# FFI RAPPORT

## HÅNDTERING AV IKT-KRISER
## - Aktører og roller

BOGEN Lene, MØRKESTØL Kristin

**FFI/RAPPORT-2005/03536**

# HÅNDTERING AV IKT-KRISER
## - Aktører og roller

BOGEN Lene, MØRKESTØL Kristin

FFI/RAPPORT-2005/03536

**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-2005/03536 | UNCLASSIFIED | 72 |
| **1a) PROJECT REFERENCE** | **2a) DECLASSIFICATION/DOWNGRADING SCHEDULE** | |
| FFI-I/1014 | - | |

**4) TITLE**

HÅNDTERING AV IKT-KRISER
- AKTØRER OG ROLLER

ICT CRISIS MANAGEMENT
- Who are involved and what are their roles?

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

BOGEN Lene, MØRKESTØL Kristin

**6) DISTRIBUTION STATEMENT**

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

**7) INDEXING TERMS**

| IN ENGLISH: | IN NORWEGIAN: |
|---|---|
| a) ICT crisis | a) IKT-kriser |
| b) Critical Infrastructure | b) Kritisk infrastruktur |
| c) Crisis management | c) Krisehåndtering |
| d) Scenarios | d) Scenarier |
| e) | e) |

**THESAURUS REFERENCE:**

**8) ABSTRACT**

This report presents an analysis and overview of the different actors involved in ICT crisis management in Norway. It particularly studies the responsibilities, roles and the measures available, and also gives an introduction to ICT crisis management in Italy and France. The study is part of a comprehensive project, "Critical Information Infrastructure Protection", and has been conducted to provide background information for future recommendations and the ranking of measures for reducing vulnerabilities.

The interviews and workshop, based on imagined crisis-scenarios, lead to the conclusion that an ICT crisis is often treated as any other crisis. It proves especially challenging to define an "owner" of an ICT crisis, due to the difficulty in allocating it in a specific sector. The operational crisis management is executed at the lowest possible level, as is also the findings from other countries. The report identifies a general need for a more frequent use of exercises, in order to better prepared for an ICT crisis.

| 9) DATE | AUTHORIZED BY<br>This page only | POSITION |
|---|---|---|
| 2005-11-11 | Jan Erik Torp | Director |

ISBN 82-464-0969-7

**UNCLASSIFIED**

**SECURITY CLASSIFICATION OF THIS PAGE**
**(when data entered)**

**INNHOLD**

**HÅNDTERING AV IKT-KRISER**
**- Aktører og roller**

# 1 INNLEDNING

Prosjektet ”Beskyttelse av samfunnet 5” (BAS5) skal utvikle metoder for å analysere sårbarheter i kritiske IKT-systemer. Denne rapporten ser nærmere på ett av delmålene i BAS5-prosjektet. Delmålet er knyttet til anbefaling og rangering av tiltak som kan føre til at ansvar og roller innen IKT-sektoren blir bedre avklart. I denne sammenheng vil rapporten se nærmere på hvilke aktører som kan bli involvert i en *IKT-krise* på nasjonalt nivå i Norge, hvilke ansvar og roller de har og hva slags virkemidler de har til rådighet. Rapporten vil dermed bidra med viktig bakgrunnsinformasjon til BAS5. Et blikk på andre lands erfaringer vil også kunne gi innspill til nye måter å håndtere en slik krise på i Norge.

Svikt i systemer som på en eller annen måte medfører at vi får en IKT-krise, kan ha mange årsaker. Dette kan blant annet være villede angrep, teknisk svikt eller naturkatastrofer. Avisoverskrifter av typen ”Al-Qaida planlegger cyberangrep” forekommer oftere, og man ser også eksempler på angrep på IKT-systemer. På en Canadisk nyhetsportal ble det 15. juli i år opplyst om et angrep på statlige datasystemer, der hackere var målrettet ute etter sensitiv informasjon (1). Slike angrep kan være økonomisk motivert, men det er også en frykt for politisk motiverte angrep som kan sette store deler av kritisk infrastruktur ut av spill. Onsdag 3. august, en tilfeldig valgt dag, kunne man finne 5 artikler om sikkerhet eller terror i noen av landets største aviser[1]. Det er lite sannsynlig at fokuset på sikkerhetsproblematikk vil avta i årene som kommer.

