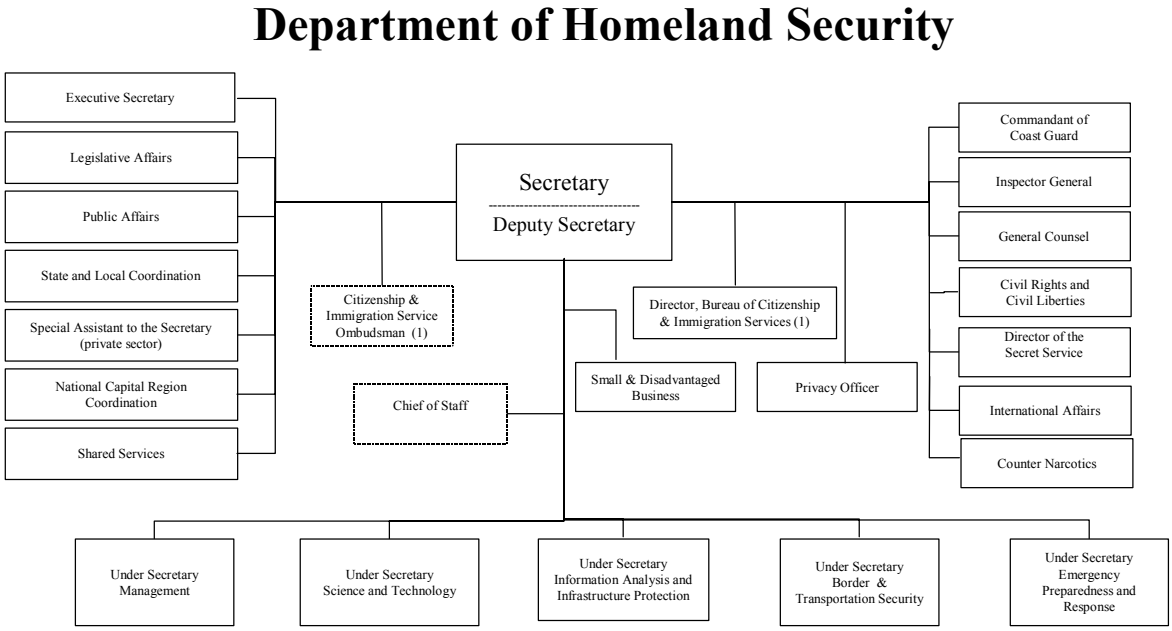
Førstnevnte, EO 13228, opprettet OHS som ble underlagt det Hvite Hus. Hovedoppgaven skulle være utarbeidelse, koordinering og implementering av en nasjonal strategi for å beskytte USA mot terrorangrep i fremtiden.[13]

Sistnevnte, EO13231, opprettet på sin side President's Critical Infrastructure Protection Board (CIPB). Dens hovedoppgave var å koordinere føderale strategier og tiltak for beskyttelse av kritisk infrastruktur, herunder CIIP. Ledere for CIPB ble presidentens nye spesialrådgiver for IKT-sikkerhetsspørsmål, og skulle rapportere til både den nasjonale sikkerhetsrådgiveren og til lederen for OHS (1). CIPBs medlemmer inkluderer en lang rekke høyere statsansatte, inkludert blant annet presidentens og visepresidentens stabssjef samt direktøren for CIA.[14]

Den nasjonale strategien for beskyttelse av USA var det første resultatet fra OHS, og ble fremlagt i juni 2002.[15] Den skulle gi et rammeverk for arbeidet med å beskytte USA mot terrorangrep blant føderale, statlige, lokale og private aktører. Strategien er bygget på de tre prinsippene: Forhindre faren for angrep; redusere USAs sårbarhet; skademinimering og reetablering.

Department of Homeland Security (DHS) ble etablert etter at President Bush godkjente Homeland Security Act of 2002", 25. november 2002. Opprettelsen av DHS er den største omorganiseringen av det amerikanske byråkratiet siden etableringen av forsvarsdepartementet i 1947, og omfatter er reorganisering av i alt 22 føderale organisasjoner. [16] Under gjengis et organisasjonskart for DHS.

[12] En oversikt over hvilke ISACer som er opprettet finnes på http://www.dhs.gov/dhspublic/display?theme=73
[13] Pressemelding Det Hvite Hus (http://www.whitehose.gov/news/releases/2001/10/print/20011008.html
[14] En full oversikt over alle medlemmene i CIPB finnes i punkt 6 i EO13231
[15] National Strategy for Homeland Security, Office of Homeland Security, juli 2002
[16] http://www.dhs.gov/dhspublic/theme_home1.jsp



Figur 4.1 Organisasjonskart for DHS[17]

Hovedansvaret for oppfølgingen av den nasjonal strategien for informasjonssikkerhet ligger i Direktoratet for informasjonsanalyse og beskyttelse av infrastruktur. Dette direktoratet er sammensatt av i alt 5 tidligere føderale byråer. Disse er [18]:

- Critical Infrastructure Assurance Office
- Federal Computer Incident Response Center
- National Communications System
- National Infrastructure Protection Center
- Energy Security and Assurance Program

4.3 Arbeidet med telesikkerhet og beredskap i USA

Arbeidet med telesikkerhet i USA strekker seg tilbake til 1962 og Cubakrisen. Kommunikasjonsproblemene mellom USA, NATO og Sovjetunionen den gang ledet til at president John F. Kennedy i etterkant satte ned en arbeidsgruppe som skulle utrede hvordan man i fremtiden kunne sikres bedre telekommunikasjon i en krisesituasjon.[19] Arbeidsgruppen anbefalte at det skulle opprettes et eget kommunikasjonssystem for blant annet presidenten og forsvarsdepartementet, og som følge av det opprettet Kennedy "National Communications System" (NCS) i 1963. NCS ble organisert under forsvarsdepartementet, og fikk i oppgave å koble sammen og forbedre ulike føderale telekommunikasjonsløsninger.

I 1984 ble NCS sine oppgaver innen telesikkerhet og beredskap utvidet. Som en følge av

[17] http://www.dhs.gov/dhspublic/interweb/assetlibrary/DHS_Org_Chart.ppt
[18] http://www.dhs.gov/dhspublic/display?theme=13
[19] http://www.ncs.gov/ncs/html/NCSHistoryBkgrd.html

utvidelsen ble ”National Coordination Center for Telecommunication” (NCC) opprettet. NCC fikk i hovedoppgave å understøtte de føderale myndighetenes behov for telekommunikasjon i krisesituasjoner (nasjonal sikkerhet og katastrofer). I januar 2000 ble oppgavene til NCC igjen utvidet ved at de fikk tildelt ansvaret for en ISAC for telekommunikasjonsbransjen, i tråd med PDD-63. NCC-ISAC skal tilrettelegge for PPP gjennom informasjonsutveksling vedrørende sårbarheter og trusler etc.

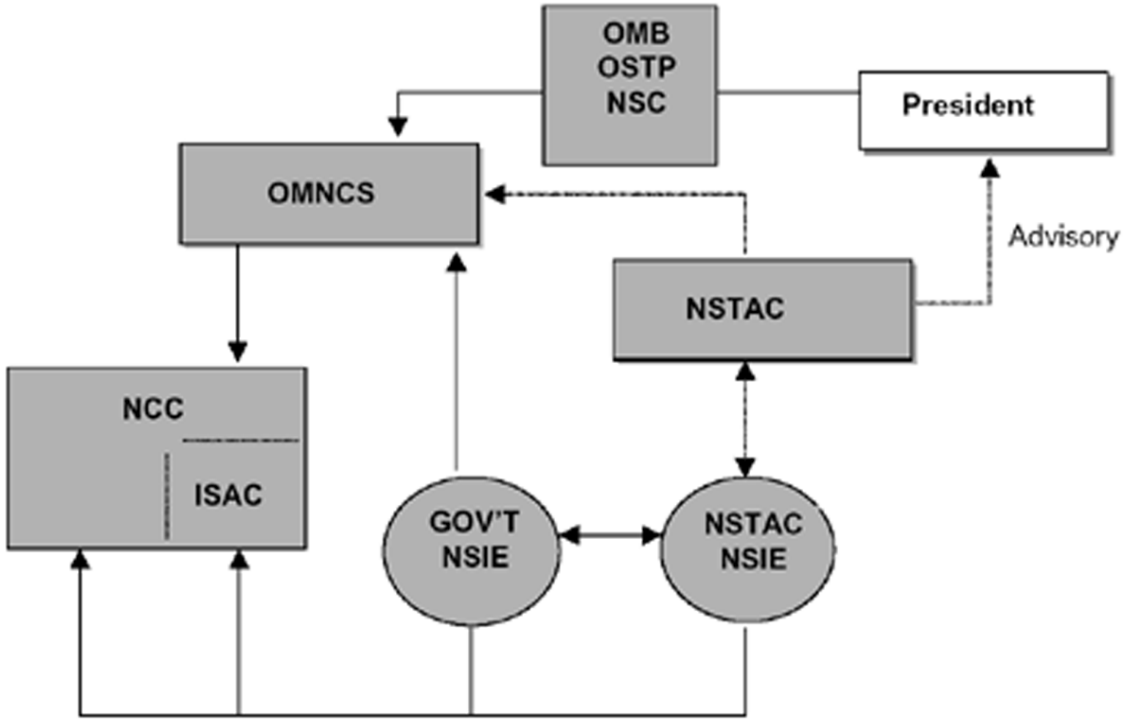
I tillegg til NCS og NCC fins også en rådgivende komité, ”National Security Telecommunications Advisory Committee” (NSTAC). Siden opprettelsen i 1982 har NSTAC gjort analyser og gitt råd til presidenten i spørsmål knyttet til telekommunikasjon, i lys av nasjonal sikkerhet og beredskap. Komiteen består av opp til 30 ledere fra ulike telekommunikasjonsselskaper, utnevnt av presidenten.[20]

Senere, i 1990, ble de to organisasjonene NSIE (Network Security Information Exchange) opprettet under henholdsvis NCS og NSTAC. Bakgrunnen var den nye trusselen fra ”hackere”, og arbeidet er informasjonsutveksling knyttet til sikkerhet innen teleberedskapen. Typiske målsetninger var å: (13)

- Øke kunnskap om innbrudd i og sårbarheter som påvirker telenettet
- Utarbeide anbefalinger som reduserer sårbarheten i nettverket
- Pålitelighets- og risikoanalyser i nettverkene
- Skaffe til veie trusselinformasjon og informasjon om hvordan disse truslene kan motarbeides
- Tilby eksperthjelp til NSTAC, slik at de kan gi velbegrunnede råd om sikkerhet i kommunikasjonsnettverk til presidenten

Figuren under gir en oversikt over hvordan arbeidet innen tele- og informasjonssikkerhet er organisert i USA (13):

[20] http://www.ncs.gov/nstac/NSTACXXIII/NSTACFactSheet.pdf



Figur 4.2 Organisatorisk forankring av NS/EP-arbeidet i USA[21]

Selv om NCC med sin ISAC og NSIE-organisasjon har samme formål, og gjennom dette kan virke noe overlappende, har de fortsatt forskjellig fokus når det gjelder tidsperspektivet, fagkompetanse og verdi. Tabellen under gir en oversikt over de viktigste forskjellene (13):

	NCC (NCC-ISAC)	**NSIE**
Fokus	Reaksjon og gjenoppretting. Alle typer trusler og farer	Beskyttelse og utholdenhet. Trusler mot og sårbarheter i nettverk og administrasjonssystemer som støtter opp om teleinfrastrukturen
Tidsramme	Nær sanntid/sanntid	Etter hendelse/Ad hoc sanntid
Fagkompetanse	Politikk og koordinering	Teknologer og sikkerhetseksperter
Produkter	Advarsler; meldinger og rapporter i etterkant av hendelser	Bedømmelse av risikoen knyttet til nettverkene og administrasjonssystemene som støtter opp om teleinfrastrukturen; workshops og policydokumenter
Verdi	Advarsler og råd om riktig reaksjon	Erfaringer og forhindring

Tabell 4.1 Forskjeller i fokus mellom NCC-ISAC og NSIE

Gjennom de ulike organisasjonenes virke innehar man en rekke ulike kapasiteter, i hele spennet fra organisatorisk til teknologisk nivå. Man benytter i stor grad offentlig kommersiell infrastruktur også for funksjoner med utvidede krav til robusthet i situasjoner innen nasjonal sikkerhet og sivil beredskap. Derfor finnes også ulike samarbeid mellom myndigheter og

[21] NCS, som er moderorganisasjonen til NCC, er i dag organisert under DHS.

kommersielle deltagere. Et eksempel på dette er ”Communications Resource Information Sharing” (CRIS) initiativet. Her søker man gjennom samarbeid å utnytte de ressurser som de enkelte aktørene har i et felleskap, for eksempel transportabelt kommunikasjonsutstyr.

Gjennom et nært samarbeid med de viktigste nettleverandørene blir tilleggsfunksjoner som øker sikkerhet og robusthet for utvalgte tjenester etablert. For eksempel tilbyr ”Government Emergency Telecommunications Service” (GETS) slike tjenester, med autentisert tilgang, utvidede rutinemekanismer og prioritetsfunksjoner for å gi utvalgte brukere prioritet i lokal og langdistanse telefoninettverk. Man har også funksjoner for prioritert gjenoppretting av spesielt viktige tjenester, så vel som prioritert brukeraksess i mobile telenett.

Det langsiktige arbeidet anses som viktig, noe som viser seg ved at myndighetene gir støtte til blant annet forskning på nasjonal sikkerhet. Det avholdes også regelmessig konferanser og seminarer på områdene informasjonssikkerhet og telekommunikasjon.

Gjennom lang tid har man bygget opp noe som synes å være et sterkt regime for telesikkerhet og beredskap. Fokus rettes i stor grad mot nasjonal sikkerhet og større trusler mot infrastrukturen og nasjonen. Dette regimet synes å være fundert på et relativt velutviklet samvirke med kommersielle aktører over lang tid..

4.4 USAs nasjonale strategi for informasjonssikkerhet

Den amerikanske nasjonale strategien for informasjonssikkerhet[22] ble utgitt i februar 2003 etter en omfattende prosess hvor mange ulike aktører var involvert under utarbeidelsen. En slik prosess hvor offentlige og private aktører samarbeider er også et av de førende prinsippene for strategien. Bakgrunnen for dette ligger i at en stor del av den kritiske infrastrukturen i USA er eid av private aktører.[23]

I tråd med ”the National Strategy for Homeland Security” har den nasjonale IKT-strategien følgende tre målsetninger (2) (8): Forhindre faren for angrep på IKT-systemer; redusere USAs sårbarhet som følge av angrep mot IKT-systemer; skademinimering og reetablering dersom slike angrep skulle forekomme.

Hovedfokus for den amerikanske nasjonale strategien for informasjonssikkerhet er rettet mot målrettede angrep fra aktører som er i stand til å forårsake stor skade på kritisk infrastruktur, som igjen vil kunne skade økonomien eller nasjonens sikkerhet. Trusler mot IKT-systemer kan komme fra mange ulike aktører med ulik grad av kompetanse. Verktøyene for å foreta angrep på ulike typer nettverk blir stadig mer utbredt, slik at antall aktører som er i stand til å foreta angrep også øker. Mange av disse aktørene er imidlertid ikke i stand til å forårsake skade på nasjonalt kritiske systemer.

[22] National Strategy to Secure Cyberspace.
[23] Se appendiks E for mer detaljert informasjon.

I de amerikanske strategien er fokus rettet mot høynivåtrusler fra nasjonale aktører eller terrororganisasjoner. Følgende sitat sier noe om hvilke mål som er relevante:

> *"In peacetime America's enemies may conduct espionage on our Government, university research centers, and private companies."*
>
> *"In wartime or crisis, adversaries may seek to intimidate the Nation's political leaders by attacking critical infrastructures and key economic functions or eroding public confidence in information systems."*

Det er tydelig av de to utdragene over at det amerikanske arbeidet er fokusert inn mot så vel fredstid som krigstid. Man er også tydelig opptatt av trusler som neppe kan stamme fra vanlige hackere.

I tråd med den oppfatningen av trusselbildet skissert over og de overordnede målene, består den amerikanske strategien av i alt 47 tiltak gruppert innenfor fem ulike fokusområder. Disse er (8):

- Et nasjonalt reaksjonssystem for IKT-sikkerhet
- Et nasjonalt program for å redusere IKT relaterte trusler og sårbarheter
- Et nasjonalt bevisstgjørings- og utdanningsprogram innen IKT sikkerhet
- Sikre statlige IKT-systemer
- Nasjonal sikkerhet og internasjonalt samarbeid om IKT-sikkerhet

En mer utdypende redegjørelse for den amerikanske strategien er gitt i appendiks C og E.

4.5 Avslutning

Arbeidet med IKT-sikkerhet i USA startet for alvor med president Clintons kommisjon for beskyttelse av kritisk infrastruktur i 1997. I 2001 ble så den første nasjonale planen for beskyttelse av informasjonssystemer gitt ut, som en følge av kommisjonens rapport og president Clintons PDD-63. Terrorangrepene den 11. september 2001 endret USA på mange måter. Fokus på beskyttelse av kritisk infrastruktur ble da betydelig større, og en rekke nasjonale strategier ble utarbeidet. Dette har bidratt til helhet i tenkningen rundt IKT-sikkerhet i USA, plassering av ansvar og lokalisering av ansvar på høyt nivå. Det er verdt å merke seg at det rettes vesentlig fokus mot høynivåtrusler. [24]

Avslutningsvis kan det være interessant å forsøke å oppsummere den amerikanske IKT-strategien og knytte noen kommentarer til strategiens utforming, og hvordan arbeidet med strategien og integrasjonen av DHS har blitt mottatt. Den amerikanske strategien har tre prioriterte hovedmålsetninger. Første prioritet er å forhindre angrep mot kritisk amerikansk IKT-infrastruktur. Videre har strategien som målsetning å redusere den nasjonale sårbarheten mot angrep på IKT-systemer. Det er urealistisk å anta at man kan forhindre alle typer angrep mot

[24] The National Strategy to Secure Cyberspace, Department of Homeland Security, februar 2003.

IKT-systemer, og strategien tar konsekvensene av denne realiteten ved at siste målsetning for strategien er å minimere skadene fra angrep og tiden det tar å få systemene opp å gå igjen, dersom angrep skulle forekomme. Dessuten argumenteres det også for å redusere trusler og motarbeide ondsinnede aktører.

Et moment som er positivt med den amerikansk strategien er fokuset på internasjonalt samarbeid for å bedre IKT-sikkerheten. Ved å inkorporere dette i den nasjonal strategien erkjenner man at informasjonsinfrastrukturer som f eks Internett ikke kjenner noen geografiske grenser og at samarbeid på tvers av landegrensene er nødvendig for å få en best mulig beskyttelse av kritiske IKT-systemer.

Dersom de amerikanske myndigheten lykkes i å realisere denne strategien vil det med stor sannsynlighet bidra til å redusere sårbarheten i kritisk amerikansk IKT-infrastruktur og konsekvensene av alvorlig svikt. Etableringen av DHS er et av de viktigste tiltakene som er gjennomført for å øke sannsynligheten for å lykkes med strategien. Ansvaret er løftet opp på høyt nasjonalt nivå og synliggjort gjennom DHS. Det er imidlertid ulike oppfatninger om hvorvidt dette er den rette veien å gå for å øke fokus på IKT-sikkerhet, og det har kommet en rekke kritiske kommentarer i media i forbindelse med DHS og etableringen av NCSD. Kritikken har vært rettet mot risikoen for å ikke få tilstrekkelig fagkompetanse inn og at omorganisering og sammenslåing av en så stor organisasjon som DHS er krevende. Det hevdes nok med rette at det også vil ta lang tid å bygge en felles virksomhetskultur.