Parallelt med et utvidet trusselbilde, settes det stadig økende fokus på myndighetenes evne til å håndtere kriser i samfunnet. Tsunamikatastrofen 2. juledag 2004 er et av de nyeste eksemplene på en krise som stilte norske myndigheter overfor store utfordringer, og i ettertid har flere vært kritiske til myndighetenes håndtering av denne krisen. Noen av svakhetene i håndteringen av denne krisen er dokumentert i ”Rapport fra evalueringsutvalget for flodbølgekatastrofen i Sørøst-Asia” (17). Ved å se tilbake på Stortingsmelding 17, ”*Samfunnssikkerhet – Veien til et mindre sårbart samfunn”* fra 2002 finner vi en noe annen vurdering av myndighetenes krisehåndteringsevne (2):

> ”Erfaringene f.eks. fra situasjoner som tilstrømmingen av flyktninger fra Kosovo i 1998 (samordningen ble ledet av Justisdepartementet), utbruddet av munn- og klovsyke i Europa i 2001 (samordningen ble ledet av Landbruksdepartementet), og tiden rundt og etter 11. september (samordningen ble ledet av Justisdepartementet innenriks og Utenriksdepartementet utenriks), har vært at håndteringen av kriser og samordningen mellom departementene har fungert tilfredsstillende. Dette skyldes ikke minst at det

[1] Aftenposten, Dagens Næringsliv, Dagsavisen, Klassekampen, Dagbladet, VG.

raskt har blitt tatt kontakt mellom de berørte departementene og Statsministerens kontor".

Ulike vurderinger og oppfatninger av vår krisehåndteringsevne tilsier at det er behov for ytterligere analyser innen dette feltet. I denne rapporten ses det på dette spesielt i lys av tenkte IKT-kriser.

# 2 FORMÅL MED OG OPPBYGGING AV RAPPORTEN

## 2.1 Formål

Formålet med rapporten er å skaffe innsikt i krisehåndtering med hensyn til svikt i viktige IKT-systemer. Dette innebærer å kartlegge hvordan en krisesituasjon vil håndteres i dag, for å kunne si noe om hvordan den ideelt kan håndteres. Følgende hovedpunkter danner utgangspunktet for rapporten:

1. **Hvem har ansvar, myndighet og virkemidler i en gitt krisesituasjon?**
   Dette innebærer å se nærmere på hvilken rolle de ulike myndighetsorganene har i en tenkt krisesituasjon, hvilke deler av krisehåndteringen de er ansvarlige for, og på hvilke tidspunkt i krisen myndighetene trer inn. Dette skal undersøkes i forhold til hvem som har en operativ, koordinerende eller kontrollerende funksjon.
2. **Hvilke virkemidler har myndighetene i en gitt krisesituasjon?**
   Virkemidler kan typisk være makt, penger og teknologisk rettede tiltak. Dette undersøkes gjennom en kartlegging av verdikjeden i en krise, det vil si hendelsesforløpet fra krisen inntreffer til det er skrevet rapport om hendelsen.
3. **Håndteres kriser forskjellig avhengig av hva slags type krise det er?**
   Spørsmålet avdekker om myndighetene og andre aktører har forskjellige roller avhengig av årsaken til krisen. Hvordan er samarbeidet og koordineringen mellom disse aktørene i ulike krisesituasjoner?
4. **Hvordan har andre land organisert seg i forhold til krisehåndtering?**
   Dette innebærer å studere andre lands organisering av krisehåndtering i forhold til de samme kriteriene som er beskrevet i gjennom punktene 1-3. Dette vil gi grunnlag for å si noe om hva Norge kan lære fra andre land.

## 2.2 Metode

Problemstillingen er behandlet gjennom datainnsamling på to måter:

- **Primærdata:** gjennom samtaler med relevante myndigheter og andre aktører
- **Sekundærdata:** ved litteratursøk, hovedsakelig på Internett.

Denne metoden er felles for både den nasjonale og internasjonale studien. Landene som er valgt for utenlandsstudien er Italia og Frankrike. Italia er valgt ut på bakgrunn av sin håndtering av

Tsunamikatastrofen, som har høstet mye ros i etterkant. Frankrike er valgt fordi de har en sentral rolle gjennom EU og underliggende arbeidsgrupper, som blant annet ENISA. Det kunne også vært interessant å se nærmere på land som USA, Canada og Storbritannia, men dette er ikke utført på grunn av tidsmessige begrensninger. I tillegg finnes det allerede mye god dokumentasjon tilgjengelig på engelsk fra disse landene.

For å kvalitetsikre resultatene fra den norske studien, inviterte vi aktørene til et felles arbeidsseminar på FFI[2]. 23 deltagere var med på å drøfte de foreløpige resultatene, og innspillene fra arbeidsseminaret har derfor blitt inkludert i denne rapporten.

For å synliggjøre og konkretisere problemstillingen er det utarbeidet tre scenarier:

1. Teknisk og driftsmessig krise
2. Naturlig forårsaket krise
3. Sikkerhetspolitisk krise

Disse har blitt brukt for å avdekke hvilke aktører som kan tenkes å være involvert i håndteringen av en IKT-krise.

En begrensning med metoden er at den primære datainnsamlingen baserer seg på meninger fra enkeltpersoner hos de ulike aktørene som har vært intervjuet. Det må derfor tas høyde for en viss grad av subjektive vurderinger, avhengig av personenes syn på problemstillingen.

### 2.3 Rapportens oppbygging

Etter de innledende kapitlene (1 og 2) gis en teoretisk introduksjon til temaer som blir diskutert gjennom resten av rapporten (kapittel 3). Kapittel 4 beskriver i korte trekk den nye formelle strukturen som eksisterer for krisehåndtering i Norge.

I kapittel 5 blir det gitt en trinnvis beskrivelse av krisehåndtering gjennom tre konstruerte scenarier. Deretter viser kapittel 6 til eksempler på hvordan IKT-kriser kan håndteres i Italia og Frankrike, før det blir gitt en kort gjennomgang av relevante EU-aktiviteter på området kritisk infrastruktur.

Til slutt blir det i kapittel 7 gitt en diskusjon av funnene i de foregående kapitlene i henhold til problemstillingen, før kapittel 8 avrunder rapporten med en kort konklusjon.

## 3 IKT-SIKKERHET I SAMFUNNET – ET TEORETISK RAMMEVERK

Følgende kapittel går i korte trekk gjennom relevante teoretiske begrep som har betydning for håndtering av kriser. Det teoretiske rammeverket plasserer emnet IKT inn i en større sammenheng. Hvordan man tenker omkring sikkerhet på lavere administrativt plan

[2] "Workshop om håndtering av IKT-kriser", 23/8-2005, med deltagere fra JD, DSB, SD, PT, NVE, FD, NSM, NorCERT, Fylkesmannen Oslo/Akershus og Forsvarets Sikkerhetsavdeling.

(bedriftsnivå) får f. eks. betydning for IKT som sikkerhetsutfordring for nasjonalstaten.

## 3.1 Hva er en IKT-krise for kritisk infrastruktur?

Begrepene "IKT-krise" og "kritisk infrastruktur" vil bli benyttet mye gjennom rapporten, og det er derfor på plass med et forsøk på begrepsavklaring. Avhengig av person og virksomhet er oppfatningene forskjellige av hvor ille en situasjon skal være for at noe skal bli kalt en krise. I rapporten etter Sårbarhetsutvalget blir *krise* definert som (18):

> "en hendelse som har potensial til å true viktige verdier og svekke en organisasjons evne til å utføre viktige funksjoner".

Flere vil hevde at det ikke er behov for en egen definisjon av IKT-krise, men at denne følger naturlig som en utvidelse av krisebegrepet. Som en arbeidsdefinisjon gjennom denne rapporten vil vi ta utgangspunkt i at en IKT-krise er *en situasjon der informasjons- og kommunikasjonssystemer blir satt ut i en grad som gjør at de ikke kan håndteres med "vanlig" bemanning og normale rutiner.*

DSB har identifisert en rekke faktorer som er betegnede for de fleste kriser, og som også kan overføres til begrepet IKT-kriser (3):

- Krisen kommer overraskende
- Mangel på kontroll
- Vitale interesser står på spill
- Mange aktører
- Tidspress
- Sammenbrudd i den regulære beslutningsprosessen
- Fokus på kortsiktige løsninger
- Usikkerhet
- Mangel på informasjon
- Intens interesse og oppfølging fra utenforstående

I praksis ser det ut til at det ikke legges stor vekt på å skille mellom IKT-kriser og andre kriser, ettersom krisen uansett skal håndteres på lavest mulig nivå. I utgangspunktet må bedriften selv håndtere krisen, men departementene vil få et politisk ansvar som innebærer krisehåndtering på et senere stadium. Dette vil bli diskutert nærmere i senere kapitler.