Den amerikanske nasjonale strategien for informasjonssikkerhet er en omfattende strategi som berører en mengde viktige punkter. Det kan imidlertid virke som det kanskje kan bli vanskelig å gjennomføre strategien fullt ut, da en rekke av tiltakene som er rettet mot det private er av frivillig karakter.[25] For at man skal lykkes med dette blir det desto viktigere å få etablert et velfungerende samarbeid mellom det offentlige og det private næringsliv, slik at man kan dra nytte av hverandres erfaringer. Dette vil også være en viktig kanal for det offentlige for å få gjennomslag for de tiltakene som er foreslått i strategien.

5 AUSTRALIA

5.1 Australias online strategi

Australske myndigheter har hatt store ambisjoner om å være en ledende nasjon i den "nye økonomien" og i e-handel.[26] Derfor var også Australia tidlig ute med tiltak og lovgivning[27] som

[25] Noe av kritikken mot strategien går nettopp på dette punktet. Se http://www.ds-osac.org/view.cfm?KEY=7E44504A4154&type=2B170C1E0A3A0F162820 for mer informasjon

[26] The Current State of Play – Australia's Scorecard 2002, ISSN 1444 – 3945: http://www.noie.gov.au/projects/framework/progress/ie_stats/CSOP_April2002/CSOP_April2002.pdf

[27] Man begynte raskt å etablere nytt lovverk for å fremme den nye økonomien, og i 1999 kom ”The electronic transaction act” og ”On-line service act”. Førstnevnte var vedrørende kjøp og salg, men har i ettertid blitt kritisert for å ikke ta nok hensyn til forbrukeren.

kunne fremme kjøp og salg over Internett.

Allerede i 1997 ble ”the National Office for the Information Economy” (NOIE) dannet, med det formål at Australia skulle få en e-handel i verdensklasse. NOIE skulle være det koordinerende og rådgivende organ vedrørende internettjenester, og hovedkontor for alt som har med informasjonsøkonomien å gjøre, inkludert:[28]

- Hvordan det som vedrører informasjonsteknologi og kommunikasjon konvergerer
- Regulatorisk og fysisk infrastruktur som trengs for online tjenester, inkludert e-handel
- Myndighetenes og alle dets organers bruk av ny IKT
- Assistanse til myndigheter og industri som leverer tjenester online

”Government online” var en stor satsning som ble lansert i 2000 og et ledd i Regjeringens ønske om at Australia skulle bli et land helt i front av IKT-bølgen. Det innebar at alle myndighetsorganer skulle være tilgjenglige på Internett. Målsettingen var økt kvalitet og effektivitet, lavere kostnader, økt tilgjengelighet av informasjon (24 timer i døgnet), effektiv bruk av skattepengene samt å stimulere til økt e-handel.[29]

Behovet for integritet og datatrafikksikkerhet meldte seg raskt på grunn av personvernlovgivningen[30] og at det er viktig at alle brukere føler seg trygge på å bruke det offentliges systemer. Derfor er IT-sikkerhet et satsningsområde for NOIE, og det er laget egne retningslinjer for de byråer som benytter IKT. De er formulert slik at det er lett å manøvrere i informasjonsmengden, samtidig som det er gitt referanser til tyngre litteratur, som for eksempel PSM og ACSI 33 (se vedlegg 4 om PSM og ACSI 33).[31]

Behovet for å skape trygghet for brukerne har ført til at NOIE har bygget opp kompetanse omkring konfidensialitet, tillit og sikkerhet på nettet.[32] Når alle offentlige kontorer fra i år skal gå over fra "online government" til E-government[33], føyer myndighetenes behov seg inn i NOIEs portefølje. E-government innebærer mer utstrakt bruk av teknologi og interaktivitet mellom bruker og system, og er ment for å øke myndighetenes effektivitet og dermed også servicenivået ytterligere. Australia søker et selvregulerende system, uten myndighetenes innblanding utover den rådgivende. Myndighetene kan imidlertid intervenere ved behov.

5.2 Beskyttelse av kritisk infrastruktur – pionerarbeidet

I 1997/1998 ble den første utredningsrapporten om beskyttelse av kritisk infrastruktur utgitt.[34]

---

[28] http://www.austlii.edu.au/au/other/CyberLRes/2001/17/
[29] 6. april 2000: Media release: "Government Online – A Strategy for the Future": http://www.dcita.gov.au/Printer_Friendly/0,,0_1-2_1-4_14924-LIVE_1,00.html
[30] The privacy act 1988: http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/
[31] For detaljer se NOIEs internettside om Online Security: http://www.noie.gov.au/projects/confidence/Securing/security.htm
[32] http://www.noie.gov.au/projects/confidence/index.htm
[33] Mer om E-government finnes her: http://www.noie.gov.au/projects/egovernment/index.htm
[34] http://www.infowar.com.au/australia/niia.php

Det var et nøkkeldokument utgitt av Foreign Affairs, Defence and Trade Group, og rapporten identifiserte kritisk infrastruktur og sårbarheter i denne. Spesielt ble sårbarheten i forhold til høykapasitets terrortrusler vektlagt.[35]

Parallelt med den første rapporten, arbeidet også Defence Signals Directorate (DSD)[36] med en konfidensiell rapport, som så på kritisk informasjonsinfrastruktur.[37] I denne rapporten foreslo DSD å etablere en formell struktur som inkluderte både private aktører og myndighetene, og som skulle ha i oppgave å koordinere og implementere myndighetenes policy for beskyttelse av nasjonal informasjonsinfrastruktur (NII). Videre ble det foreslått at man måtte ha et nasjonalt Computer Emergency Response Team (CERT) for myndighetsorganer, og at man burde opprette et "Vulnerability Analysis Team" for å teste og vurdere IT-sikkerhetssystemene som myndighetene benytter.

En tverrdepartemental komité (Interdepartment Committee, IDC), ledet av Justisdepartementet, ble i august 1997 nedsatt av Secretaries' Committee on National Security (SCNS)[38] for å utrede hvordan man kan implementere anbefalingene gitt av DSD for beskyttelse av nasjonal informasjons infrastruktur.[39] De foreslo en struktur som gjengitt i Figur 5.1, der IDC fortsetter å eksistere som en selvstendig gruppe, SIDC.[40] SIDCs viktigste oppgave skulle være som koordinator i den nye strukturen. SIDC skulle også ha ansvaret for å utarbeide et akkrediteringssystem for institusjoner og kurs i opplæring innenfor NII, prioritere og fordele ressurser ut fra hva gruppen mener er av "nasjonal betydning" og drive kontaktskapende arbeid i utlandet.

Årlig ville etablering og drift av strukturen for beskyttelse av Australias NII koste 8,8 millioner NOK, fordelt på DSD, Protective Security Coordination Centre (PSCC), The Australian Security Information Organisation (AISO), Australian Federal Police (AFP) og Information and Security Law Division under Justisdepartementet (ISLD).[41] Sistnevnte er interessant å merke seg ettersom man henter inn juridisk ekspertise på et svært tidlig stadium i prosessen.

Ett av de andre tiltakene som ble foreslått, er at AusCERT[42] får en sentral rolle som konsulent i

---

[35] Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks, Research paper 18, 1997-98: http://www.aph.gov.au/library/pubs/rp/1997-98/98rp18.htm

[36] DSD er Australias motstykke til FLO/IKT

[37] Defense Signals Directorate, 1997: Australia's National Information Infrastructure: Threats and Vulnerabilities. Et ugradert sammendrag av rapporten finnes på følgende link: http://www.asio.gov.au/Work/Content/niireport/niirpt.htm#attachA

[38] Secretaries Committee on National Security (SCNS), er underlagt National Security Committee of the Cabinet, som igjen er del av Kabinettet i Australia.

[39] PROTECTING AUSTRALIA'S NATIONAL INFORMATION INFRASTRUCTURE – Report of the interdepartmental committee on protection of the national information infrastructure: http://www.asio.gov.au/Work/Content/niireport/niirpt.htm

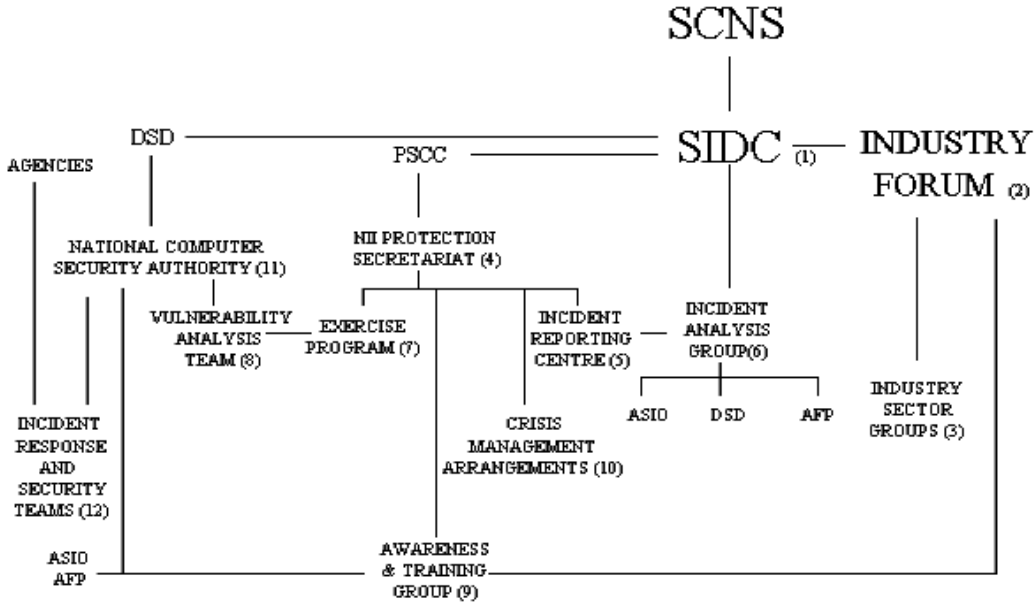
[40] SIDC : Standing Interdepartmental Committee for Protection of the National Information Infrastructure

[41] 1,7 millioner $ til lønn og ytterligere $ 125 000 i driftskostnader pr. år i perioden 1999 frem til og med 2001. Per 1. september 2003 er kursen på 1 AUD 4,83 NOK.

[42] AusCERT (national Computer Emergency Response Team for Australia) er en non-profit organisasjon som er lokalisert ved the University of Queensland, og kan på visse områder sammenliknes med den Norske CERT-funksjonen under Uninett. Det er meningen at AUSCert og NCSA (national computer security authority; (Under

arbeidet med å bygge opp rapportering av hendelser og responskapasitet. Videre ble det foreslått at direktøren for PSCC og direktøren for Emergency Management Australia (EMA)[43] skulle samarbeide om å koordinere alle aktiviteter innen beskyttelse av nasjonal infrastruktur, inkludert informasjonsinfrastruktur. Bakgrunnen for dette er at man ønsket å unngå overlapping mellom ulike aktiviteter. Det ble også foreslått at det ble opprettet en krisehåndteringsstab for angrep på informasjonssystemer, og at man i den sammenheng skulle dra nytte av det arbeidet som ble gjort i forkant av Sydney OL i 2000.

På bakgrunn av anbefalingene fra det interdepartementale utvalget, valgte Regjeringen i 1999 en fempunkts strategi.[44] Innholdsmessig svarer denne strategien til anbefalingene fra IDC, og de fem punktene er oppsummert i appendiks D.1.



Figur 5.1 Foreslått struktur for organisseringen av beskyttelse av Australias kritiske informasjonsinfrastruktur.

5.3 Australias beskyttelse av kritisk infrastruktur – med vekt på CIIP

Australske myndigheter har generelt vært meget opptatt av IKT-sikkerhet, men fokus har vært rettet mot sikkerhet og trygghet for enkeltpersoner, og få ressurser har vært satt av til å håndtere trusselen fra høykapasitetsaktører. Selv om man så smått begynte å se på slike ting fra 1997 og utover, kan arbeidet frem til 2001, som den norske BAS-forskningen, sees på som et forprosjekt hva angår å identifisere kritisk infrastruktur og tiltak. Imidlertid har arbeidet tatt mer form de siste to årene, og man har begynt å se på de viktigste utfordringene identifisert i den første DSD-rapporten: Det som vedrører Rikets sikkerhet; det som får andre konsekvenser, f eks

---

DSD)) skal utfylle hverandre, og at utvidelse av NCSA ikke skal gå ut over AUSCert, se: http://www.asio.gov.au/Work/Content/niireport/niirpt.htm . Mer om AusCERT finnes på følgende link: http://www.auscert.org.au/render.html?it?=2252

[43] Hjemmesiden til Emergency management australia: http://www.ema.gov.au/

[44] Daryl Williams: Speech to the National Information Infrastructure Consultative Industry Forum, 27. august 1999: http://www.law.gov.au/www/attorneygeneralHome.nsf/Web+Pages/87CD1525545A4E27CA256B590015D5D0?OpenDocument

økonomiske; og CERT-funksjonen.

E-Security Co-ordination group – det øverste koordinerende organ
Det øverste koordinerende organ innen beskyttelse av NII[45] er E-Security Co-ordination Group (ESCG), som ble opprettet i februar 2001.[46] Gruppen består av representanter fra nøkkelposisjoner i the Commonwealth's byråer, nær sagt alle departementene, AFP, DSD, AISO samt fra Action Group on Law enforcement (AGLEC). Gruppen ledes av NOIE, og får også administrativ støtte fra E-Security Policy Section under NOIE.

ESCG vil sørge for at trusler slik som virus, hacking, DoS (denial of service) og informasjonskrigføring blir behandlet strategisk. Metoden synes å være å rapportere hendelser, sette fokus på sikkerhetsstandarder, øke sikkerhetstankegangen og fokusere på områder med for lav kompetanse. Det synes altså som om ESCG skal ha den rollen som ble tiltenkt SIDC (se forrige underkapittel, Figur 5.1).

Beskyttelse av CIP med hensyn på Rikets sikkerhet
Det ble dannet en underkomité av ESCG, som ble ledet av Justisdepartementet, Critical Infrastructure Priorities Group (CIPG). Gruppen skulle fokusere på de kritiske elementene av NII, ved for eksempel å gjøre risiko og sårbarhetsvurderinger av nøkkelinfrastruktur med hensyn til IT.[47] [48] Budsjettet for disse to gruppene var i 2000/2001 på ca 10 millioner NOK.[49]

Til nå har den viktigste oppgaven til CIPG vært å lede trussel- og sårbarhetsvurderingene som har blitt utført i nært samarbeid med de respektive sektormyndighetene.[50] Vurderingene har vært gjennomført med hensyn på IKT innen fire sektorer: Telekommunikasjon, kraftforsyning, bank og finans og lufttrafikkontroll.

Beskyttelse av CIP med vekt på samfunnsøkonomiske interesser
Business-Government Task Force on Critical Infrastructure ble opprettet i november 2001 under ledelse av Justisdepartementet. Mens CIPG skal jobbe mot temaer som er av betydning for rikests sikkerhet, skal Business-Government Task Force on Critical Infrastructure jobbe med flere og bredere aspekter, slik som hendelser av økonomisk betydning.[51] Gruppen består av bedriftsledere og sikkerhetseksperter i bedrifter innen kritisk informasjonsinfrastruktur, slik som transport, bank og finans samt telekommunikasjon. Gruppen skal for eksempel jobbe med å implementere OECDs retningslinjer[52] og å sette fokus på å etablere en "sikkerhetskultur".[53]

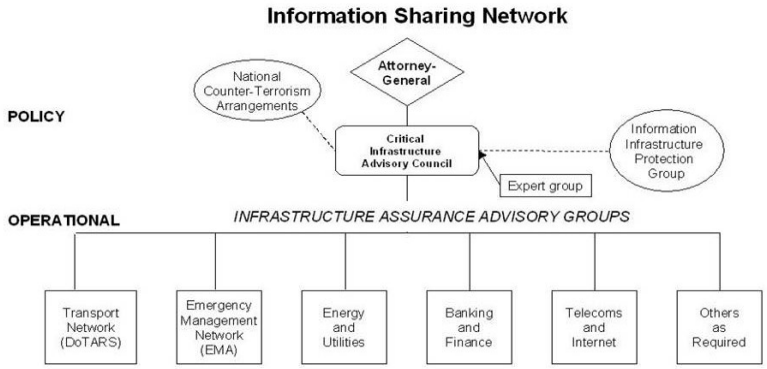
---

[45] NII innebefatter i denne sammenheng informasjonsinfrastruktur innenfor: telekommunikasjon, bank og finans, transport og distribusjon, energi og hjelpesystemer, informasjonstjenester, forsvaret og nødetatene.
[46] http://www.dcita.gov.au/Printer_Friendly/0,,0_1-2_1-4_15531-LIVE_1,00.html
[47] http://www.ddsi.org/Documents/final%20docs/DDSI_Country_Reports_Final_Australia.pdf
[48] http://www.dcita.gov.au/Printer_Friendly/0,,0_1-2_1-4_15531-LIVE_1,00.html
[49] 2 millioner AUD, kurs 4,83 per 1. september 2003
[50] Ref: www.noie.gov.au/projects/confidence/Protectiong/nat_agenda.htm
[51] http://www.law.gov.au/www/agdHome.nsf/Alldocs/4F350604C5F930AFCA256BDB000B2B53?OpenDocument
[52] OECD Guidelines for the Security of Information Systems and Networks: http://www.oecd.org/pdf/M00034000/M00034292.pdf

I et møte ble det besluttet opprettet et forum der man kunne diskutere sikkerhetsrelaterte saker uten frykt for at informasjonen kunne misbrukes. Trusted Information Network Shearing (TISN) ble dannet i 2002, og streber etter å være mest mulig lik, og knytte nære bånd til, det amerikanske motstykket ISAC. TISN er industriforumet som ble foreslått av den interdepartementale gruppen (se Figur 5.2).

Som i USA, delte man inn undergrupper etter hvilken kritisk infrastruktur man tilhørte, såkalte Crititcal Infrastructure Advisory Councils (CIAC). CIAC består av representanter for den aktuelle infrastruktursektor fra Staten, territoriene og de relevante commonwealth-byråene. Gruppene ledes av Justisdepartementet.

CIAC kommer til å fokusere på ikke-umiddelbare trusler, de som spenner fra middels til lang sikt. Spesielt kommer CIAC til å være opptatt av saker som krever koordinering med privat sektor og som er av preventiv natur, og ikke responsaktivitet. Se for øvrig Figur 5.2 for oversikt over organisering.[54]



Figur 5.2 Organisering av TISN, med underforum for hver kritisk infrastruktur.

Computer Emergency Responce Team (CERT)
Australia har lenge hatt en privat CERT-funksjon, AusCERT, men den har bare vært tilgjengelig for betalende medlemmer. I tillegg har den i hovedsak vært basert på spørreundersøkelser, og derfor ikke i stand til å respondere raskt. For statlige og offentlige virksomheter er det DSDs ISIDRAS-system som har vært tilbudet, men dette synes heller ikke å ha vært i omfattende bruk.

Bruken av hendelsesrapporteringssystemene har imidlertid økt kraftig, delvis på grunn av myndighetenes strategiske føringer, og som resultat av at angrepene mot IKT-systemer har økt kraftig. Allerede i 2000 oppfordret NOIE til økt bruk av ISIDRAS.[55]

Fra og med 2003 har også AusCERT blitt gratis (altså betalt av de føderale myndighetene).

---

[53] http://www.cript.gov.au/www/attorneygeneralHome.nsf/eb+Pages/07E41A49ACC7CFA6CA256C0F00177092?OpenDocument
[54] http://www.cript.gov.au/www/attorneygeneralHome.nsf/Web+Pages/E078BAC9BA04FEBCCA256C800012C461?OpenDocument
[55] http://www.noie.gov.au/projects/confidence/Securing/security.htm

AusCERT har også nylig begynt med online rapportering, noe som korter ned reaksjonstiden.[56] Dette skal øke Australias responsevne ved koordinerte IKT-angrep.

5.4 Telemarkedet fra et beredskapssynspunkt – fra monopol til konkurranse

Telemarkedet ble åpnet for konkurranse i 1997, og siden dette har prisene på teletjenester i snitt falt med 6,9 prosent årlig, samtidig med at det er gjort nyinvesteringer for 19,7 milliarder AUD (75,5 milliarder NOK), frem til 2002. Parallelt har en rekke nye aktører dukket opp og gitt konkurranse til Telstra[57]. I denne perioden har man også satset sterkt på mobiltelefoni, og den nasjonale mobilstrategien er at 18 prosent av landområdene skal være dekket, noe som tilsvarer 98 prosent av befolkningen. I den videre nasjonale strategien vil utbygging av bredbånd og internettilkobling være prioritert, i tillegg til fortsatt satsning på mobiltelefoni. Myndighetenes fokus har vært rettet mot områder med lav befolkningstetthet, og mer enn en milliard australske dollar[58] har blitt øremerket til IKT-infrastruktur og tjenesteproduksjon i utkantstrøk etter telemonopolets fall (se appendiks D.2 for mer informasjon om utbygging i grisgrendte strøk).

De australske telemyndighetene, Australian Communication Authority ACA[59] har omfattende myndighet, og kan blant annet ilegge bøter.[60] Det er de som i utgangspunktet plikter å påse at aktørene innen telesktoren følger lovverket. I følge the Telecommunications Act 1997[61], er teleselskapene pliktig å sikre seg mot hendelser ut over det som kan forventes under vanlige driftsforhold, slik som krig, terror og naturkatastrofer.[62] Imidlertid er dette noe verken telemyndighetene (ACA) eller infrastruktureierne har vært opptatt av. Derimot er myndighetene opptatt av at reparasjon og installasjon tar for lang tid, særlig i grisgrendte strøk (se appendiks D.2). Man har også sørget for at noen brukere får prioriterte linjer, eksempelvis syke personer. For å bøte på manglende vedlikehold og nødvendige investeringer, har man introdusert kundegarantiordninger, men til nå ser dette ikke ut til å ha hjulpet mye.[63]

Avslutningsvis bør det nevnes at hovedpoenget med reguleringen av telesektoren synes å være å sikre seg mot unødig og kostbar dublering og sørge for konkurransefremmende prising av tjenester.[64] Det fokus som har vært rettet mot nasjonal sikkerhet, har ikke vært mot infrastrukturen, men i retning av aktører som bruker den, for eksempel hvordan teleselskaper skal opptre i forhold til sikkerhetspolitiet og politiet i avlyttingssaker.[65] [66] Se appendiks D for

---

[56] http://www.nationalsecurity.gov.au/www/attorneygeneralHome.nsf/ Web+Pages/64534A395BA69AF4CA256D24007BDCA2?OpenDocument

[57] Telstra er den tidligere statsmonopolisten innen telefoni

[58] Tilsvarer rundt 4,8 milliarder NOK per 1. september 2003

[59] Australian Communications Authority: http://www.aca.gov.au

[60] Vanligvis er det for øvrig ombudsmannen som tar seg av klager

[61] http://scaleplus.law.gov.au/html/pasteact/2/3021/top.htm

[62] http://www.dcita.gov.au/Article/0,,0_1-2_1-4_105520,00.html

[63] Kundegarantiordningene er : Customer Service Guarantee (CSG) og Universal Service Obligation (USO). Disse ordningene var ment for å gi teleoperatørene incentiver for å bedre forhold som dekning, reparasjonstid og kundeservice. Imidlertid har ordningene blitt revidert en rekke ganger på grunn av ulike mangler.

[64] http://www.ddsi.org/Documents/final%20docs/DDSI_Country_Reports_Final_Australia.pdf

[65] Se for eksempel: Faktaskriv til industrien om hvordan internettaktører plikter å forholde seg til politiet og sikkerhetspolitiet: http://www.aca.gov.au/consumer_info/fact_sheets/industry_fact_sheets/fsi13.pdf

detaljer.

5.5 Fremtidig strategi og FoU

Fremtidig strategi
I 2002 satte myndighetene inn en offensiv for å styrke NII, og det ble satt av 24,9 millioner AUD (120 millioner NOK) som fordeles over 4 år.[67] Disse pengene blir fordelt på de ulike organisasjonene som DSD, AISO, NOIE, AFP, og PSCC for å styrke deres arbeid, i tillegg til å finansiere diverse fora som ESCG og TISN.

Hovedpunktene i den nye strategien er foreløpig å videreføre arbeidet som drives, som å utvikle kontakter med industrien, øke sikkerhetstankegangen hos infrastruktureierne og operatørene, øke kompetansen blant aktørene og FoU-aktivitet.

Mer spesifikt skal the Commonwealth implementere følgende innen regnskapsåret 2002/2003:

- Planlegging av en nasjonal kampanje for å øke bevissthetsnivået blant NII eiere og operatører.[68]
- Jobbe for å lage et hendelsesrapporteringssystem for både privat og offentlig sektor.[69]
- Undersøke hvordan ferdighetene innen datasikkerhet er, med hensyn til å sette i gang tiltak for å øke kompetansen til et akseptabelt nivå
- Sørge for at det juridiske rammeverket er slik at det kan ta seg av nye elektroniske trusler.
- Aktivt delta i fora slik at man kan fremme internasjonal infrastrukturbeskyttelse
- Øke samarbeidet mellom de ulike operasjonelle myndighetsorganene.

FoU
Australske myndigheter satser tungt på forskning og utvikling (FoU), og i 2002 brukte the Commonwealth $ 5,1 milliarder på vitenskap og innovasjon. I 2002 kunngjorde statsministeren i Australia at man skulle ha fire nasjonale satsningsområder:[70]

- Et bærekraftig miljø i Australia
- Fremme god helse
- Være i front teknologisk, innen for eksempel IKT, biokjemi og nanoteknologi
- ”Safeguarding Australia”

---

[66] Se for eksempel: Industrikodeks for assistanse til politiet og myndighetene i tilfeller angående rikets sikkerhet http://www.aca.gov.au/telcomm/industry_codes/codes/c537b.pdf
[67] http://www.law.gov.au/www/agdHome.nsf/Alldocs/4F350604C5F930AFCA256BDB000B2B53?OpenDocument
[68] NOIE er sentral i denne aktiviteten, og en av de viktigste oppgavene er en informasjonskampanje rettet mot små og mellomstore bedrifter, og som utføres i samarbeid med Internet Industry Association. Starten på dette var at man i juni 2002 iverksatte en informasjonskampanje, "Trusting the Internet", som er en serie av faktaark.
[69] Man har kommet langt i dette arbeidet, jf underkapittel 5.2.
[70] Referanse for hele avsnittet: Press release: http://www.pm.gov.au/news/speeches/2002/meddia_release2018.htm
[71] Liikanens hjemmeside er: http://europa.eu.int/comm/commissioners/liikanen/index_en.htm (European Commissioner for Enterprise and Information Society)

Det innebærer at man velger å satse tungt på forskning innen beskyttelse av kritisk infrastruktur. Første skritt i implementeringen vil være at forskningssentre og myndighetenes forskningsbevilgningsinstitusjoner setter opp planer der det inngår hvordan man planlegger å benytte midlene. Planene skal sendes til myndighetene innen mai 2003.

5.6 Organisatorisk forankring

Justisdepartementet (Attorney General's Department) har det overordnede ansvaret for beskyttelse av Australias kritiske infrastruktur. Videre har departementet delansvar gjennom å være overordnet de tre organisasjonene: Protective Security Coordination Centre (PSCC), Australian federal police (AFP) og The Australian Security Information Organisation (ASIO). IKT-kompetansen er det derimot DSD som besitter, og de er derfor ansvarlig for The Commonwealths online sikkerhetsretningslinjer og tekniske politikk.

AFP er det føderale politiet, og har i hovedsak rene politioppgaver. AISO befatter seg vanligvis ikke med hverdagskriminalitet, men med aktører som kan være en trussel mot riktes sikkerhet, inkludert organisert kriminalitet. Deres rolle innen IKT-sårbarhet er at de har stor kompetanse på fysisk sikring og gjør trusselvurderinger. PSCC har hovedansvaret for å vedlikeholde Protective Security Manual (PSM), som inneholder prosedyrer, prinsipper og standarder i henhold til myndighetenes sikkerhetspolicy.

Foruten det tidligere nevnte hendelsesrapporteringssystemet ISIDRAS, er DSD ansvarlig for sertifisering av utstyr og IKT-løsninger. DSD lager også tekniske retningslinjer innenfor datasikkerhet.

Joint Operating Arrangements (JOA) er et samarbeid innen IKT-sikkerhet mellom AISO, AFP og DSD. I den anledning har AISO bygget opp en liten kapasitet innen etterretning på Internett.

For mer fyldig informasjon vises til appendiks D.4.

5.7 Avslutning

Australia har ikke hatt et sterkt fokus på kritisk infrastruktur før 1997. Fra da har myndighetene arbeidet videre med utgangspunkt i noen tidlige rapporter som identifiserte sårbare funksjoner i samfunnet.

I forbindelse med satsningen på å bli en ledende IKT-nasjon, har imidlertid sikkerhet blitt meget viktig. For det første må befolkningen være trygge på at bruk av Internett ikke er til hinder for den ønskede økonomiske vekst. For det andre må man ivareta hensynet til personvern. Myndighetene, representert ved NOIE, har bygget opp betydelig kompetanse med hjelp av DSD: Man har en PKI-strategi, ulike veiledere og "best practice"-guider, i tillegg til sertifiseringsordninger. For eksempel kan alle myndighetsorganer sertifisere sin internettilkobling i henhold til ulike sikkerhetsnivåer. Slike tiltak vil gi synergier for alle deler av IKT-sikkerheten.

I år 2000 ble det fart i det systematiske arbeidet med beskyttelse av kritisk infrastruktur generelt og NII spesielt, med opprettelsen av ESCG og underliggende CIPG. Førstnevnte har overordnet ansvar for CIIP, mens sistnevnte skal ha fokus på det som har med rikests sikkerhet å gjøre. For å ivareta en industriens behov og for å møte de truslene som bare var av stor økonomisk betydning og ikke kunne true riket, opprettet man en Business-Government Task Force on Critical Infrastructure i 2001, som tar for seg all kritisk infrastruktur. Denne opprettet Trusted Information Network Shearing (TISN) det påfølgende året, og er en parallell til det ISACene er i USA.

Frem til 2002 har man brukt kun beskjedne ressurser på arbeidet med å sikre kritisk infrastruktur, for eksempel ESCG som hadde et årlig budsjett på 10 millioner NOK. Fra og med 2002 har man imidlertid øket satsningen betydelig, og kommer årlig til å bruke ca 30 millioner NOK i fire år til beskyttelse av NII. I tillegg er også ”Safeguarding Australia” satt opp som ett av fire punkter i den nasjonale FoU-strategien, der det årlig deles ut rundt 25 milliarder NOK.

I følge the Telecommunication Act er alle som driver teleselskaper pliktig å ha en beredskap mot uforutsette hendelser slik som for eksempel terror. Imidlertid er det ikke kjent om man har spesielle funksjoner innrettet mot sikkerhet og beredskap. Reguleringen synes i hovedsak å være rettet mot effektiv utbygging i grisgrendte strøk og å sikre et velfungerende kommersielt telemarked. Det ligger imidlertid som beskrevet ovenfor ressursinnsats i å beskytte NII, hvor telekommunikasjon er en vesentlig del. Det er mulig at en innsats innen telesikkerhet og –beredskap er kanalisert gjennom arbeidet knyttet til NII. Det er også uklart hvilken rolle det militære og deres ressurser har for nasjonal offentlig telesikkerhet og -beredskap.

Virksomheten synes å være rettet mot hensynet til nasjonal sikkerhet i forhold til større trusler, så vel som til den daglige kommersielle virksomheten til et næringsliv som blir stadig mer avhengig av informasjonsinfrastruktur. Fordelingen i innsats mellom disse to ytterpunktene i målsetting er imidlertid uklar med basis i det informasjonsgrunnlag FFI har hatt til gang til.

Innen forskning synes man å befinne seg i en tidlig fase, men det synes nå å legges vesentlige ressurser til grunn for fremtidig virke. Innretningen i forhold til trusselbilde er imidlertid uklar.

6 DEN EUROPEISKE UNION (EU)

EUs arbeid med IKT-sikkerhet er ikke knyttet opp mot nasjonal sikkerhet. Nasjonal sikkerhet er i utgangspunktet tillagt nasjonale myndigheter. Det er likevel av interesse å få oversikt over det generelle arbeidet om IKT-sikkerhet i EU; i mange tilfeller er det gråsoner mellom forretningskritiske, samfunnskritiske og nasjonalt kritiske systemer, og det kan tenkes at mye av dette er nyttig i BAS 5 sammenheng.

6.1 Organisatorisk forankring

IKT-spørsmål er lagt til kommisær for anskaffelse og informasjonssamfunnet Erkki Liikanen.[71] Under seg har han to Generaldirektorater (*Directorate-General* (DGer)), nemlig *Enterprise Directorate-General* og *Information Society Directorate-General*.[72] Det er den sistnevnte som er relevant i denne sammenheng. Hensikten med denne DGen er å tilrettelegge for de overordnede mål om vekst og fremgang med hjelp av informasjonsteknologi.

IKT-spørsmål ligger til kommisjonens politikkområde/aktivitet "Informasjonssamfunnet" (*Information Society*).[73] IKT spørsmål blir i EU-parlamentet behandlet i flere komiteer. Den mest sentrale er: *Committee on Industry, External Trade, Research and Energy*. Andre komiteer kan bli bedt om å gi uttalelser.[74]

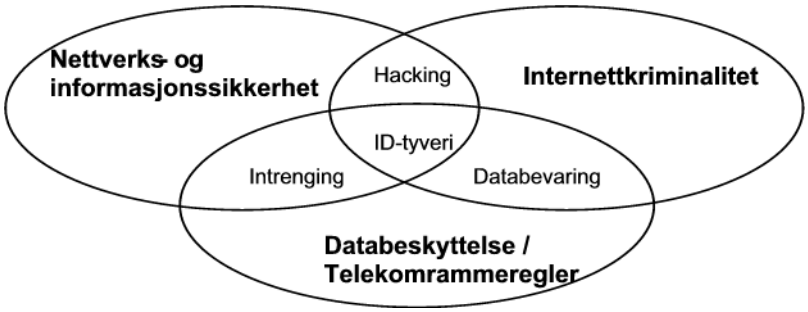
6.2 eEurope 2002 – EUs handlingsplan for bruk av IKT frem til 2002

Et rammeverk som ligger til grunn for målsettingene, er de såkalte *eEurope* handlingsplanene. Det har frem til nå kommet tre slike fra kommisjonen. Den første hadde navnet *eEurope* og ble erstattet av *eEurope 2002.* Sistnevnte varte frem til 2002, og ble så avløst av den nye og gjeldende handlingsplanen; *eEurope 2005*. Den første handlingsplanen vil på grunn av alderen ikke bli nærmere omtalt her.

eEurope 2002 hadde som mål å øke antall brukere av digitale tjenester over Internett, og å bidra til at Internett ble et fortrinn for privatpersoner, forretningsvirksomhet og offentlig virksomhet i EU-området. eEurope 2002 er avløst av EUs nye handlingsplan eEurope 2005, men det er likevel av interesse å peke på en rapport fra Kommisjonen innenfor rammen av eEurope 2002 med navn: "Nettverk og informasjonssikkerhet: Forslag til en europeisk strategi."[75] Rapporten som ble utgitt i juni 2001, var Kommisjonens svar på Det Europeiske Råds uttalelse i mars 2001 om viktigheten av sikkerhet i IKT-systemer. Av særlig interesse er at rapporten var EUs første forsøk på å dekke et hull i IKT-sikkerhetsrelaterte forhold. Den var et forsøk på å få plassert det såkalte nettverks- og informasjonssikkerhetskonseptet sammen med allerede eksisterende strategier for telekom-rammeregler, databeskyttelse og internettkriminalitet.

---

[72] Hjemmeside: http://europa.eu.int/comm/dgs/information_society/index_en.htm
[73] Hjemmeside: http://www.europa.eu.int/scadplus/leg/en/lvb/l24100.htm ; http://europa.eu.int/information_society/index_en.htm
[74] http://www2.europarl.eu.int/omk/sipade2?PUBREF=-//EP//NONSGML+REPORT+A5-2003-0013+0+DOC+PDF+V0//EN&L=EN&LEVEL=2&NAV=S&LSTDOC=Y
[75] MEDDELELSE FRA KOMMISSIONEN TIL RÅDET, EUROPA-PARLAMENTET,DET ØKONOMISKE OG SOCIALE UDVALG OG REGIONSUDVALGET. Net- og informationssikkerhed: Forslag til en europæisk strategi, Bruxelles, den 6.6.2001, KOM(2001)298 endelig. http://europa.eu.int/eur-lex/da/com/cnc/2001/com2001_0298da01.pdf



Figur 6.1 Strategier for IKT-sikkerhet i EU

Rapporten peker på at de overnevnte områdene overlapper hverandre som det er vist eksempler på i Figur 6.1. Rapporten har ingen spesiell innretning mot sårbarhet i samfunnskritiske funksjoner. Det er de dagligdagse sikkerhetstruslene som har fokus, selv om det i korte trekk blir en bekymring over koblingen mellom nasjonal sikkerhet og informasjonssystemer. Det kan likevel hevdes at mange av forholdene som rapporten peker på har relevans i forhold til sårbarhet i samfunnskritiske og nasjonalt kritiske funksjoner.

Den tredje delen av rapporten legger frem forslag til en europeisk strategi. Den viser til at beskyttelse av kommunikasjonsnettene i stigende grad betraktes som en viktig oppgave for beslutningstakere, hovedsakelig på grunn av krav om beskyttelse av data, behovet for å sikre en velfungerende økonomi, hensynet til nasjonal sikkerhet og ut fra ønsket om å fremme elektronisk handel. Å fortsette å legge til rette for et lovverk som tar hensyn til dette fremstår som en av hovedstrategiene i rapporten. Videre peker den på viktigheten av å skape en felles forståelse for sikkerhetsutfordringene og de tiltak som må treffes for å skape korrekte lover og regler. Rapporten viser også til at politiske tiltak må benyttes til å rette opp og styrke markedsprosessene der hvor de ikke fungerer tilfredsstillende – også på sikkerhetsområdet.