### 3.1.1 Hva er kritisk infrastruktur?

Det finnes utallige forslag til definisjoner av kritisk infrastruktur, både nasjonalt og internasjonalt. I et FFI-notat fra 2005 blir forskjellen mellom kritisk infrastruktur og samfunnsfunksjoner beskrevet som følgende (4):

> "Kritisk infrastruktur er de nettverk som er grunnlaget for all annen samfunnsvirksomhet, mens samfunnsfunksjoner er tjenester som benytter de kritiske

> infrastrukturene for å dekke behovene til befolkningene, virksomheter og aktører i samfunnet."

I samme notat gir Professor Kåre Petter Hagen noen innspill til definisjonen, og mener kritisk infrastruktur må sees på fra behovsiden, og at det må mangle substitusjonsmuligheter for at en tjeneste skal være kritisk. Et enkelt eksempel som blir nevnt er tilgang på antibiotika. Dette er en kritisk tjeneste for en person med livstruende infeksjoner, ettersom det ikke finnes noe erstatning for antibiotika som vil gi samme effekt.

En av de nyeste utredningene om begrepet kritisk infrastruktur er gitt til Utvalget for sikring av landets kritiske infrastruktur (Infrastrukturutvalget) i juli 2005[3]. Etter en diskusjon om samfunnsverdier og kritiske samfunnsfunksjoner er det bygget opp følgende definisjon:

> "Kritisk infrastruktur er de objekter, systemer, tjenester og ressurser som understøtter samfunnets grunnleggende verdier. Samfunnets grunnleggende verdier er fred og nasjonal selvstendighet, en demokratisk rettsstat, en god samfunnsøkonomi, velferd til befolkningen, liv og helse, livsmiljøet og nasjonal trygghetsfølelse"

Det er verdt å legge merke til at det for tiden pågår flere diskusjoner om hvordan man kan definere kritisk infrastruktur. Blant annet jobber Infrastrukturutvalget med å komme frem til én dekkende definisjon, som vil bli inkludert når avslutningsrapporten foreligger ved årsskiftet 2005-06[4].

## 3.2 Kan man skille mellom safety og security?

Begrepene "safety" og "security" vil også være relevante ift. IKT-kriser. Svært forenklet går skillet på at safety-begrepet som regel er forbundet med utilsiktede handlinger, mens security innebærer ondsinnete handlinger. Dette vil si at begrepene i hovedsak er forskjellige ved å ha ulike årsaksforhold. Enkelte vil hevde at konsekvensene på mange samfunnsnivåer blir de samme, uavhengig av om hendelsen skyldes en ulykke eller et angrep. Uansett årsak vil mange aktører opprettholde den samme rollen i fasene med skadebegrensning og gjenoppretting. Likevel vil det være en stor forskjell i den politiske oppmerksomheten rundt hendelser avhengig av hvilken årsak de har, og virkemidlene som tas i bruk for å håndtere krisen vil variere med årsaksforholdet (f.eks. kan politiet eller Forsvaret få en rolle når det gjelder å håndtere aktørene som står bak en security-relatert utfordring). Slike forskjeller blir viktige å avklare i forhold til krisehåndtering.

En rekke professorer gikk hardt ut mot organiseringen av beredskapsarbeidet i Norge i en kronikk i Aftenposten i år (5). Her trekkes det frem at forskning på risiko og sikkerhet i stor grad baserer seg på skippertaksarbeid i etterkant av store katastrofer. Et viktig tiltak for å forbedre dette kan være å satse på et tettere samarbeid mellom forskningsmiljøene innen safety-

[3] Notat mottatt per e-post av Kjetil Sørli (DSB), 22.07.05
[4] Ref. samtale med sekretariatsleder i Infrastrukturutvalget, Dagfinn Buseth (JD), 25.07.05

og security-hendelser, ettersom det er mange sammenfallende berøringspunkter i forhold til sårbarhet og krisehåndtering.