Med blant annet denne rapporten i bunn, innførte EU en strategi for sikkerhet i datanettverk som ble godkjent av rådet i desember 2001.[76] Det er for omfattende å referere hele innholdet, men av særlig interesse er delen der rådet ber medlemslandene om å:

- Evaluere effektiviteten i den nasjonale organiseringen av håndteringen av kriser i datainfrastrukturen, med et særlig blikk på virusalarm systemer og evne til å forebygge, oppdage og reagere effektivt på nasjonalt nivå.
- Promotere bruken av fellesstandarder (ISO-15408)

[76] Council of the European Union, Brussels, 11 December 2001, 15152/01: http://europa.eu.int/information_society/eeurope/news_library/pdf_files/netsecres_en.pdf ; Rapport fra EU-Parlamentet, Committee on Industry, External Trade, Research and Energy, eEurope 2005: an information society for all: action plan in view of the Seville European Council, 21-22 June 2002, side 15: http://www2.europarl.eu.int/omk/sipade2?PUBREF=-//EP//NONSGML+REPORT+A5-2003-0013+0+DOC+PDF+V0//EN&L=EN&LEVEL=2&NAV=S&LSTDOC=Y

6.3 eEurope 2005 – EUs handlingsplan for bruk av IKT frem til 2005[77]

EU har en bred tilnærming til IKT innenfor rammen av den såkalte handlingsplanen eEurope 2005. eEurope 2005 etterfulgte strategien eEurope 2002. eEurope 2005 favner bredt, for det første med et særlig fokus på hvilke muligheter utnyttelse av bredbåndteknologi gir, og for det andre, hvilke muligheter utnyttelse av såkalt multiplattformtilgang gir. Det sistnevnte viser særlig til bruken av mobile enheter og digital tv for å koble seg til Internett. Det blir hevdet at det er disse to faktorene som fremover vil ha en særlig innvirkning på bruken av Internett. eEurope 2005 ble godkjent på toppmøtet i Sevilla i juni 2002.

- Målsettingen for eEurope 2005 er å skape et gunstig miljø for private investeringer, skape nye arbeidsplasser, øke produktivitet og modernisere offentlig tjenestevirksomhet. Alle skal gis mulighet til å delta i og høste nytte av informasjonssamfunnet. Handlingsplanen angir på denne bakgrunnen målene til å være å stimulere sikre tjenester, programvare og innhold basert på tilgjengelig bredbåndsteknologi. Innen 2005 er det satt opp en rekke mål som skal være nådd.

6.3.1 eEurope 2005 – hva med sikkerheten?

Handlingsplanen bygger videre på tidligere EU-strategier på sikkerhetsområdet[78] og foreslår tre handlinger relatert til sikkerhet. For det første opprettelsen av en *Cyber Security Task Force* (CSTF) med oppstart fra midten av 2003.[79] Hensikten er å skape et senter med kompetanse for IKT-sikkerhetsspørsmål. For det andre en såkalt *Culture of security*. I dette noe løse begrepet ligger å bygge sikkerhet inn i nye dataprodukter. Målsettingen er at dette skal gjennomføres innen 2005. Den tredje handlingen er å opprette et system for sikker kommunikasjon av gradert informasjon mellom medlemslandene.

Av særlig interesse er utviklingen av den såkalte *Cyber security task force*. Dette organet er fra

---

[77] Handlingsplanen eEurope 2005, ble godkjent av Det Europeiske Råd i Sevilla i juni 2002. COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS eEurope 2005: An information society for all An Action Plan to be presented in view of the Sevilla European Council, 21/22 June 2002. Brussels, 28.5.2002, COM(2002) 263 final.
http://europa.eu.int/information_society/eeurope/news_library/documents/eeurope2005/eeurope2005_en.pdf

[78] I handlingsplanen blir disse oppgitt til å være: Network and Information Security: Proposal for A European Policy Approach, COM(2001) 298 of 6.6.2001; Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890 of 22.1.2001; Directive 97/66/EC of the European Parliament and of the Council on 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24 of 30.1.1998; Council Resolution of 28 January 2002 (http://register.consilium.eu.int/pdf/en/01/st15/15152en1.pdf); Commission proposal for a Council Framework Decision on attacks against information systems (33 http://europa.eu.int/comm/dgs/justice_home/index_en.htm, COM(2002) 173 final of 19.4.2002.).

[79] I rådsresolusjonen om en europeisk strategi for en nett- og informasjonssikkerhetskultur av 18. februar 2003 og av 28. januar 2002 om nettverks- og informasjonssikkerhet, yttrykte Rådet tilsutning til Kommisjonens planer om å fremsette et forslag til opprettelsen av en *Cyber security task force*. Se: http://europa.eu.int/eur-lex/pri/da/oj/dat/2002/c_043/c_04320020216da00020004.pdf; http://europa.eu.int/eur-lex/pri/da/oj/dat/2003/c_048/c_04820030228da00010002.pdf ; http://europa.eu.int/eur-lex/da/com/cnc/2001/com2001_0298da01.pdf

februar 2003 omtalt som *European Network and Information Security Agency*.

6.3.2 European Network and Information Security Agency (ENISA)

I februar 2003 foreslo kommisjonen å opprette *European Network and Information Security Agency*. I forslaget legges det opp til et organ med et omfattende og ambisiøst nedslagsfelt. Utgangspunktet for opprettelsen var medlemslandenes forskjellige tilnærminger til IKT-sikkerhet og at medlemslandene er på forskjellige nivåer med forskjellig utgangspunkt i arbeidet med IKT-sikkerhet. Kommisjonen foreslo at det nye organet skal ha en rådgivende og koordinerende funksjon innenfor hele det indre marked (EØS-området).[80] Organet ble foreslått å fungere fra januar 2004 til utgangen av 2008 med en bemanning på 31 personer. Budsjettet ble satt til 24,3 millioner €.[81]

6.3.3 Et nedskalert European Network and Information Security Agency

På rådsmøtet i Luxembourg 5. juni 2003 ble det klart at ambisjonene måtte reduseres.[82] Det skyldtes motstand fra medlemsland som heller vil satse på nasjonale *Computer Emergency Response Teams* (CERT).[83] ENISA ble i større grad et rådgivende organ som overlater den endelige myndigheten til relevante nasjonale institusjoner. Denne løsningen ble stadfestet november 2003, da rådet og parlamentet formelt ble enige om å etablere organet.[84] Det ble da stadfestet at oppgavene skal knyttes til å:

- gi råd til medlemslandene og kommisjonen om IKT-sikkerhetsspørsmål
- analysere informasjon om nåværende og kommende IKT-trusler
- støtte EU i utviklingen av politikk på IKT-sikkerhetsfeltet
- øke bevisstheten om IKT-sikkerhetsspørsmål blant befolkning, forretningsliv og forvaltning samt hjelp til selvhjelp på feltet
- utføre risikovurderinger og risikostyring
- følge med i utviklingen av ny forskning på området

Det kan i denne sammenhengen nevnes at også Norge tar sikte på å delta i dette samarbeidet.[85] ENISA skal være operativt fra 2004.

---

[80] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Establishing the European Network and Information Security Agency, Brussels, 11.2.2003, COM(2003) 63 final,2003/0032 (COD). http://europa.eu.int/information_society/eeurope/news_library/documents/nisa_en.pdf

[81] Om lag 197 millioner NOK (juni 2003).

[82] Se pressemelding: 2515th Council meeting - TRANSPORT, TELECOMMUNICATIONS AND ENERGY - Luxembourg, 5 June 2003, 9686/03 (Presse 146) http://ue.eu.int/pressData/en/trans/76064.pdf

[83] http://www.infosecuritymag.com/2003/jun/digest09.shtml#news5

[84] Se pressemelding fra kommisjonen datert 20/11/2003: " "Commission welcomes agreement of Council and Parliament to set up the European Network and Information Security Agency", http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/03/1577|0|AGED&lg=EN&display=

[85] Nasjonal strategi for informasjonssikkerhet, juni 2003. Forsvarsdepartementet, Nærings- og handelsdepartementet og Justis- og politidepartementet, http://www.odin.dep.no/archive/nhdvedlegg/01/06/Nasjo006.pdf

6.4 Andre relevante tiltak og forskningsinitiativ innenfor rammen av IKT-sikkerhet i EU

6.4.1 ESOs

En viktig del av IKT-sikkerhetsarbeidet er knyttet til standardisering av sikkerhetsteknologier. EU-kommisjonen har bedt tre organisasjoner om å ta på seg et slikt arbeid. To av disse er relevante i vår sammenheng. De heter *The European Committee for Standardization* (CEN) og *The European Telecommunications Standard Institute* (ETSI).[86] Begge ligger innenfor rammen av *European Standardization Organizations* (ESOs) som arbeider med standardisering innen en rekke områder.[87] [88] Dette arbeidet har sitt utspring i en generell anerkjennelse om at standardiseringsarbeid er viktig for utbredelsen av teknologier, og er forankret i eEurope-handlingsplanene.

6.4.2 IST forskningsprogrammer

IST (*Information Society Technologies*)[89] ligger innenfor det såkalte sjette rammeverket for forskning og utvikling i EU og støtter en rekke relevante forskningsprogrammer. Av disse er de såkalte "veikartprosjektene" relatert til IKT-sikkerhet av interesse.[90] Disse er:

- DDSI
  Dependability policy support
- ACIP
  Critical Infrastructure protection
- WG-ALPINE
  Active Loss Prevention
- AMSD
  Overall Dependability, e-business embedded CIP privacy
- PAMPAS
  Mobile privacy & security
- AMSD
  Dependable embedded systems
- RAPID
  Privacy/Identity Management
- BVN
  Biometrics
- RESET
  SmartCards

[86] Den tredje organisasjonen heter CENELECog er "*the European Committee for Electrotechnical Standardization*". Den faller utenfor vår ramme. For mer info om CENELEC, se: http://www.cenelec.org
[87] Smartkort, elektroniske signaturer, mobile signaturer, elektronisk autentisering, mobil telefonitrafikk, lovlig inntrengning i datatrafikk, kryptografialgoritmer, sikker trådløs teknologi, sikring av personlig informasjon og nye IP-standarder.
[88] For mer informasjon om arbeidsområdene, se http://www.eeurope-standards.org/Docs/E-Security.pdf
[89] http://www.cordis.lu/ist/
[90] http://www.cordis.lu/ist/ka2/rmapsecurity.html

- STORK
  Crypto

Det vil i denne omgang trekkes frem det mest relevante, nemlig DDSI og ACIP.

6.4.3 DDSI (Dependability Development Support Initiative)

DDSI var et prosjekt som ble startet juni 2001 for å understøtte EU-kommisjonen i utviklingen av strategier for pålitelighet i elektroniske informasjonssystemer. Arbeidet ble avsluttet i november 2002. Arbeidsgruppen bestod av personer fra institusjoner som RAND Europe sammen med King's College i London, Industrieanlagen-Betriebsgesellschaft mbH (IABG) fra Tyskland og Cellnetwork fra Sverige.[91] Den hadde som målsetting å skape et nettverk av interessenter, skaffe til veie grunnlagsdata og utvikle policy-retningslinjer. Hovedfokus var på pålitelighet i informasjonsinfrastruktur og elektroniske tjenester innenfor rammen av EUs politikkområde/aktivitet *Information Society*. Av særlig interesse er for det første oversikten de har laget over 31 forskjellige lands arbeid på IKT-sikkerhetsområdet. Blant disse er de nordiske land, Storbritannia, Australia, Kina, Russland og USA.[92] For det andre er DDSIs hovedrapport av interesse.[93] Den ser på hvilke handlinger det er behov for, og hvilke valg og konsepter myndigheter og andre står overfor ved diskusjoner om pålitelighet i IKT-systemer.

6.4.4 ACIP - Analysis and Assessment for Critical Infrastructure Protection

Prosjektet ble startet juni 2002 og avsluttet sommeren 2003. Deltagerne var blant annet fra IABG i Tyskland, Fraunhofer i Tyskland, Rand Europe og Cell Network i Sverige.[94] Målet med prosjektet var å fastslå hvordan beskyttelse av kritisk infrastruktur kan bli analysert og vurdert ved hjelp av modeller og simulering. Det er blitt produsert en rekke rapporter av både teknisk og mer policy-orientert karakter, og det vil i denne omgangen bare bli trukket frem hovedmålsetningene med prosjektet:

- Identifisering og evaluering av status på kritisk infrastruktur beskyttelse (CIP - *critical infrastructure protection*)
- Analyse av gjensidig avhengighet i infrastrukturer og kaskadeeffekter ved tilfeller av forstyrrelser
- Utredning av forskjellige scenarier for å finne hull, mangler og robusthet i CIP
- Identifisering av teknologisk utvikling og nødvendige beskyttende forhåndsregler med hensyn til CIP

[91] Også andre insitusjoner ble trukket med, men disse fire ble definert som kjernegruppen. For de andre institusjoene, se DDSIs hjemmeside: http://www.ddsi.org/DDSI-F/main-fs.htm
[92] DDSI har laget oversikt over IKT-sikkerhetsarbeidet i følgende land: Australia, Østerrike, Belgia, Canada, Kina, Kypros, Tsjekkia, Danmark, Estland, Finland, Frankrike, Tyskland, Helleas, Ungarn, India, Irland, Italia, Japan, Liechtenstein, Luxembourg, Nederland, Norge, Polen, Portugal, Russland, Slovenia, Spania, Sverige, Sveits, Storbritannia, USA. http://www.ddsi.org/DDSI-F/main-fs.htm
[93] http://www.ddsi.org/Documents/final%20docs/DDSI_D1_concept_paper_f.pdf
[94] For en full liste over medlemmer av konsortiumet, se http://www.iabg.de/acip/members.html og http://www.iabg.de/acip/management.html

6.5 Avslutning

Kommisær Erkki Liikanen peker på tre brede kategorier av arbeide med cybersikkerhet i EU.[95] For det første er EU i ferd med å få et lovverk om telekommunikasjon og databeskyttelse på plass. Blant annet vil et direktiv om databeskyttelse bli implementert. Også et lovrammeverk for elektronisk kommunikasjon vil komme i løpet av kort tid. Denne skal sikre tilgjengelighet, integritet og konfidensialitet i all elektronisk kommunikasjon. For det andre er det en stadig utvikling i politikken knyttet til Cyberkriminalitet. *Justice and Home Affairs Council* (i Unionsrådet) tok opp en (*adopted*) såkalt *Framework decision on attacks on information systems* som ifølge Liikanen blir sett på som et stort skritt for å hindre at Europa blir et friområde for elektronisk kriminalitet. Den tredje brede kategorien er aktiviteter på feltet nettverks- og informasjonssikkerhet. Her er det særlig det såkalte *European Network and Information Security Agency* som bli fremhevet som en viktig aktivitet av Liikanen.

Hva kan trekkes ut av strategien for IKT-sikkerhet i EU? Hovedstrategien for IKT generelt må naturlig nok sies å være å tilrettelegge for ytterligere verdiskapning og bedre tjenester for EUs innbyggere. Det er lagt opp til en tresidig strategi hvor for det første lovverket må ligge på plass som en tilrettelegger. For det andre må en stimulere slik at privat forretningsvirksomhet kan vokse og levere relevante tjenester til brukere. Det er her et særlig fokus på bredbåndsteknologi og multiplattformtilgang. Handlingsplanen eEurope 2005 kommer inn her. For det tredje må en stimulere til forskning og utvikling. EUs sjette rammeverk for forskning og utvikling som løper i perioden 2002-2006, legger opp til dette. Dette rammeverket har for øvrig et totalt budsjett på 17,5 mrd €. EUs arbeide med IKT-sikkerhet skal bygge opp under og sikre disse tre hovedstrategiene.

Hva så med den delen av IKT-sikkerhet som er relevant for BAS5, nemlig de samfunnskritiske og nasjonalt viktige systemene? Det er funnet en del forskningsprosjekter som kan dekke dette, men det er naturlig at forhold knyttet til nasjonal sikkerhet i en eller annen form i første rekke er forankret hos nasjonale myndigheter. Fra EU-kommisjonens side har de gjennomførte og foreslåtte tiltakene i første rekke som formål å sikre forretningsvirksomhet, offentlige kontorers virksomhet og privatpersoners bruk.

En av utfordringene med EUs tilnærming til IKT-sikkerhet er den store kompleksiteten. Et forhold er behandlingen og initiativ mellom EUs forskjellige institusjoner, en annen er den store innsatsen som blir lagt ned i forskning. Under EUs femte rammeverk (1998-2002 *Framework Programmes*) for forskning og utvikling ble feltet IKT-sikkerhet støttet med 80 mill. € fordelt på 75 prosjekter. Vi er nå inne i EUs sjette rammeverk, og det er naturlig å anta dette feltet vil vokse fremover. En oversikt over hvilke nye prosjekter som iverksettes kan vise seg å være svært nyttig, i tillegg til at de kan bidra til å gi en forståelse for hva som skjer i EU-land hvor språket i utgangspunktet er en barriere. Som en kompliserende faktor er den store mengden med forskning og initiativer fra EUs side, som tilsier en sterk bevissthet rundt prioritering og

[95] Cybersecurity and the European Network and Information Agency, tale av Erkki Liikanen, 11. juni 2003. http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=SPEECH/03/293|0|RAPID&lg=EN&display=

utvelgelse av informasjon. Et fokus på EU-kommisjonens arbeide innenfor rammen av eEurope 2005 og et fokus på hva som skjer i det såkalte IST *research programme* er det beste utgangspunktet for en videre oppfølgning.[96] Arbeidet med EUs nye grunnlov i det såkalte konventet er ikke tatt med, og det vites ikke om dette vil få noen påvirkning i vår sammenheng.

7 OPPSUMMERING OG AVSLUTTENDE VURDERINGER

Denne rapporten er en første gjennomgang av arbeidet med strategier og planer for informasjonssikkerhet i tre utvalgte land, nemlig Norge, USA og Australia. I tillegg er initiativer EU har tatt på dette feltet studert. Hensikten har vært å avdekke om det er laget strategier for informasjonssikkerhet på nasjonalt plan og avdekke nasjonenes mål og virkemiddelbruk.

Både USA og Norge har strategidokumenter relatert direkte mot informasjonssikkerhet på nasjonalt nivå. USA har, slik vi tolker, det et vesentlig større fokus mot målrettede trusler og planlagte ondsinnede anslag enn det Norge har. Det norske fokuset er rettet mot tilfeldige anslag og trusler som typisk oppstår i ordinære fredssituasjoner. Imidlertid må det legges til at det norske regimet innen telesikkerhet og –beredskap har større fokus mot høynivå trusler enn det som går frem av det nasjonale strategidokumentet. EUs rolle er litt spesiell, i og med at EU er en overbygning for det nasjonale nivået, samtidig som ansvaret for sikkerhet er lagt på nasjonene. EUs forslag om en europeisk CERT strandet også fordi nasjonene heller ville ha nasjonale CERTer. EUs rolle blir dermed mer en tilrettelegger på tvers av nasjonsgrenser. Australia har ikke noe strategidokument, så langt vi har sett, men har allikevel implementert en rekke tiltak og gjort mye innenfor området informasjonssikkerhet. Arbeidet har vært drevet av en ambisjon om å ligge i teten internasjonalt når det gjelder bruk av IKT. Det australske fokuset synes også å være mer fredsrettet, blant annet er fysisk redundans i nettene et ”ikke mål”.

I USA er ansvaret for informasjonssikkerhet plassert i DHS og hele sikkerhetsfokuset er blitt sentralisert og løftet opp på føderalt nivå. Det norske sikkerhetsfokuset må derimot hevdes å være sektorisert. Ansvaret for informasjonssikkerhet er fragmentert og oppdelt på ulike departementer og offentlige etater. For å bøte på dette er det i strategien foreslått et koordinerende utvalg. Etter vårt syn er det tvilsomt om dette er en god løsning, blant annet fordi det er mange som er involvert. Manglende kompetansetilgang i forhold til en svært kompleks teknologisk sektor vil også være et problem ved en slik tilnærming. I Australia er det ESCG som er den øverste koordinator. EU tar ikke noe ansvar i så måte, men det er likevel verdt å nevne at informasjonssikkerhet sorterer under Information Society Directorate General.

Når det gjelder tiltak for øvrig er det mye som er felles. Det er opprettet organisasjoner som har ansvar for å være meldingssentraler ved datainnbrudd og –angrep, ha rådgivende funksjoner

[96] IST: http://www.cordis.lu/ist/ ; http://europa.eu.int/information_society/eeurope/index_en.htm ; http://europa.eu.int/comm/dgs/information_society/index_en.htm ; http://europa.eu.int/information_society/index_en.htm

mm, og det satses på å bygge sikkerhetskultur, å heve kunnskapsnivået gjennom utdanning og forskning, på internasjonalt samarbeid, harmonisering av lovverk, PKI og sertifiseringsordninger for informasjonssikkerhet. De nasjonale variasjonene går på plassering av ansvar og vektleggingen av samarbeid mellom private og offentlige virksomheter. USA er spesiell i så måte fordi USA har hatt et liberalisert markedsregime innenfor kritisk infrastruktur lengst. Dermed er privatiseringen kommet lengst her, og samarbeidet med privat sektor er dermed svært viktig.

Dette har vært en første tilnærming til det arbeidet som er gjort i Norge og andre utvalgte land, og kan følges opp med mer detaljerte studier blant annet med hensyn til tiltak og deres kostnader. Dessuten vil det også være nyttig å følge med på forskning innenfor området både det som skal skje i regi av Norges forskningsrådsprogram SoS og i EUs 6 rammeprogram. Dersom hele trusselspekteret skal legges til grunn for sårbarhetsanalyser og anbefaling av tiltak i BAS5-prosjektet, vil det også være viktig å følge med i den militære forskningen innenfor defensive og offensive Computer Network Operations (CNO). Tilsvarende gjelder også for utviklingstrender innen mulig fremvekst av cyber-terror.

APPENDIKS

A OECDS GRUNNLEGGENDE PRINSIPPER

De ni grunnleggende OECD-prinsippene er:

- Bevisstgjøring: Aktørene må være bevisste på behovet for å sikre informasjonssystemer og nettverk og hva de kan gjøre for å forbedre sikkerheten.
- Ansvar: Alle aktører er ansvarlige for sikkerheten til informasjonssystemer og nettverk.
- Reaksjon: Aktørene må reagere raskt og på en samarbeidsrettet måte for å forebygge, oppdage og reagere på sikkerhetshendelser.
- Etikk: Aktørene må respektere andre aktørers rettmessige interesser.
- Demokrati: Sikkerheten til informasjonssystemer og nettverk må være forenlig med grunnleggende verdier i et demokratisk samfunn.
- Risikovurdering: Aktørene må gjennomføre risikovurdering.
- Sikkerhetsdesign og iverksettelse: Aktørene må gjøre sikkerheten til en integrert del av informasjonssystemer og nettverk.
- Sikkerhetsadministrasjon: Aktørene må innføre en helhetlig tilnærming til sikkerhetsadministrasjon.
- Løpende vurdering: Aktørene må løpende gjennomgå og vurdere sikkerheten til informasjonssystemer og nettverk og foreta hensiktsmessige endringer i politikk, rutiner, tiltak og prosedyrer. [97]

[97] http://www.digi.no/dtno.nsf/pub/dd20020926151643_ero_80736552

B DEN NORSKE STRATEGIEN FOR INFORMASJONSSIKKERHET – FOKUSOMRÅDER

Norges fokusområder for informasjonssikkerhet er:

- Fellesstandarder for ROS
- Prioriterte linjer
- Ansvar for regelverket
- Koordineringsutvalg
- Sikkerhetsstandarder
- Informasjonsside på nettet
- VDI
- Sertifisering
- FoU
- PKI
- Internasjonalt samarbeid

Nedenfor utdypes intensjonene for disse:

Fellesstandarder for ROS
Under det første punktet, beskytte kritisk IT-infrastruktur, ønsker Regjeringen gjennom denne strategien blant annet å "lage et felles sett med kriterier som gjør det mulig å identifisere samfunnskritisk IT-infrastruktur og systemer" (10). Videre ønsker man å gjennomføre risiko og sårbarhetsvurderinger av slike systemer. Gjennomføringsansvaret for dette er spredt på blant annet JD, FD, DSB og NSM.

Prioriterte linjer
I en krisesituasjon hvor telenettene blir overbelastet grunnet ødeleggelse på nettene eller annen ødeleggelse som skaper stor trafikkmengde i nettet, vil ikke nøkkelpersoner eller etater, slik systemet er i dag, være garantert dekning. Dette ønsker Regjeringen å gjøre noe med ved å innføre prioritetsordninger i telenettet. En slik ordning vil måtte omfatte alle tilbyderne av offentlige teletjenester og Post- og teletilsynet har fått i ansvar å utarbeide krav til en slik ordning.

Ansvar for regelverket
Vi har i dag en situasjon hvor ansvaret for ulike regelverk knyttet til IKT-sikkerhet er spredt rundt på mange offentlige instanser. Tabell A.1, som er hentet fra vedlegg 2 i strategien, gir en oversikt over noen sentrale regelverksforvaltere innen informasjonssikkerhet (10). Situasjonen som Tabell A.1 viser gjør at håndhevingen av regelverket innen IKT-sikkerhet kan bli komplisert. Regjeringen ønsker derfor, som en del av den nasjonale strategien for informasjonssikkerhet, å foreta en gjennomgang av eksisterende regelverk for å en bedre og mer

samordnet håndhevning av regelverket. Videre oppfordres de ulike regelforvalterne til å foreta periodiske gjennomganger av regelverket for å vurdere hvordan dette faktisk fungere i praksis, og på bakgrunn av dette vurdere eventuelle endringer i regelverket (10).

Myndighet	**Aktuelt lov-/regelverk**
Forsvarsdepartementet/Nasjonal sikkerhetsmyndighet	Sikkerhetsloven med forskrifter, beskyttelsesinstruksen (IT-delen)
Samferdselsdepartementet / Post og teletilsynet	Teleloven (Lov om elektronisk kommunikasjon) med forskrifter
Nærings- og handelsdepartementet	Lov om elektronisk signatur, forskrift om krav til utsteder av kvalifiserte sertifikater mv
Datatilsynet	Tilsyn i forhold til personopplysningsloven med forskrifter
Arbeids- og administrasjonsdepartementet	Forskrift til personopplysnings loven, forskrift om elektronisk kommunikasjon med og i forvaltningen
Statsministerens kontor	Beskyttelsesinstruksen (kgl. res. av 17.3.72, endret 29.6.01)
Justisdepartementet	Personopplysningsloven, forvaltningsloven og offentlighetsloven, flere kongelige resolusjoner
Direktoratet for samfunnssikkerhet og beredskap	Sivilforsvarsloven, kgl. res. av 24.3.73, av 16.9.94, og av 3.11.00, flere andre lover
Kredittilsynet	Kredittilsynsloven/IT-forskriften
Norges Bank	Sentralbankloven
Økokrim (Politiets datakrimsenter)	Straffeloven, Straffeprosessloven
Politiets sikkerhetstjeneste	Politiloven (§17a,b,c)
Forsvarets Overkommando / Etterretningsstaben	Lov om Etterretningstjenesten
Næringslivets sikkerhetsorganisasjon	Sivilforsvarsloven, HMS-forskrifter
Sosial- og helsedirektoratet	Helsepersonelloven
Rikstrygdeverket	Folketrygdloven (§25)

Tabell A.1 Oversikt over noen sentrale regelverksforvaltere innen informasjonssikkerhet

Koordineringsutvalg
For å samordne utøvelsen av tilsynsvirksomheten, bedre samordningen av videreutviklingen av IT-sikkerhetsregelverket og samordne håndhevingen av IT-sikkerhetsbestemmelser for å forenkle etterlevelse hos brukerne (10), ønsker Regjeringen å opprette et permanent koordineringsutvalg for IT-sikkerhet. Ansvaret for opprettelsen av dette utvalget er gitt til JD, FD, NHD og AAD.

Sikkerhetsstandarder
For spesielt å bedre små- og mellomstore bedrifter evne til å håndtere IT-sikkerhet skal det i regi av NHD i samarbeid med bransjeorganisasjoner, regelverksforvaltere og internasjonale

organisasjoner utarbeides verktøy og metoder for risiko og sårbarhetsanalyser (10). Regjeringen ønsker også at relevante sektororganisasjoner og sektormyndigheter i samarbeid med Næringslivets Sikkerhetsorganisasjon utarbeider klassifikasjonsordninger og sikkerhetsnormer for private virksomheters informasjonsbehandling.

Informasjonsside på nettet
For å gjøre arbeidet med å sikre kritiske IKT-systemer enklere er informasjon om temaet et viktig hjelpemiddel. Det er spesielt viktig at informasjon om IKT-sikkerhet når ut til vanlige bruker med i utgangspunktet lite eller ingen spesifikk kunnskap om IKT-sikkerhet. I den nasjonale strategien for informasjonssikkerhet ønsker derfor Regjeringen å etablere en nettbasert informasjonstjeneste med generell informasjon og lenker til relevant tilleggsinformasjon. Tjenesten, som NHD i samarbeid med JD har fått i ansvar å opprette, skal også gi mulighet til å besvare spørsmål fra brukerne. Videre ønsker Regjeringen å øke fokus på IKT-sikkerhet i så vel skole som næringsliv ved å utarbeid en "undervisningspakke" innen IKT-sikkerhet for grunn- og videregående skole. Regjeringen, gjennom NHD og AAD, vil også arbeide for at ledere i private og offentlige virksomheter tar ansvar for å sikre at virksomheten har tilstrekkelig kompetanse innen IKT-sikkerhet (10).

VDI
Under fokusområde 7, varsle og gi råd, i strategien forslår Regjeringen i alt to tiltak, rettet mot telesektoren spesifikt i form av et kriseteam for telesektoren og et varslingssystem for digital infrastruktur (VDI) (10). VDI har i en periode vært organisert som et prøveprosjekt, men er fra 1. januar 2004 vedtatt etablert som en permanent ordning under NSM. VDI har som oppgave og analysere trafikkmønstre på Internett for å fange opp mulige angrep og hendelser.

Sertifisering
Som et ledd i ansvarliggjøringen av bransjen og de ulike leverandørene oppfordrer Regjeringen gjennom strategien de ulike aktørene til å følge anerkjente sikkerhetsnormer og standarder og gjøre kjent hvilket sikkerhetsnivå tjenesten tilbyr. Det er også viktig å synliggjøre stabiliteten i tjenesten som tilbys, og hvilken brukerhjelp som kan ytes ved en feilsituasjon (10).

For å bedre IKT-sikkerheten i norske organisasjoner og produkter oppfordrer Regjeringen gjennom denne strategien norske virksomheter til å bedre ta i bruk sertifiseringsordninger for implementering av IKT-sikkerhet i organisasjoner og produkter. Her nevnes blant annet BS7799-ordningen under Norsk Akkreditering og SERTIT-ordningen under NSM (10).

FoU
Norges Forskningsråd har i samarbeid med NHD, JD og FD etablert et flerårig forskningsprogram innen IKT-sikkerhet som skal dekke ulike sider ved IKT-sikkerhet. Fokus på sikkerhet innen IKT-forskningen blir også bekreftet i NHDs "Strategi for IKT-forskningen 2003-2004" utgitt i januar 2003 hvor Sikkerhet og tillit er et prioritert område i tråd med EUs IST-arbeidsprogram (12). Regjeringen ønsker også å fokusere på IKT-sikkerhet innen høyere utdanning og det er en uttalt målsetning gjennom strategien at det skal fokuseres på

undervisning i IKT-sikkerhet ved universiteter og høyskoler, spesielt gjennom studier innen IKT-sikkerhet på mastergradsnivå. [98]

PKI

For å gi elektroniske dokumenter den samme juridiske trygghet som papirbasert dokumenter er det viktig å ha en tilfredsstillende infrastruktur som muliggjøre dette. Det vil her være viktig at infrastrukturen er bygd opp på en måte som gjør det mulig å skape tillit mellom de personer som ikke kjenner hverandre. Det er også viktig at informasjonens integritet og konfidensialitet beskyttes. Regjeringen ønsker å etablere en slik infrastruktur ved hjelp av elektroniske signaturer og PKI (10). Den nasjonale strategien for informasjonssikkerhet legger på dette området opp til en rekke tiltak rettet mot både offentlig og private sektor for å stimulere til økt bruk av PKI-løsninger. En nærmere beskrivelse av de aktuelle tiltakene finnes i strategienes fokusområde nr 11.

Internasjonalt samarbeid

Det siste fokusområdet i strategien omhandler internasjonalt samarbeid og inneholder 2 tiltak rettet mot deltakelse i ulike internasjonale fora. Blant annet ønsker Regjeringen å arbeide for at internasjonale fora som arbeider med IKT-sikkerhet legger sine møter til Norge, slik at flest mulig norske aktører kan dra nytte av dette arbeidet. Videre er deltakelse i det planlagte organet for nettverks- og informasjonssikkerhet i EU en prioritet fra Regjeringens side.

[98] Høgskolen i Gjøvik tilbyr fra høsten 2003 en Mastergradsutdanning i Informasjonssikkerhet. For mer informasjon se http://www.hig.no

C USAS NASJONALE STRATEGI FOR INFORMASJONSSIKKERHET

Den amerikanske nasjonale strategien for informasjonssikkerhet ble utgitt i februar 2003 etter en lang prosess som inkluderte mange ulike aktører. Det ble blant annet holdt møter i ti store byer for å få innspill fra lokale myndigheter og private aktører (8). I etterkant av disse møtene ble det gjennomført en høringsrunde på et utkast til strategien på Internett, og de som ønsket det kunne gi tilbakemeldinger over nettet. Et viktig prinsipp i strategien er samarbeidet mellom offentlige og private aktører for å muliggjøre best mulig beskyttelse av kritiske IKT-systemer. Dette prinsippet har også vært gjeldende for utviklingen av strategiene ved at det som innspill til strategiarbeidet, er utviklet en rekke sektorspesifikke informasjonssikkerhetsstrategier under ledelse av organisasjonen "The Partnership for Critical Infrastructure Security" (PCIS). Under følger en liste over de sektorvise strategiene som ble utarbeidet, og offentliggjort 18 september 2002 (8):[99]

- Bank og finans
- Forsikring
- Kjemisk industri
- Olje og gass
- Kraftforsyning
- Politi
- Høyere utdanning
- Transport (Jernbane)
- Informasjons- og kommunikasjonsteknologi
- Vannforsyning

I tråd med "the National Strategy for Homeland Security" har den nasjonale IKT-strategien følgende tre målsetninger (2) (8):

- Forhindre angrep mot amerikanske kritiske IKT-systemer
- Redusere den nasjonale sårbarheten som følge av angrep mot IKT-systemer
- Redusere skadene og reetableringstiden dersom angrep mot kritiske IKT-systemer allikevel skulle forekomme

Da mye av den kritiske infrastrukturen befinner seg på private hender, er man avhengig av et sterkt offentlig-privat samarbeide for å nå disse målsetningene. Som nevnt over, har et slik samarbeide vært et viktig prinsipp under arbeidet med strategiene. Andre førende prinsipper som ligger til grunn for strategiene er følgende (8):

1. ***En nasjonal innsats.*** USA har en tradisjon for begrenset statlig eierskap av kritisk infrastruktur. Dette gjør at en strategi for å sikre nasjonale kritiske IKT-systmer må være

[99] Disse strategiene er tilgjengelige på http://www.pcis.org

en nasjonal innsats hvor ikke-statlige organisasjoner også gjør en innsats. Et førende prinsipp for det statlige engasjementet er at nytten overgår kostnadene for de ulike tiltakene. Som en konsekvens av at dette må være en nasjonal innsats oppfordres alle som ønsker å være med i arbeidet med å sikre IKT-systemer, om å gjøre dette. Myndighetene vil støtte opp om ulike samarbeidsordninger mellom det offentlige og det private for blant annet å øke bevisstheten knyttet til IKT-sikkerhet og å utdanne personell.

2. ***Beskytte privatlivet og sivile rettigheter.*** Misbruk av kritiske IKT-systmer er en trussel mot privatlivet og etablerte sivile rettigheter. I følge den nasjonale IKT-strategien er det viktig for de føderale myndigheten og påse at slikt misbruk ikke finner sted. Det er derfor viktig at beskyttelsen av kritiske IKT-systmer faktisk ikke også medfører en trussel mot privatlivet og etablerte sivile rettigheter. Et eksempel, som trekkes frem her, er at informasjon som frivillig blir gitt til myndighetene behandles på korrekt måte (konfidensialitet).

3. ***Regulering og markedskrefter.*** Reguleringer fra føderalt hold, om hvordan selskaper skal sikre sine kritiske IKT-systemer, vil kunne føre til at sikkerheten i slike systemer blir dårligere enn dersom slike reguleringer ikke hadde eksistert. En av grunnen til dette ligger i at slike reguleringer kan føre til mindre forskning på området. Derfor ønsker ikke de føderale myndighetene å bruke reguleringer som det fremste virkemiddelet for å øke IKT-sikkerheten, men forventer at den største drivkraften for å sikre kritiske IKT-systemer kommer fra markedet selv.

4. ***Ansvar og myndighet.*** Et fokusområdet for den nasjonale IKT-strategien er å etablere en mer fleksibel og pålitelig informasjonsinfrastruktur. For å få til dette blir det utpekt departementer eller byråer som får hovedansvar for en bransje når det gjelder føderale initiativer i forhold til IKT-sikkerhet. DHS vil også få en sentral rolle i arbeidet med implementeringen av den nasjonale IKT-strategien.

5. ***Sikre fleksibilitet.*** Trusselen mot IKT-systemer endres raskt. Det er derfor viktig at man opprettholder en god fleksibilitet i evnen til å besvare slike trusler. Ved å være fleksible i planleggingsarbeidet vil man raskere kunne revurdere truslene mot IKT-systemene og iverksette relevante tiltak mot den aktuelle trusselen.

6. ***Flerårig planlegging.*** Arbeidet med å sikre IKT-systemer er en pågående prosess, etter hvert som nye teknologier og trusler oppstår. Slik det fremgår av den nasjonale IKT-strategien danner den strategien et utgangspunkt for å bedre sikkerheten i kritiske IKT-systemer. Det oppfordres imidlertid til at departementer, byråer og andre aktuelle aktører benytter seg av et flerårig planleggingsløp for å styrke sin rolle i beskyttelsen av respektive IKT-systemer.

Prinsippene over har vært førende for utviklingen av strategien. For å nå målsettingene som

nevnt over, skisserer den nasjonale IKT-strategien i alt 47 ulike tiltak fordelt på følgende fem prioriterte områder:

- Et nasjonalt reaksjonssystem for IKT-sikkerhet
- Et nasjonalt program for å redusere IKT relaterte trusler og sårbarheter
- Et nasjonalt bevisstgjørings- og utdanningsprogram innen IKT sikkerhet
- Sikre statlige IKT-systemer
- Nasjonal sikkerhet og internasjonalt samarbeid om IKT-sikkerhet

Disse områdene med tilhørende tiltak vil bli nærmere presentert i egne avsnitt under. Først presenters imidlertid en mer generelle og tallmessig analyse av tiltakene i strategien. Under gis en oversikt over hvordan de ulike tiltakene er fordelt mellom føderale myndigheter, statlige/lokale myndigheter og private aktører.