## 3.3 Sikkerhetisering

”Sikkerhetisering”[5] er en betegnelse som stammer fra Ole Wæver og Barry Buzan (6). Begrepet inngår i en ny måte å tenke sikkerhetspolitikk på, som ble anerkjent med ”Københavnerskolen” (København Center for Freds- og Konfliktforskning, COPRI). Sikkerhetisering innebærer at hva som defineres som sikkerhetspolitikk ikke nødvendigvis er gitt på forhånd, men er avhengig av hva som til enhver tid oppfattes som en *risiko* for en stats suverenitet. Barry Buzan har utdypet begrepet om sikkerhetisering med å spesifisere at man snakker om risiko dersom det kreves ekstraordinære tilpasninger og/eller nødhandlinger for å hanskes med den. Han hevder at sikkerhetisering legitimerer maktbruk i klassisk forstand, og Neumann og Offerdal legger til at det også hever saken over vanlig politikk og til den mer ”panikkpolitiske” sfæren. Her gjelder ikke vanlige regler for politikk, noe som ”…rettferdiggjør hemmelighold, ekstra utøvende myndigheter og aktiviteter som ellers ville være ulovlige” (7).

Problematikken omkring sikkerhetisering er på den ene side at man først etter å ha ”løftet” et emneområde inn i sikkerhetsdialogen som et risikoområde, vil ta det på alvor fra et politisk standpunkt. Det kan da være snakk om at nødvendige bevilgninger og ekstraordinære tiltak iverksettes. Dette har betydning for IKT som sikkerhetsmoment, fordi det kan være grunner til å bruke sikkerhetisering av IKT som et *virkemiddel* for å sette fokus på IKT som risikofaktor. På den annen side kan sikkerhetisering av IKT føre til at det blir satt i verk tiltak som bryter med personvern eller at utgifter til IKT utelukker andre viktige budsjettposter i samfunnet. Dette ville i så fall være i kontrast til de gjeldende prinsipper i organiseringen av samfunnssikkerhet i det norske samfunn, nemlig *ansvars-*, *likhets-* og *nærhetsprinsippet*[6].

## 3.4 Interaksjoner mellom IKT-systemer

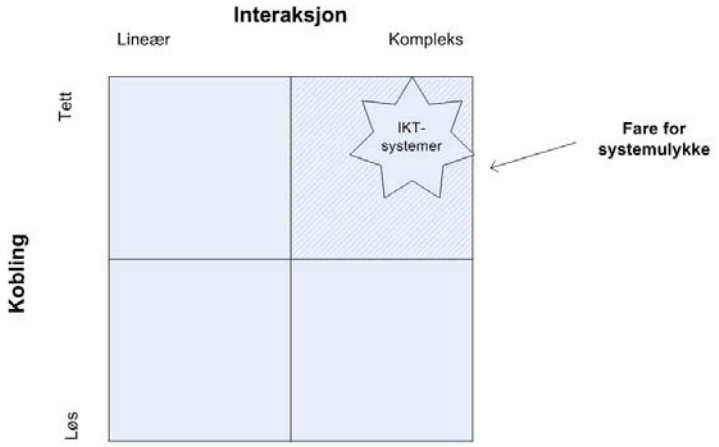
Sentralt i arbeidet med beredskap og krisehåndtering står forståelsen av å se systemer og sektorer i samspill med hverandre. De fleste kriser og katastrofer blir til gjennom en rekke feil i ulike systemer og på ulike nivåer. Charles Perrow beskriver teorien om systemulykker (normal accidents), og sier at disse skyldes uforutsette interaksjoner av multiple feil i et tett koblet system (8). Med tette koblinger menes her at en hendelse som inntreffer i én enhet vil virke inn på den neste, ettersom det ikke er designet tilstrekkelig *buffer* mellom disse enhetene.

I følge Perrow kan disse interaksjonene være både lineære og komplekse. I lineære interaksjoner foregår samspillet i en forventet sekvens, mens det i komplekse interaksjoner foregår i en ikke-forventet sekvens. Det vil si at komplekse interaksjoner ikke er designet inn i systemet, og at det ikke er meningen at de skal henge sammen. Komplekse systemer er som regel sammensatt av en

[5] *”Sikkerhetisering”* er den norske oversettelsen av *”securitization”*, ref bl.a. Den Norske Atlanterhavskomiteen; http://www.atlanterhavskomiteen.no/publikasjoner/andre/kortinfo/2003/pdf/Kortinfo7_2003.pdf samt Anders Kjølberg FFI-rapport ”Når Religionen Blir Truet” 2003/00330, http://www.nupi.no/IPS/filestore/00330.pdf

[6] Se kapittel 4 i denne rapporten, ”Ny formell struktur for krisehåndtering”

rekke lineære, synlige systemer. Sammenhengen mellom systemene er i seg selv ikke-lineær og skaper dermed kompleksitet. Figur 3.1 under viser i hvilket område systemulykker oppstår, og hvor IKT-kriser kan inntreffe:




*Figur 3.1 – Interaksjon-koblingsmatrise (Perrow, 1984)*

IKT-systemer er et tydelig eksempel på et tett koblet system med komplekse interaksjoner, ettersom flere og flere systemer både fysisk og logisk er koblet sammen. Dette tilsier at det er vanskelig å forutsi hvordan en hendelse i et IKT-system vil forplante seg, men at mulighetene for store feilsituasjoner er til stede, selv etter relativt enkle feil.

Avhengigheten til IKT er stor i mange sektorer, og en sikkerhetssjef i norsk bank har uttrykt at kun ”0,5% av pengene som flyter frem og tilbake daglig er faktiske penger (mynter, sedler)” (9). Scenariene som blir beskrevet i kapittel 5 viser tydelig hvordan feil på én sektor får konsekvenser for andre sektorer og samfunnsfunksjoner.

## 4 NY FORMELL STRUKTUR FOR KRISEHÅNDTERING

Til grunn for organisering av samfunnssikkerhet i Norge, ligger sektorprinsippet og prinsippene om *ansvar, likhet og nærhet*. Ansvarsprinsippet innebærer at den som har et ansvar i en normalsituasjon, også har ansvar i kriser. Likhetsprinsippet betyr at kriseorganisasjonen skal være mest mulig lik den organisasjonen man opererer med til daglig. Prinsippet om nærhet går ut på at krisen skal håndteres på lavest mulig nivå. Disse prinsippene gjennomsyrer beredskapstankegangen i Norge, og innebærer at hver sektor blir ansvarlig for å etablere beredskapsplaner og ta høyde for krisesituasjoner.

I juli 2005 vedtok Stortinget en ny struktur for koordinering av krisehåndtering på sentralt nivå gjennom (11):

- **Regjeringens kriseråd:**
  Regjeringens kriseråd vil være det overordnede administrative koordineringsrådet dersom krisen er av en slik karakter at flere departementer er involvert og det er behov

for omfattende koordinering. Det kan bli behov for en slik koordinering også ved en IKT-krise. Regjeringens kriseråd består av faste medlemmer fra Statsministerens Kontor (Regjeringsråden), Utenriksdepartementet (UD) Justis- og Politidepartementet (JD), Forsvarsdepartementet (FD) og Helse- og omsorgsdepartementet (HOD), som alle kan ta initiativ til innkalling av rådet.

- **Lederdepartementet**
  Det departementet *som er mest berørt* av krisen får ansvar for å samordne krisestyringen på departementsnivå. Det er utarbeidet kriterier for utpeking av lederdepartementet, samt en liste over oppgaver som tilfaller dette departementet. Likevel blir det ingen endringer *i ansvarsforhold i* departementene; de beholder det ansvaret de har jf. ansvarsprinsippet.
- **Krisestøtteenhet**
  Dette er en døgnbemannet enhet (fra 01.01.2006) som administrativt er underlagt Justisdepartementet. Krisestøtteenheten skal være en støtte til det departementet som blir utpekt til lederdepartement. En av de viktigste oppgavene til denne enheten blir å tilby *fellesressurser* for departementene, som for eksempel mobilt teknisk utstyr, felles elektronisk loggføringssystem og telefonlinjekapasitet. Enheten skal i tillegg bidra til å bygge opp et oppdatert situasjonsbilde og koordinere sikkerhets- og beredskapstiltak.