	Føderal	Statlig/lokal	Private aktører
Antall tiltak	40	1	11
%-vis fordeling	77 %	2%	21%

Tabell C.1 Fordeling av tiltak mellom føderale myndigheter, statlige/lokal myndigheter og private aktører[100]

Som Tabell C.1 viser er de fleste tiltakene rettet mot de føderale myndighetene. En av bakgrunnene for dette ligger nok i ønsket om ikke å bruke reguleringer for private aktører for å oppnå bedre IKT-sikkerhet. Ser man på hvor mange av tiltakene som er rettet mot de ulike aktørene kommer det klart fram at tiltakene rettet mot det private i all hovedsak er frivillige tiltak og anmodninger, mens tiltakene rettet mot føderale myndigheter for det meste er pålegg.

	Føderal	Statlig/lokal	Private aktører
Frivillig	7,5 %	100 %	90,9 %
Pålegg	92,5 %	0 %	9,1 %

Tabell C.2 %-vis fordeling mellom frivillige tiltak og pålegg

C.1 Nærmere beskrivelse av de fem fokusområdene i USAs IKT-strategi

Det første fokusområdet har som mål å forbedre USAs evne til å reagere mot IKT-sikkerhetsrelaterte hendelser, samt redusere den potensielle skaden fra slike. Strategiene foreslår i alt 7 ulike tiltak under dette fokusområdet, herunder etablering av et offentlig-privat samarbeid for å bedre kunne besvare angrep mot nasjonal kritisk IKT-infrastruktur.

Under det andre fokusområdet foreslår strategien i alt 15 ulike tiltak rettet mot å redusere trusselen mot, og sårbarheten i IKT-systemer. Vi har i dag en rivende utvikling innen teknologi, hvor stadig nye systemer og teknologier blir lansert. Dette fører igjen til at nye potensielle sårbarheter blir introdusert i kritiske systemer. Den amerikanske strategien anser det som lite

[100] Grunnen til at antall tiltak i tabellen er flere enn de tidligere nevnte 47 er at enkelte av tiltakene henvender seg til flere aktører

realistisk å eliminere alle sårbarheter og trusler mot kritiske ITK-systmer, og har derfor følgende delmål for dette fokusområdet:

- Redusere trusler og motarbeide ondsinnede aktører gjennom effektive tiltak for å identifisere og straffe slike aktører.
- Identifisere og minimere de gjenværende sårbarhetene som kan skape de største konsekvensen for kritisk infrastruktur dersom de blir utnyttet
- Utvikle nye systemer med færre sårbarheter samt vurdere nye teknologi for sårbarhetsredusering

Det tredje fokusområdet i strategien foreslår 9 ulike tiltak for å bedre kunnskapen om sikkerhet blant brukere av IKT-systemer. Mange av de sårbarhetene som i dag eksistere i en rekke systemer, kunne enkelt vært fjernet dersom brukere og administratorer hadde hatt den rette kunnskapen. Et viktig området for den amerikanske strategiene er derfor å foreslå tiltak som er rettet inn mot å bedre kunnskapen og bevisstheten om sikkerhet i IKT-systemer blant brukerne av slike systemer.

Selv om mye av den kritiske infrastrukturen i USA er eid av private aktører, har også myndighetene ansvaret for en rekke kritiske systemer. Enkelte av disse systemene kan også være av vital nasjonal interesse. Det er derfor viktig at statlige IKT-systemer er sikre, slik at disse ikke kan misbrukes. Det fjerde fokusområdet foreslår i alt 6 ulike tiltak rettet mot å bedre sikkerheten i statlige IKT-systemer. Et annet poeng med å sikre statlige systemer, som også fremheves i strategien, er at staten på den måten kan gå foran med et godt eksempel for hvordan man skal sikre sine IKT-systemer.

Internett er et verdensomspennende nettverk som visker ut de tidligere så klare geografiske grensene mellom land. Dette gjør at stadig flere aktører vil være i stand til å gjøre skade på amerikanske kritisk infrastruktur. Den nasjonal strategien for informasjonssikkerhet ser dette som et stort problem, og ser derfor behovet av et internasjonalt samarbeid for å utveksle informasjon og redusere sårbarheter i systemer. Under dette fokusområdet foreslår strategien i alt 10 ulike tiltak, som er rettet mot å øke den nasjonale sikkerheten og bedre det internasjonale samarbeidet knyttet til IKT-sikkerhet

C.2 Ressursforbruk

Fokus på beskyttelse av kritisk infrastruktur står høyt i USA. Dette gjør seg også gjeldende i de ressursene som settes av til dette formålet i budsjettet for 2004. I forslaget til budsjett for DHS for 2004 har departementet fått i alt 36,2 mrd USD til disposisjon, noe som er en økning på 7,4% fra 2003 og over 64% mer enn det som ble brukt på disse aktivitetene i 2002 (9). For Direktoratet for informasjonsanalyse og beskyttelse av infrastruktur foreslår budsjettet i alt 829 millioner USD, som blant annet skal brukes til å utvikle og vedlikeholde en database over nasjonens kritiske infrastruktur. Denne databasen vil danne grunnlag for risikoanalyser og analyser av konsekvensen av bortfall av det aktuelle infrastrukturelementet. Andre oppgaver som disse midlene skal brukes til er en døgnkontinuerlig etterretnings og analysekapasitet, samt

at det skal arbeides med statlige og private aktører for å identifisere og prioritere beskyttelsestiltak rettet mot kritisk infrastruktur (9).

Direktoratet for vitenskap og teknologi, som har ansvaret for FoU aktivitet i tilknytning til IKT-sikkerhet, har i forslaget til budsjett for 2004 fått i alt 803 millioner USD til disposisjon. Av dette skal blant annet 90 mill brukes til å utvikle nye systemer for å bedre DHS sin mulighet til analyse av trusselinformasjon og sårbarheter (9).

C.3 Kritikk mot DHS og NCSD

Noe av kritikken går på organisasjonsmessige problemer i det å integrere 22 tidligere byråer til en organisasjon på over 170.000 ansatte og at man ved å fjerne stillingen som spesialrådgiver til presidenten i IKT-spørsmål, og legge denne stillingen under NCSD, gir inntrykk av at myndighetene ikke lenger prioriterer dette spørsmålet like høyt som tidligere. En toppleder i industrien og tidligere innehaver av stillingen som spesialrådgiver til presidenten i IKT-spørsmål, Richard Clarke, frykter at den nye lederen for NCSD rent organisatorisk vil være for lite knyttet til presidenten, og dermed få for lite makt. [101] Videre er enkelte redde for at DHS vil få problemer med å skaffe den rette personen for jobben. Når stillingen er så langt nede i hierarkiet, er det desto mer viktig at personen som innehar stillingen er en vel ansett og dyktig innen IKT-sikkerhet. [102] Den mangelen på autoritet, som enkelte i privat sektor ser at den nye stillingen vil ha, vil føre til at de best kvalifiserte søkerne til jobben ikke ønsker jobben. [103] Richard Clarke ser også rent organisasjonsmessige problemer i det å integrere 22 tidligere byråer til en organisasjon på over 170000 ansatte. Clarke mener det vil ta flere år før de ulike organisasjonskulturene blir sveiset sammen til en kultur og den nye organisasjonen effektivt kan arbeide med de tiltenkte oppgavene. [104]

[101] http://www.ds-osac.org/view.cfm?KEY=7E44504A4154&type=2B170C1E0A3A0F162820, http://www.computerweekly.com/articles/article.asp?liArticleID=122444&liFlavourID=1&sp=1
[102] http://www.infosecuritymag.com/2003/jun/digest09.shtml#news3
[103] http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,83242,00.html
[104] http://www.nwfusion.com/news/2003/0709helpyours.html

D NÆRMERE BESKRIVELSE AV ARBEIDET I AUSTRALIA

D.1 Regjeringens IKT-strategi fra 1999

Basert på anbefalingene fra IDC, foreslo Regjeringen en fempunktstrategi for IKT-sikkerhet:

1. Bygge opp et industriforum for beskyttelse av kritisk infrastruktur, der både myndighetene og de private infrastruktureierne er representert. Ett av hovedpoengene er at myndighetene er brukere, men at infrastrukturen eies av private. Dette punktet er derfor strategiens hovedpunkt. Man ønsker også at arbeidet med beskyttelse av NII skal ha svakt innslag av lovregulering, men i stedet øke bevisstheten blant aktørene. Myndighetenes rolle skal i særlig grad være å bistå med teknisk ekspertise.

2. Myndighetene ønsker å integrere beskyttelse av informasjonsinfrastrukturen med arbeidet som gjøres innen annen infrastrukturbeskyttelse da fysisk sikrings- og responskapasiteter allerede finnes.

3. Man vil bygge opp en responskapasitet mot angrep på privat sektor forbedre responskapasiteten som finnes for staten. I tillegg ønsker man en samkjøring av de to sektorene. AusCERT og DSD står sentralt i dette arbeidet.

4. I tillegg til ren responskapasitet mot elektroniske angrep, ønsker man også å lage en database der hendelser rapporteres, slik at det kan lages trussel og sårbarhetsvurderinger basert på et bredt datautvalg.

Det siste punktet er å endre myndighetenes strategi slik at den hele tiden samsvarer med teknologisk utvikling og endret trusselbilde. Dette vil i praksis bety at administrative forhold må være under konstant vurdering og eventuell revisjon. For eksempel kan det nevnes at AFP har opprettet en døgnbemannet "hot-line" i samarbeid med G8-landene for å kunne etterforske nettkriminalitet.

D.2 Litt bakgrunn om utbygging av teleinfrastruktur i Australia

Australia har store områder der befolkningsgrunnlaget ikke er stort nok til å drive kommersielt, og det er derfor nødvendig med øremerkede midler.[105] Mer enn 3,8 milliard norske[106] kroner har blitt øremerket IKT-infrastruktur og tjenesteproduksjon i utkantstrøk etter telemonopolets fall. For eksempel har det blitt bevilget 340 millioner NOK[107] til utbygging av bank og transaksjonsnettverk på landet. Statens overføringer til utbygging av telenettet stammer i hovedsak fra salg av andeler i Telstra, den tidligere statsmonopolisten.

[105] "Australian Telecommunication 2002": http://www.dcita.gov.au/download/0,6183,4_112190,00.pdf
[106] En milliard australske dollar
[107] 70 millioner AUD

En faktor som i følge det australske konkurransetilsynet[108] er med på å dempe utbyggingen i grisgrendte strøk, er myndighetenes priskontroll på Telstra. Som tidligere monopolist eier Telstra svært mye av infrastrukturen, og er pålagt å leie denne videre til strengt regulerte priser. Ettersom disse prisene ikke gjenspeiler kostnadene ved nyinvestering i mindre trafikkerte områder, taper Telstra på å bygge ut. Man lar dermed være å bygge ut.

En høringsrapport[109] som ble levert i 2002, slo fast at reparasjonskapasitet og telefon- og internettinfrastrukturen var for dårlig, særlig på landsbygda. Derfor ble tidskravet for installering av fasttelefon skjerpet fra ett år til et halvt år for privatpersoner, og til 30 dager for bedrifter. Kravet til oppretting av feil ble satt til fem dager for bedriftskunder. Det ble også vedtatt at byer med mer enn 500 mennesker skulle ha mobildekning, og at de uten mobildekning skulle få tilbud om subsidiert satelittelefon. Alle disse tiltakene har positiv effekt i et beredskapsperspektiv, men det er krav om tilgang på datanettverk og mobildekning som ligger bak.

D.3 Standarder for teleindustrien

Australian communicatons industry forum (ACIF)[110] lager koder og standarder for den australske telekommunikasjonsindustrien, som det er frivillig å følge i mangle på regulering.[111] Med henblikk på sikkerhet har man bare jobbet innenfor personvern og tilgang på informasjon. De relevante industrikodene er:

ACIF C523:1999, Protection of Personal Information of Customers of Telecommunications providers
ACIF 537:2003, Provision of Assistance to National Security, Enforcement and Government Agencies

Sistnevnte tar særlig for seg hvordan teleoperatørene skal forholde seg i forhold til personvern og det å gi opplysninger til myndighetene. Den tar for eksempel konkret for seg rapporteringsplikten til AISO, som er nedfelt i Telecommunications act 1997.[112]

D.4 Utdypende informasjon om noen av organisasjonene som arbeider innen IKT-sikkerhet

Justisdepartementet og organisasjonene under
Det er Justisdepartementet som har det overordnede ansvaret for arbeidet med sikkerhet og

[108] Australian Competition and Consumer commission (ACCC)
[109] Regional Telecommunications Inquiry (RIT)
[110] http://www.acif.org.au/ACIF/index.cfm?requesttimeout=300
[111] På side 6: http://www.ddsi.org/Documents/final%20docs/DDSI_Country_Reports_Final_Australia.pdf
[112] Ref.: ACIF C537:2003 (finnes under nettsidene til ACIF).

beskyttelse av kritisk infrastruktur i Australia, og har ansvaret for[113]

- å gi administrativ støtte til the Critical Infrastructure Protection Group (CIPG)
- å ha en koordinerende rolle som sikrer at beskyttelsen av nasjonal informasjonsinfrastruktur (NII) gjøres på en strukturert og kvalitetssikret måte, i henhold til the Commonwealth's policy.
- koordinere utviklingen av NII policy, spesielt med hensyn på revisjon av lovverket og i forbindelse med kriminalitetsbekjempelse
- ha ansvaret for prosjekter som jobber med beskyttelse av kritisk infrastruktur beskyttelse
- arbeide med NOIE for å skape kontakter med industrien
- utvikle krisehåndtering som kan takle angrep på NII
- koordinere Australias deltakelse i internasjonalt NII-beskyttelsessamarbeid

Videre har Justisdepartementet, gjennom Protective Security Coordination Centre (PSCC), hovedansvar for å:[114]

- utvikle, vedlikeholde og koordinere Australias nasjonale anti-terror kapasiteter,
- koordinere Australias nasjonale krisehåndteringssystemer i tilfelle trusler om terrorisme eller utførelse av terror
- koordinere beskyttelsen av viktige personer, slik som diplomater og regjeringsmedlemmer
- utvikle og promotere en sikkerhetspolicy, herunder gi råd og lage felles standarder for sikring
- gi opplæring/kurs/seminarer av Commonwealth personell innen sikkerhet, slik som fysisk sikring, personellsikring, datasikkerhet, anti-terror etc[115]

---

[113] http://www.austlii.edu.au/au/other/CyberLRes/2001/17/
[114] http://www.sac-pav.gov.au/www/agdHome.nsf/HeadingPagesDisplay/Security+Coordination?OpenDocument
[115] "Security in government", se link:
http://www.ag.gov.au/www/protectivesecurityHome.nsf/HeadingPagesDisplay/Security+In+Government?OpenDoc
ument
[116] http://www.ag.gov.au/www/pscctraininghome.nsf
[117] http://www.sac-pav.gov.au/www/protectivesecurityhome.nsf
[118] http://www.asio.gov.au/Default.htm
[119] 64 millioner AUD

- administrere sikkerhetsklarering av personell og
- gi assistanse til Justisministeren[116]

PSCC har også det faglige hovedansvaret for the Protective Security Manual (PSM), som gis ut av Justisdepartementet.[117] PSM inneholder prosedyrer, prinsipper og standarder i henhold til myndighetenes sikkerhetspolicy og er ment som en manual for alle myndighetsinstanser. Manualen er i kontinuerlig forandring ettersom teknologien skrider frem, men har nylig vært gjennom en stor revisjon. Svært mange etater har vært involvert i revideringen gjennom the Protective Security Policy Committee (PSPC).

Hovedpunktene i PSM er

- myndighetenes policy
- retningslinjer for håndtering av sikkerhetsrisiko
- informasjonssikkerhet (mye av dette er utarbeidet av DSD)
- personellsikkerhet (med vekt på standarder for sikkerhetsklarering av ansatte)
- fysisk sikring (omfattende beskrivelse av beskyttelse av infrastruktur, informasjon, personale etc)
- sikkerhetsrammeverk i forhold til outsourcing, slik at private firmaer, som gjør oppdrag for myndighetene, holder samme sikkerhetsprofil som oppdragsgiverne (mye av dette er uarbeidet av Department of Finance and Administration)
- retningslinjer for sikkerhetsrelaterte hendelser og påfølgende etterforskning og rapportering
- retningslinjer for hjemmebasert jobb (hjemmekontor)

Den nye utgaven av PSM er ikke begrenset, men er heller ikke være tilgjenglig for distribusjon utenfor myndighetsorganer og bedrifter som arbeider for myndighetene.

AISO og AFP
Både AFP og AISO er underlagt Justisdepartementet. ASIOs (The Australian Security Information Organisation) hovedrolle er å beskytte Australia mot aktører som kan true landets suverenitet.[118] AISO har ingen befatning med hverdagskriminalitet, men kan arbeide mot organisert kriminalitet av slik orden at den er en trussel mot nasjonen. AISO gir råd til myndighetsorganer, og kan bistå slike med å gjennomføre risikoanalyser og finne kosteffektive mottiltak.

AISO arbeider meget med fysisk sikring, og har store fasiliteter for å teste ut sikkerhetsprodukter. De gir også ut en katalog med slike, men den er gradert begrenset. I tillegg kan de sikkerhetsklarere personell, og har kompetanse på å gjøre trussel og sårbarhetsvurderinger. Årlig budsjett for AISO lå på 309 millioner NOK[119] i skatteåret 2000/2001.

De lager også trusselvurderinger med jevne mellomrom, som blant annet PSCC og APS benytter

i sitt arbeide.[120] De fikk i 1999 lov til å hacke for å drive elektronisk overvåkning. Dette har vært kritisert.[121]

AFP (Australian Federal Police) har ansvar for politioppgaver, og derfor også ett ansvar innen IKT sikkerhet. AFP har et hendelsesrapporteringssystem på kritisk infrastruktur, lokalisert ved hovedkvarteret i Canberra.

Australian Protective Service[122] (APS) er en politienhet som jobber under det føderale politiet. De driver politioppgaver, men er meget rettet mot sikkerhet og beskyttelse. For eksempel har de ansvar for sikkerhet rundt atomkraftverk og viktige personer, som for eksempel politikere.

DSD

Det er Defence Signals Directorate (DSD) som er ansvarlig for The Commonwealths online sikkerhetsretningslinjer og teknisk politikk. DSD har en rekke programmer som involverer IKT-sikkerhet, og de viktigste er gjengitt nedenfor:

DSD er ansvarlig for utgivelse og oppdatering av en serie sikkerhetsinstruksjoner, ACSI (Australian Communications-Electronic security Instructions). Den viktigste i denne sammenhengen er ACSI 33,[123] som alle myndighetsinstanser er pliktet til å følge.[124] Bakgrunnen for dette er at man gjennom PSM er pålagt å vurdere sikkerhet knyttet til elektroniske informasjonssystemer, selv på de systemene som ikke er graderte.[125]

ACSI er på et teknisk nivå, og er rettet direkte mot sikkerhetspersonal og IT/drift. ACSI er en serie av håndbøker som dekker hver sine områder innen IT-sikkerhet. ACSI holder seg til de nasjonale standardene for sikkerhet, som for eksempel de utgitt av Standards Australia.[126] De relevante standarder i denne sammenheng er:

- AS/NZS 4360:1999: Risk management [127]
- AS/NZS 4444.2:200 : Information security management - Specification for information security management systems (Redesignated as AS/NZS 7799.2:2000 on 15 August

[120] Referanse: http://www.asio.gov.au/Work/comp.htm
[121] http://www.ddsi.org/Documents/final%20docs/DDSI_Country_Reports_Final_Australia.pdf
[122] For mer informasjon se link: http://www.aps.gov.au/docs/whoweare.htm#place

[123] http://www.dsd.gov.au/infosec/acsi33/acsi_index.html
[124] referanse: http://www.govonline.gov.au/projects/confidence/index.htm
[125] referanse: http://www.dsd.gov.au/infosec/acsi33/Intro.html
[126] Standards Australia er et "konsulentfirma" som lager standarder og som kan godkjenne i forhold til andres standarder, som for eksempel ISO. De er eget selskap, men får rundt 2,5 % av inntektene fra The Commonwealth, og har ingen krav til avkastning (intet utbytte). De har laget to relevante standarder, se for eksempel: http://www.standards.com.au/catalogue/Script/search.asp
[127] Link til der man kan kjøpe den. Fins blant annet innholdsfortegnelse med mer: http://www.standards.com.au/catalogue/script/details.asp?DocN=stds000023835

2001)[128]

DSD skal etter Cabinet Directive, gi bistand og assistanse (sikkerhetsmessig) til Commonwealths myndighetsinstanser der hvor det fins data som kan være gradert. DSD skal også bistå der hvor det gjelder ikke-gradret materiale, men der hvor man ikke ønsker uautorisert bekjentgjøring.

I den forbindelse har DSD et program for sertifisering av internettløsningene til myndighetene. For eksempel der hvor to byråer må utveksle informasjon via internett, kan DSD gi sertifisering gjennom deres program "Public Network Gateway Certification". Det finnes ulike sertifiseringsnivåer, avhengig av konfidensialiteten av den informasjon som skal utveksles.

DSD er ansvarlig også for rådgivning innen kryptering og nøkkelhåndtering. De har for eksempel laget en egen liste over produkter som DSD mener oppfyller spesifikke krav til sikkerhet, og har utgitt en oversikt gjennom "DSD's Evaluated product list" (ELP).[129] [130] Videre har de laget to Guidelines: ACSI 53 og ACSI 57, som er håndbøker for håndtering av kryptografi. DSD er også faginstans i NOIEs PKI-strategi.[131]

ISIDRAS (Information Security Incident Ready Reckoner)[132] er et system som håndteres av DSD, og der myndighetsorganene oppfordres til å rapportere inn sikkerhetsbrudd av ulike slag. Dette for å lage statistisk data for å lettere kunne gi råd og for å kunne gi en trusselvurdering. ISIDRAS har en slags CERT-funksjon for myndighetinstanser.

NCTC

The National Counter-Terrorism Committee (NCTC) ble dannet i 2002.[133] En av de viktigste oppgavene i tiden fremover vil være å komme opp med en Nasjonal Strategi for beskyttelse av kritisk infrastruktur innen 2003.[134] NCTC har utarbeidet en anti-terrorplan.[135]

---

[128] http://www.standards.com.au/catalogue/Script/details.asp?DocN=AS355047432596

[129] http://www.dsd.gov.au/infosec/aisep/EPL.html

[130] I Australia evalueres produkter i henhold til Australian Information Security Evaluation programme. Før 1995 ble all informasjonssikkerhet evaluert av DSD, da de hadde rolle som National Computer Security Advisory Authority. Da behovet for evalueringer steg, ble Australian Information Security Evaluation Programme (AISEP), dannet i 1995. Under programmet fins uavhengige selskaper, AISEF (Australian Information Security Evaluation Facilities), som har fått lisens fra DSD (en slags akkreditering der firmaene må vise til kvalitetssikring etc). Disse selskapene (AISEF) foretar evaluering av produkter i henhold til the Common Crtieria eller ITSEC (IT Security Evaluation Criteria). Deretter blir evalueringen gjennomgått av DSD og godkjent (tror at siste gjennomgang av DSD er for å sjekke at det er kvalitetssikret). Et av de største poengene med EPL-programmet er, for uten at man kan avdekke sikkerhetshull.

[131] Foredrag om PKI, som skal holdes på 2003 Security in Government – konferansen: http://www.ag.gov.au/www/rwpattach.nsf/viewasattachmentPersonal/ABC8FD820EDA6AB1CA256D21001FCD86/$file/Secure%20Email.pdf

[132] http://www.dsd.gov.au/infosec/pdfdocs/incident_ready_reckoner.pdf

[133] NCTC har overtatt etter SAC-PAV (Standing Committee on Commonwealth/ State Cooperation for Protection against Violence) som ble etablert i 1979 etter Hilton-bombingen. NCTC har utvidet ansvarsområde i forhold til SAC-PAV.

[134] http://www.cript.gov.au/www/rwpattach.nsf/viewasattachmentPersonal/C0270F5DDC451CD7CA256CF6007C9965/$file/NCTC%20CIP%20in%20Australia.pdf

[135] http://www.nationalsecurity.gov.au/www/nationalsecurityhome.nsf/AllDocs/RWPCD8501294925DA06CA256D42001C1A4C?OpenDocument

E EN DETALJERT GJENNOMGANG AV TILTAKENE I DEN AMERIKANSKE STRATEGIEN

Nedenfor gis en detaljert gjennomgang av tiltakene i den amerikanske strategien. Tiltakene er sortert på de fem fokusområdene, og så langt rammene for denne studien har tillatt det er tiltakenes status oppgitt.

E.1 Fokusområde: Et nasjonalt reaksjonssystem for IKT-sikkerhet

Under dette fokusområdet foreslår strategien i alt 7 ulike tiltak. Disse tiltakene er alle rettet inn mot opprettelsen av et nasjonalt reaksjonssystem for IKT-sikkerhet. Dette systemet vil være et offentlig-privat samarbeide bestående av statlige og ikke-statlige organer, som for eksempel private informasjonsdelings- og analysesentre (ISAC). Systemet skal bedre mulighetene for analyse av trusler og sårbarheter inne kritiske IKT-systemer, forbedre arbeidet med kontinuitet i offentlig og privat kritisk infrastruktur, samt bedre informasjonsdelingen mellom ulike aktører slik at den samlede IKT-sikkerheten blir forbedret (8).

Slik strategiene er formulert ser man ikke for seg at etableringen av dette systemet skal behøve å føre til nye byråkratiske programmer. I stedet ser man for seg at opprettelsen av DHS og samlingen av ulike føderale byråer og organisasjoner under det nye Direktoratet for informasjonsanalyse og beskyttelse av infrastruktur vil gi de nødvendige synergier for å etablere dette systemet.

Følgende tiltak er anbefalt under dette fokusområdet (8):

- DHS skal opprette et kontaktpunkt for de føderale myndighetenes samarbeide med industri og andre partnere, med døgnkontinuerlig aktivitet. Dette skal muliggjøre analyse av kritiske IKT-systemer, varsling og informasjonsdeling, mulighet for å reagere i forhold til alvorlige hendelser samt en bedret reetableringsinnsats på nasjonalt nivå. Private organisasjoner, med bidrag innen disse funksjonene, oppfordres til å koordinere sine aktiviteter slik at man får et best mulig kontinuerlig oversikt over tilstanden til kritiske IKT-systemer (A/R 1-1).
- De føderale myndighetene skal i tråd med budsjettet for 2003 ferdigstille installeringen av et sikkert nettverk for å formidle analyser og varslingsinformasjon, samt foreta krisehåndtering. Nettverket kalles CWIN (Cyber Warning and Information Network) (A/R 1-2).
- For å evaluere ulike byråers sikkerhetstenkning og beredskapsplaner, vil DHS gjennomføre ulike øvelser for å anslå betydningen av IKT-relaterte angrep på statlige arbeidsrutiner. Avdekkede svakheter vil bli inkludert i de respektive byråenes forbedringsplaner og oversendt Office of Management and Budget (OMB) (A/R 1-3).
- Bedrifter oppfordres til jevnlig å gjennomgå og utarbeide beredskapsplaner for IKT-systemer i organisasjonen. Videre oppfordres bedrifter til å se på mulighetene for å

benytte flere leverandører av IKT-tjenester som et middel for å redusere risikoen (A/R 1-4).

- Sektorer med ansvar for infrastruktur oppfores til å etablere gjensidige bistandsprogrammer i tilfelle IKT-relaterte kriser skulle oppstå. Justisdepartementet og den føderale handelskommisjonen vil samarbeide med disse sektorene for å fjerne eventuelle barrierer for et slikt samarbeid, hvor det er mulig. I tillegg skal DHS gjennom Direktoratet for informasjonsanalyse og beskyttelse av infrastruktur koordinere utarbeidelsen og den regelmessige oppdateringen av frivillige beredskapsplaner for IKT-systemer som et felles samarbeid mellom myndighetene og industrien (A/R 1-5).
- DHS skal øke bevisstheten knyttet til fjerning av hindre for informasjonsdeling knyttet til IKT-sikkerhet og sårbarhet i infrastruktur mellom statlig og privat sektor. Departementet skal også opprette et programkontor for beskyttelse av infrastruktur, som vil få i oppgave å administrere informasjonsflyten, herunder utarbeidelsen av rutiner for hvordan frivillig rapportert informasjon knyttet til kritisk infrastruktur skal behandles (A/R 1-6).
- Bedrifter oppfordres til å vurdere et aktivt engasjement i sektorvise informasjonsdelingsprogrammer knyttet til IKT-sikkerhet, herunder de mulige fordelene ved å knytte seg til en relevant ISAC. Høyskoler og universiteter oppfordres til å etablere; (1) en eller flere ISACer for å håndtere angrep mot og sårbarheter i IKT-systemer, og (2) et kontaktpunkt for ISPer og politiet til bruk hvis skolenes IKT-systemer blir benyttet til angrep på andre IKT-systemer (A/R 1-7).

Tiltakene over er i varierende grad gjennomført. Det er imidlertid vanskelig å presentere en full oversikt over status for de ulike tiltakene, da det per nå ikke eksisterer en slik oversikt fra myndighetenes side. Enkelte av tiltakene er imidlertid gjennomført. Den 6 juni annonsert statsråd Tom Ridge at DHS etablerer en ” National Cyber Security Division” (NCSD) med i alt 60 ansatte. [136] Denne gruppen vil være en viktig bidragsyter i gjennomføringen av den nasjonale strategien for IKT-sikkerhet[137] [138], og vil få ansvaret for å gjennomføringen av flere av tiltakene i strategien.

E.2 Fokusområde: Et nasjonalt program for å redusere IKT relaterte trusler og sårbarheter

Trusler mot IKT-systemer kommer i dag fra mange ulike hold og gjøre seg nytte av mange ulike teknologier. Dette gjøre det umulig å sette som målsetning for strategien å fjerne alle sårbarheter eller trusler mot IKT-systemer. Den amerikanske nasjonale strategien for IKT-sikkerhet setter derfor tre ulike delmål for dette fokusområdet. Disse delmålene presenteres under (8):

- Redusere trusler og motarbeide ondsinnede aktører gjennom effektive tiltak for å identifisere og straffe slike aktører.

[136] Pressemelding fra DHS 6 juni 2003, se http://www.dhs.gov/dhspublic/display?theme=31&content=915
[137] The National Strategy to Secure Cyberspace
[138] A/R 1-1 må anses som gjennomført ved opprettelsen av NCSD

- Identifisere og minimere de gjenværende sårbarhetene som kan skape de største konsekvensen for kritisk infrastruktur dersom de blir utnyttet
- Utvikle nye systemer med færre sårbarheter samt vurdere nye teknologi for sårbarhetsredusering

For å lykkes med disse målsetningen påpekes det igjen i strategien at dette ikke er et arbeid de føderale myndighetene kan gjøre på egen hånd, men at det krever et aktivt samarbeid mellom føderale, statlige og lokale myndigheter og private aktører. Hovedansvaret for gjennomføringen av dette fokusområdet ligger hos DHS (8). Strategien identifiserer i alt 15 ulike tiltak som skal gjøre det enklere å nå disse tre delmålene. Under gjengis disse tiltakene i sin helhet:

- Justisdepartementet og andre egnede byråer skal utvikle og implementere strategier for å redusere IKT-angrep og trusler mot IKT-systemer ved bruk av følgende virkemidler;
    - Identifisere ulike måter for å bedre informasjonsdeling og koordinering av etterforskningsinnsats inne føderale, statlige og lokale politimyndigheter som arbeider med kritisk infrastruktur og IKT-relaterte sikkerhetsspørsmål, og mellom andre byråer og privat sektor,
    - Vurdere ulike måter for å kunne tilby tilfredsstillende etterforskningsressurser og trening for å kunne gjennomføre en hurtig etterforskning og oppklaring av saker relatert til kritisk infrastruktur,
    - Utarbeide bedre data knyttet til IKT-kriminalitet og innbrudd for å bedre forstå omfanget av problemet og bedre kunne spore endringer over tid (A/R 2-1).
- DHS skal i samarbeid med relevante byråer og privat sektor lede utviklingen av en nasjonal trusselvurderingskapasitet som gjør bruk av red team/blue team og andre metoder for å identifisere innvirkningen av mulige angrep på ulike typer mål (A/R 2-2).
- Handelsdepartementet skal nedsette en arbeidsgruppe for å vurdere ulike aspekter ved IPv6, herunder hvilken rolle myndighetene skal ha, internasjonal interoperabilitet, sikkerhet ved overgang til ny standard, samt vurderinger av kostnader og nytte. Arbeidsgruppen skal få innspill fra berørte sektorer (A/R 2-3).
- DHS skal i samarbeid med Handelsdepartementet og andre relevante byråer koordinere et offentlig/privat samarbeid som skal oppfordre til;
    - økt bruk av forbedrede sikkerhetsprotokoller,
    - utviklingen av sikrere ruterteknologi,
    - at ISPer tar i bruk ”regler for god forretningsskikk”, herunder metoder for IKT-sikkerhet og samarbeid knyttet til sikkerhet. DHS vil gi disse tiltakene nødvendig støtte for at de skal lykkes, gitt det til en hver tid gjeldende budsjett for departementet (A/R 2-4).
- DHS skal sammen med Energidepartementet og andre berørte byråer og i samarbeid med industrien utarbeide en ”bestepraksis” og nye teknologier for å bedre sikkerheten i prosesstyringssystemer (DCS/SCADA), identifisere de mest kritiske prosesstyringssystemene og utarbeide en prioritert plan for å bedre IKT-sikkerheten i disse systemene på kort sikt (A/R 2-5).

- DHS skal i samarbeid med det nasjonale rådgivningsorganet for infrastruktur (NIAC) og organisasjoner i privat sektor utvikle mekanismer og metoder for å avsløre sårbarheter (A/R 2-6).
- US General Services Administration (GSA) skal sammen med DHS arbeide for å etablere en garantiinstitusjon for programpatcher for de føderale myndighetene. DHS skal også dele erfaringer fra dette arbeidet med privat sektor og oppfordre til opprettelsen av en tilsvarende frivillig garantiinstitusjon for andre sektorer og store selskaper (A/R 2-7).
- Programvareindustrien oppfordres til å implementere sikrere standardinstallasjoner og implementeringer av industriens produkter, inkludert økt fokus på;
    - brukerbevissthet knyttet til sikkerhetskomponenter i produktene,
    - brukervennelighet i sikkerhetsfunksjonaliteten,
    - dersom mulig, støtte opp om utarbeidelsen av retningslinjer og ”bestepraksis” for bedre å kunne gjennomføre slike tiltak (A/R 2-8).
- DHS skal etablere og lede et offentlig/privat samarbeid for å identifisere tverrsektorielle avhengigheter både når det gjelder fysisk infrastruktur og IKT-infrastruktur. Dette samarbeidet skal lede frem til en plan for å redusere disse avhengighetene i samsvar med tiltak foreslått i ”the National Strategy for Homeland Security”. Det nasjonale infrastruktur simulerings og analysesentret under DHS skal støtte opp om dette arbeidet ved å utvikle modeller for å identifisere virkningen av slike avhengigheter (A/R 2-9).
- Når DHS blir anmodet og finner dette hensiktsmessige, vil de støtte frivillige innsats fra eiere og operatører av IKT-systemer for å utvikle reetablerings- og beredskapsplaner for å redusere konsekvensene av store fysiske ødeleggelser på anlegg som støtter slike systemer, og for å utvikle passende prosedyrer for å begrense tilgangen til kritiske anlegg (A/R 2-10).
- Direktøren for ”the Office of Science and Technology Policy” (OSTP) skal koordinere utviklingen av en FoU plan på IKT-sikkerhet for de føderale myndigheten. Planen skal oppdateres årlig og inneholde prosjektprioriteringer på kort sikt (1-3 år), mellomlang sikt (3-5 år) og lang sikt (lengre enn 5 år). Eksisterende prioriteter er blant annet inntregningsdeteksjonssystemer, sikkerhet i Internetts infrastruktur, applikasjonssikkerhet, DoS, kommunikasjonssikkerhet, høysikkerhetssystemer og sikker systemsammensetning (A/R 2-11).
- For å optimalisere FoU aktiviteten i forhold til privat sektor skal DHS påses at nødvendige mekanismer for koordinering av FoU aktivitet mellom akademia, industri og myndigheter etableres (A/R 2-12).
- Privat sektor oppfordres til å fokusere noe av den kortsiktige FoU aktivitetene rundt utviklingen av operativsystemer med høy sikkerhet og pålitelighet. Dersom slike systemer blir utviklet og tilfredsstillende evaluert, vil de føderale myndighetene, gitt nødvendig budsjettdekning, fremskynde anskaffelsen av slike systemer (A/R 2-13).
- DHS vil støtte et offentlig/privat samarbeid for å kunngjøre ”beste praksis” og metoder som støtter integritet, sikkerhet og pålitelighet i uvikling av programvare, herunder prosesser og prosedyrer som minimere muligheten for feilaktig kode, ondsinnet kode eller bakdører som kan bli innført under utviklingen (A/R 2-14).
- DHS skal i samarbeid med OSTP og andre relevante byråer muliggjøre nødvendig kommunikasjon mellom det offentlige og private forsknings- og sikkerhetsmiljøer, slik at ny

teknologi med jevn mellomrom blir gjennomgått av en relevant gruppe innen "the National Science and Technology Council" (NSTC) for å vurdere denne teknologiens relevans i forhold til nasjonal kritisk IKT-sikkerhet og i forhold til den føderale FoU planen (A/R 2-15).

Som nevnt over finnes det ikke en oversikt over hvor langt man har kommet i gjennomføringen av de ulike tiltakene. Dette gjør det vanskelig å si noe om statusen for tiltakene under dette fokusområdet. Enkelte tiltak er imidlertid fullført også under dette fokusområdet. Et eksempel på dette er garantiinstitusjonen, "Patch Authentication and Dissemination Capability" (PADC), for programvarepatcher som er opprettet av "Federal Computer Incident Response Center" (FedCIRC). [139]

E.3 Fokusområde: Et nasjonalt bevisstgjørings- og utdanningsprogram innen IKT-sikkerhet

For å være i stand til å skape sikre IKT-systmer er man avhengig av at de personene som utvikler og benytter systemene har en forståelse for hva IKT-sikkerhet innebærer og hva de selv kan gjøre for å skape et så sikkert system som mulig. For å skape større forståelse for hva IKT-sikkerhet innebærer, forslår den amerikanske nasjonale strategien for IKT-sikkerhet i alt 9 ulike tiltak under dette fokusområdet. Strategien identifiserer også fire delmål for dette fokusområdet. Disse delmålene er (8):

- Utvikle et omfattende nasjonalt bevisstgjøringsprogram for å gjøre alle amerikanere, bedrifter, arbeidere og befolkningen generelt, i stand til å sikre sine egne IKT-systemer.
- Støtte hensiktsmessige opplærings- og utdanningsprogrammer for å støtte opp om nasjonens kunnskapsbehov knyttet til IKT-sikkerhet.
- Øke effektiviteten i eksisterende føderale opplæringsprogrammer for IKT-sikkerhet.
- Støtte godt koordinerte og anerkjente private sertifiseringsmyndigheter innen IKT-sikkerhet.

Hovedansvaret for gjennomføringen av dette fokusområdet ligger hos DHS, og den nylig opprettede NCSD[140] vil få en sentral rolle i dette arbeidet. For å nå målsetningene under dette fokusområdet identifiserer strategien følgende tiltak (8):

- DHS skal i samarbeid med relevante føderale, statlige og lokale organisasjoner og privat sektor utarbeide en omfattende bevisstgjøringskampanje med materiale tilpasset ulike grupper tilhørere. Videre skal "Surf Sikker" (StaySafeOnline) kampanjen utvides, og det skal etableres en pris for de selskapene som er med på å gi et stort bidrag til IKT-

[139] Se http://padc.fedcirc.gov for mer informasjon om denne tjenesten. Et informasjonsdokument om tjenesten er tilgjengelig på http://padc.fedcirc.gov/images/PADC_slipsheet.pdf
[140] NSCD ble opprettet i juni 2003. Se pressemelding fra DHS på http://www.dhs.gov/dhspublic/display?theme=31&content=915 for mer informasjon om denne enheten

sikkerhet (A/R 3-1).

- DHS vil i samarbeide med Utdanningsdepartementet oppfordre til og støtte, gitt nødvendig budsjettdekning, statlige, lokale og private organisasjoner i utarbeidelsen av utdanningsprogrammer og retningslinjer knyttet til IKT-sikkerhet for elever i grunnskole og videregående skole (A/R 3-2).
- Hjemmebrukere og små bedrifter kan hjelpe til å sikre nasjonens kritiske IKT-infrastruktur ved å sikre sine egen tilgang til Internett. Installasjon av softwarebaserte brannmurer, oppdatering av slik programvare, oppdatering av antivirusprogramvare og oppdatering av operativsystemer og andre applikasjoner med nye sikkerhetsoppdateringer er eksempler på handlinger privatpersoner og IT ansvarlige i små selskaper kan gjøre for å være med på sikre kritisk IKT-infrastruktur. For å støtte opp om dette vil DHS opprette en offentlig/privat arbeidsgruppe med private bedrifter, organisasjoner og konsumenter for å identifisere måter leverandører av IKT-produkter og tjenester, og andre organisasjoner, kan gjøre det enklere for hjemmebrukere og små bedrifter å sikre sine egen IKT-systemer (A/R 3-3).
- Store selskaper oppfordres til å evaluere sikkerheten i sine egne IKT-systmer, som kan påvirke sikkerheten i nasjonal kritisk infrastruktur. En slik evaluering kan inkludere;
    - gjennomføre revisjoner for å forsikre seg om effektivitet og bruk av ”bestepraksis”,
    - utarbeide driftsplaner som tar høyde for eksternt personell og utstyr,
    - deltakelse i informasjonsdeling og utbredelse av ”bestepraksis” inne bransjen (A/R 3-4).
- Høyskoler og universiteter oppfordres til sikre sine egne IKT-systemer ved å iverksette et eller flere av følgende tiltak hvor dette er relevant;
    - Etablere en eller flere ISAC for å håndtere angrep mot og sårbarheter i IKT-systemer,
    - Utarbeide gode retningslinjer som gir informasjonssjefen nødvendig handlingsrom,
    - Utarbeide et eller flere sett med ”bestepraksis” for IKT-sikkerhet,
    - Utarbeide programmer og materiale for å bedre brukerbevisstheten når det gjelder IKT-sikkerhet (A/R 3-5).
- Et offentlig/privat samarbeid bør fortsette arbeidet med å hjelpe til med å sikre nasjonal kritisk IKT-infrastruktur gjennom deltakelse i en teknologi og FoU avviksanalyse som vil gi innspill til den føderale FoU planen innen området IKT-sikkerhet. Videre bør man koordinere fremdriften i annen relevant forskning og utarbeide og offentliggjøre ”bestepraksis” for IKT-sikkerhet (A/R 3-6).
- DHS vil implementere og oppmuntre til etableringen av ulike typer utdanningsprogrammer for å styrke den faglige kompetansen hos IKT-sikkerhetspersonell i USA. Dette skal koordineres med NSF, OPM og NSA for å påvirke eksisterende programmer innen dette området for på best mulig måte å kunne håndtere disse viktige utdannings og opplæringstemaene (A/R 3-7).
- DHS skal i samarbeid med andre byråer med ansvar for IKT-sikkerhetsopplæring, utarbeide en koordineringsmekanisme for å kople sammen føderale

utdanningsprogrammer innen IKT-sikkerhet og IKT-etterforskning (A/R 3-8).

- DHS vil oppfordre til tiltak som er nødvendige for å bygge det nødvendige fundamentet for utviklingen av et program for sikkerhetssertifisering som er bredt akseptert i offentlig og privat sektor. DHS og andre føderale myndigheter kan støtte en slik prosess ved å gi uttrykk for de behov de føderale IKT-sikkerhetsansvarlige har (A/R 3-9).

E.4 Fokusområde: Sikre statlige IKT-systemer

De offentlige myndigheter driver en rekke tjenester som er kritiske for at samfunnet skal fungere tilfredsstillende. Gitt de senere års endringer i bruk av IKT i privat sektor er det også naturlig at de offentlige tjenestene blir stadig mer avhengig av IKT i den daglige driften. Dette gjør seg blant annet gjeldende i et stadig sterkere fokus på å gjøre offentlige tjenester tilgjengelige på Internett. [141] Denne sterkere fokuseringen på IKT gjør også at man i stadig økende grad må fokusere på sikkerhet i disse systemene. Dette er i overensstemmelse med den amerikanske nasjonale strategiene for IKT-sikkerhet, som har identifisert i alt 6 ulike tiltak under dette fokusområdet. Et annet viktig moment ved å øke fokus på sikkert i offentlige IKT-systemer er at myndighetene på den måten kan gå foran som et godt eksempel på hvordan IKT-sikkerhet skal praktiseres. Dette vil være med på å øke fokus knyttet til dette området og kan samtidig gi verdifull erfaring for den private sektoren. For å styrke IKT-sikkerheten i offentlige systemer identifiserer strategien følgende tiltak (8):

- Føderale byråer skal fortsette å øke bruken av automatiserte systemer for å evaluere sikkerheten i byråenes IKT-systemer. Videre skal man i større grad ta i bruk verktøy for å bedre sikkerhetsregimet i organisasjonen og verktøy for å stoppe angrep mot IKT-systemene. De føderale myndighetene vil vurdere hvorvidt det er nødvendig med ulike tiltak for å øke bruken av slike systemer (A/R 4-1).
- Gjennom det pågående eAutentiseringsprogrammet, vil de føderale myndighetene vurdere behovet for sterkere adgangskontroll og autentisering, samt vurdere hvorvidt alle departementer kan ta i bruk samme fysiske og logiske verktøy for adgangskontroll og autentiseringsmekanismer for derigjennom å øke interoperabiliteten (A/R 4-2).
- Føderale byråer bør vurdere å installere systemer for inntregningsdeteksjon. Byråenes strategier bør vurdere andre tiltak for å redusere risikoen, blant annet ved bruk av sterk kryptering, toveis autentisering, skjermingsstandarder og andre tekniske sikkerhetsvurderinger. I tillegg bør man ha et program for bevisstgjøring og opplæring knyttet til IKT-sikkerhet (A/R 4-3).
- De føderale myndigheten vil foreta en grundig gjennomgang av "the National Information Assurance Partnership" (NIAP) for å avgjøre hvorvidt dette programmet i tilfredsstillende grad adresserer problemet med sikkerhetsfeil i kommersiell programvare. Denne gjennomgangen vil inkludere erfaringer fra implementeringen av Forsvarsdepartementets strategi fra juli 2002, som forlanger at man anskaffer produkter som er evaluert av NIAP eller andre tilsvarende evalueringsprosesser (A/R 4-4).

[141] Mer informasjon om myndighetenes strategi for dette arbeidet finnes på http://www.whitehouse.gov/omb/egov/2003egov_strat.pdf

- De føderale myndighetene skal utrede hvorvidt private vaktselskaper som tilbyr tjenester til de føderale myndighetene skal sertifiseres for å møte bestemte minimumskriterier, blant annet hvorvidt disse selskapene er tilfredsstillende uavhengige (A/R 4-5).
- Statlige og lokale myndigheter oppfordres til å etablere IKT-sikkerhetsprogrammer for deres departementer og byråer, som inneholder momenter knyttet til bevisstgjøring, revisjoner og standarder. Statlige og lokale myndigheter oppfordres til å delte i etablerte ISACer (A/R 4-6).

E.5 Nasjonal sikkerhet og internasjonalt samarbeid om IKT-sikkerhet

Internett har gjort at geografiske grenser mellom land forsvinner. Det er ikke lenger nødvendig å befinnes seg fysisk i USA for å kunne skade amerikanske interesser. Dette har gjort at de amerikanske myndighetene har blitt svært opptatt av å beskytte nasjonens sikkerhet også på Internett. Internett er et verdensomspennende nettverk, noe som gjør at man også er helt avhengig av et godt internasjonalt samarbeid på dette området for å kunne motarbeide terrorister og andre som ønsker å ødelegge nasjonale kritiske IKT-systmer. Den nasjonale strategien foreslår i alt 10 tiltak for å bedre den nasjonale sikkerheten og øke det internasjonale samarbeidet om IKT-sikkerhet. Tiltakene er gjengitt nedenfor (8):

- FBI og etterretningsmiljøet skal påse at USA har en sterk kontra-etterretning for å motvirke innhenting av etterretningsinformasjon mot de amerikanske myndighetene, kommersielle organisasjoner eller utdanningsinstitusjoner. Dette arbeidet må inkludere opparbeidelsen av en dypere forståelse for eventuelle fienders evne og hensikt når det gjelder bruk av IKT-systemer for å innhente etterretningsinformasjon (A/R 5-1).
- Etterretningsmiljøet, Forsvarsdepartementet og politimyndighetene må forbedre nasjonens evne å raskt kunne identifisere kilden til angrep mot IKT-systmer for å kunne motarbeide slike angrep på en best mulig måte. I tråd med ”the National Security Strategy” vil disse anstrengelsene også forsøke å utvikle metoder for å forhindre at slike angrep i det hele tatt når kritiske systemer og infrastruktur (A/R 5-2).
- USA må forbedre samarbeidet mellom organisasjoner innen politiet, nasjonal sikkerhet og forsvaret som arbeider med IKT-relaterte problemer, for å påse at den rette organisasjonen får ansvaret for det aktuelle problemet. ”The National Security Council” (NSC) og OHS vil gjennomføre en studie for å påse at et slike samarbeide fungerer hensiktsmessig (A/R 5-3).
- Når en nasjon, en terrororganisasjon eller andre fiender angriper USA ved bruk av IKT, bør ikke reaksjonen fra USA være begrenset til kriminell straffeforfølgning. USA påberoper seg retten til å reagere på slike angrep på det måten USA selv finner mest hensiktsmessig. USA vil være forberedt på slike eventualiteter (A/R 5-4).
- USA vil gjennom arbeid i internasjonale organisasjoner og i samarbeide med industrien støtte en dialog mellom utenlandske offentlige og private sektorer knyttet til beskyttelse av informasjonsinfrastrukturen. Videre vil USA støtte opp om en global ”sikkerhetskultur” (A/R 5-5).
- USA vil sammen med Canada og Mexico arbeider for å gjøre Nord Amerika til ”sikker internettsone”. Arbeid vil rettes inn mot programmer som identifiserer og sikrer kritiske

nettverk som støtter telekommunikasjon, kraftforsyningen, transportsektoren, bank og finanssektoren, nødetatene, mat og vannforsyning og helsesektoren (A/R 5-6).

- USA vil oppfordre alle land til å bygge videre på kunnskapene de tilegnet seg i forbindelse med år 2000 problematikken, samt etablere en sentral kontaktperson som kan fungere som en kontaktperson mellom nasjonale og internasjonale tiltak innen IKT-sikkerhet. Ved å etablere slike kontaktpunkter kan man få en betydelig forbedret internasjonal koordinering og løsning av sikkerhetsproblemer. USA oppfordrer også hver enkelt nasjon til å bygge opp sin egen varslings- og overvåkingstjeneste som er i stand til å informere offentlige og private organisasjoner samt andre land om overhengende farer og virus (A/R 5-7).
- For å muliggjøre deling av trusselinformasjon i sanntid etter hvert som denne informasjonen blir tilgjengelig, vil USA lede etableringen av et internasjonalt nettverk i stand til å motta, vurdere og spre denne type informasjon globalt (A/R 5-8).
- USA vil oppfordre regionale organisasjoner som APEC, EU og OAS til å etablere en komité med ansvar for IKT-sikkerhet. Slike komiteer vil ha nytte av å etablere arbeidsgrupper med representanter fra privat sektor. USA vil også oppfordre de nevnte regionale organisasjonene til å opprette en felles komité med ansvar for IKT-sikkerhet. En slik komité må ha representanter fra så vel statlig som privat sektor (A/R 5-9).
- USA oppfordrer andre nasjoner til å slutte seg til Europarådets konvensjon om IKT-kriminalitet eller forsikre seg om at deres nasjonale lover er minst like omfattende (A/R 5-10).

F FORKORTELSER

A/R	Action and Recommendation
AAD	Arbeids- og administrasjonsdepartementet
ACA	Australian communication authority
ACCC	Australian Competition and Consumer commission
ACIF	Australian communications industry forum
ACIP	Analysis and Assessment for Critical Infrastructure Protection
ACSI 33	Australian Communications-Electronic security Instructions
AFP	Australian Federal Police
AGLEC	Acton Group on Law enforcement
AISO	Australian Security Information Organisation
ANAO	Australian National Audit Office
APEC	Asia Pacific Economic Cooperation forum
APS	Australian Protective Service
AusCERT	National Computer Emergency Response Team for Australia
BAS	Beskyttelse av samfunnet
CEN	The European Committee for Standardization
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CIAC	Critical Infrastructure Advisory Council
CIAO	Critical Infrastructure Assurance Office
CIP	Critical Infrastructure Protection
CIPB	President's Critical Infrastructure Protection Board
CIPG	Critical infrastructure Priorities Group
CSG	Customer Service Guarantee
CSTF	Cyber Security Task Force
CWIN	Cyber Warning and Information Network
DCS/SCADA	Digital Control System / Supervisory Control and Data Acquisition System
DDSI	Dependability Development Support Initiative
DG	Directorate-General
DHS	Department of Homeland Security
DoS	Denial of Service
DSB	Direktoratet for samfunnssikkerhet og beredskap
DSD	Defence Signals Directorate
ELP	Evaluated product list
EMA	Emmergency Management Australia
EO13228	Executive Order 13228 – Executive Order Establishing Office of Homeland Security
EO13231	Executive Order 13231 – Critical Infrastructure Protection in the information age

ESCG	E-Security Co-ordination Group
ESO	European Standardization Organizations
ETSI	The European Telecommunications Standard Institute
EU	Den Europeiske Union
FD	Forsvarsdepartementet
FedCIRC	Federal Computer Incident Response Center
FoU	Forskning og utvikling
GETS	Government Emergency Telecommunications Service
GIG	Global Information Grid
GSA	General Services Administration
HØYKOM	Høyhastighetskommunikasjon
IDC	Interdepartemental komité, som er en tverrdepartemental komité/ekspertgruppe innen IKT-sikkerhet
IKT	Informasjons- og kommunikasjonsteknologi
ISAC	Information Sharing and Analysis Center
ISIDRAS	Information Security Incident Ready Reckoner
ISLD	Information and Security Law Division under Attorney Generals Department
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Information Society Technologies
IT	Informasjonsteknologi
JD	Justisdepartementet
JOA	Joint Operating Arrangements
NBF	Nettverksbasert forsvar
NCC	National Coordinating Center (for Telecommunication)
NCS	National Communications System
NCSA	National Computer Security Authority, underlagt DSD
NCTC	The National Counter-Terrorism Committee
NHD	Nærings- og handelsdepartementet
NIAC	National Infrastructure Advisory Council
NIAP	National Information Assurance Partnership
NII	Nasjonal Informasjonsinfrastruktur
NIPC	National Infrastructure Protection Center
NOIE	National Office for the Information Economy
NOU	Norsk Offentlig utredning
NSA	National Security Agency
NSC	National Security Council
NSF	National Science Foundation
NSIE	Network Security Information Exchange
NSM	Nasjonal Sikkerhetsmyndighet
NSTAC	National Security Telecommunications Advisory Committee
NSTC	National Science and Technology Council
OAS	Organization of American States

OECD	Organisation for Economic Co-operation and Development
OHS	Office of Homeland Security
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSTP	Office of Science and Technology Policy
PADC	Patch Authentication and Dissemination Capability
PCCIP	Presidents Commission for Critical Infrastructure Protection
PCIS	The Partnership for Critical Infrastructure Security
PDD-63	Decision Directive 63
PKI	Public Key Infrastructure
PSCC	Protective Security Coordination Centre
PSM	Protective Security Manual
PSPC	Protective Security Policy Committee
RIT	Regional Telecommunications Inquiry
SCNS	Secretaries' Committee on National Security er underlagt National Security Committee of the Cabinet, som igjen er del av Kabinettet i Australia, og opptrer altså på Regjeringens vegne
SIDC	Standing Interdepartmental Committee for Protection of the National Information Infrastructure
SIS	Senter for Informasjonssikring
TIFKOM	Teleberedskap I Fritt Konkurransemarked
TISN	Trusted information network shearing
TSP	Telecommunications Service Priority
USO	Universal Service Obligation
WPS	Wireless Priority Service

Litteratur

(1) RAND Europe (NL) (2002): National Dependability Policy Environments - United States of America.

(2) Office of Homeland Security (2002): National Strategy for Homeland Security.

(3) The White House (1996): Executive Order 13010.

(4) President's Commission on Critical Infrastructure Protection (1997): Critical Foundations - Protecting America's Infrastructures.

(5) Critical Infrastructure Assurance Office (2000): Legal Issues White Paper (http://www.ciao.gov/resource/whitepaperprinter.html).

(6) The White House (2001): Executive Order 13228.

(7) The White House (2001): Executive Order 13231.

(8) Department of Homeland Security (2003): The National Strategy to Secure Cyberspace.

(9) Department of Homeland Security (2003): Budget in Brief.

(10) Forsvarsdepartementet, Nærings- og handelsdepartementet og Justis- og tolldepartementet (2003): Nasjonal strategi for informasjonssikkerhet - Utfordringer, prioriteringer og tiltak.

(11) Nærings- og handelsdepartementet (2002): OECD retningslinjer for sikkerhet i informasjonssystemer og nettverk.

(12) Nærings- og handelsdepartementet (2003): Strategi for IKT-forskningen 2003-2004.

(13) The Office of the Manager, National Communications System (2001): Guide to understanding the National Coordinating Center for Telecommunication and the Network Security Information Exchanges (http://www.ncs.gov/nstac/NSTACXXIII/NSTACFactSheet.pdf).