Regjeringens kriseråd skal kunne håndtere alle typer kriser. Dette vil også måtte inkludere eventuelle IKT-kriser. Et viktig problem med IKT-kriser er imidlertid at de er tverrsektorielle, og dette vil kunne gi problemer ifm. å peke ut et lederdepartement for krisen. Nærhetsprinsippet vil likevel fortsatt gjelde, slik at krisen skal håndteres på et så lavt nivå som mulig. Det departementet som blir utpekt som lederdepartement vil lede Regjeringens kriseråd. Justisdepartementet har ansvar for å sikre en *effektiv samordning av krisehåndteringen* dersom det er usikkert hvem som er hovedansvarlig departement. Hvis det oppstår uenighet om hvem som har hovedansvaret for krisehåndteringen, skal saken avgjøres av Regjeringen.

For å kunne teste ut handlekraften i kriser, må beredskapsplaner og ansvarslinjer testes ut gjennom reelle beredskapsøvelser. Lillestrøm-ulykken i april 2000, der en jernbanevogn med gass kom i brann, er et godt eksempel på en katastrofe som ble avverget blant annet fordi god beredskap var på plass (2).

## 5 SCENARIER FOR IKT-KRISER

Scenarier kan være et godt virkemiddel for å synliggjøre forskjeller i krisehåndtering. I denne rapporten er det utviklet scenarier som beskriver IKT-kriser på tre ulike nivå. Disse har blitt benyttet i intervjuer og en workshop[7] for å avklare hvilke aktører som kan få en rolle i håndteringen av krisene.

En utfordring med bruk av scenarier er å finne riktig detaljgrad. Mer detaljer i scenarier gjør ofte at diskusjonen med intervjupartnerne blir mer konkret og at usikkerheten i resultatene reduseres.

[7] "Workshop om håndtering av IKT-kriser", 23/8-2005, med deltagere fra JD, DSB, SD, PT, NVE, FD, NSM, NorCERT, Fylkesmannen Oslo/Akershus og Forsvarets Sikkerhetsavdeling.

På den andre siden kan for stor detaljgrad bidra til at resultatene bli gyldige kun innen det aktuelle scenariet. I denne rapporten er det utviklet scenarier som ikke er for detaljerte, men som har en viss fleksibilitet innebygget. Dette er valgt for å gjøre det mulig å trekke allmengyldige konklusjoner ut av resultatene.

I beskrivelsene i dette kapittelet gis det en beskrivelse av hendelsesforløpet fra krisene i scenariene inntreffer, gjennom det som skjer under krisene, til det som blir gjort i etterkant. Dette er illustrert ved hjelp av modeller som fremstiller hvilke aktører som er involvert på ulike stadier. Modellene skiller ikke mellom beslutningsnivåer, men tar med de aktørene som det har blitt henvist til i de innledende intervjuene og under arbeidsseminaret på FFI[8]. Dette vil dermed være de aktørene som er operasjonelle innenfor sin sektor i de ulike scenariene.

Et problem i aktørbeskrivelsen er omtalen av NorCERT. Det er i statsbudsjettet for 2006 satt av midler[9] til at NorCERT skal bli en nasjonal CERT som skal håndtere alvorlige dataangrep mot norsk infrastruktur på nasjonalt plan. I skrivende stund er ikke alle detaljer rundt NorCERT klarlagt, men et mandat vil foreligge i løpet av året. Når vi i det følgende omtaler NorCERT, tar vi utgangspunkt i det etablerte prosjektet slik det er per i dag, underlagt Nasjonal Sikkerhetsmyndighet.

Kapittelet gir ikke forklaring på myndighetenes rolle ved normal drift, annet enn at det er gitt henvisninger til relevant bakgrunnsinformasjon. Forøvrig vises det til Riksrevisjonens rapport om myndighetenes arbeid med å sikre IT-infrastruktur som vil foreligge i slutten av november 2005[10].

Det understrekes til slutt at vurderingene i dette kapittelet er sammenstilt med bakgrunn i uttalelser av enkeltpersoner under intervjuer og den før nevnte workshopen.

## 5.1 Scenario 1 - Teknisk og driftsmessig svikt

Scenario 1 er som følger:

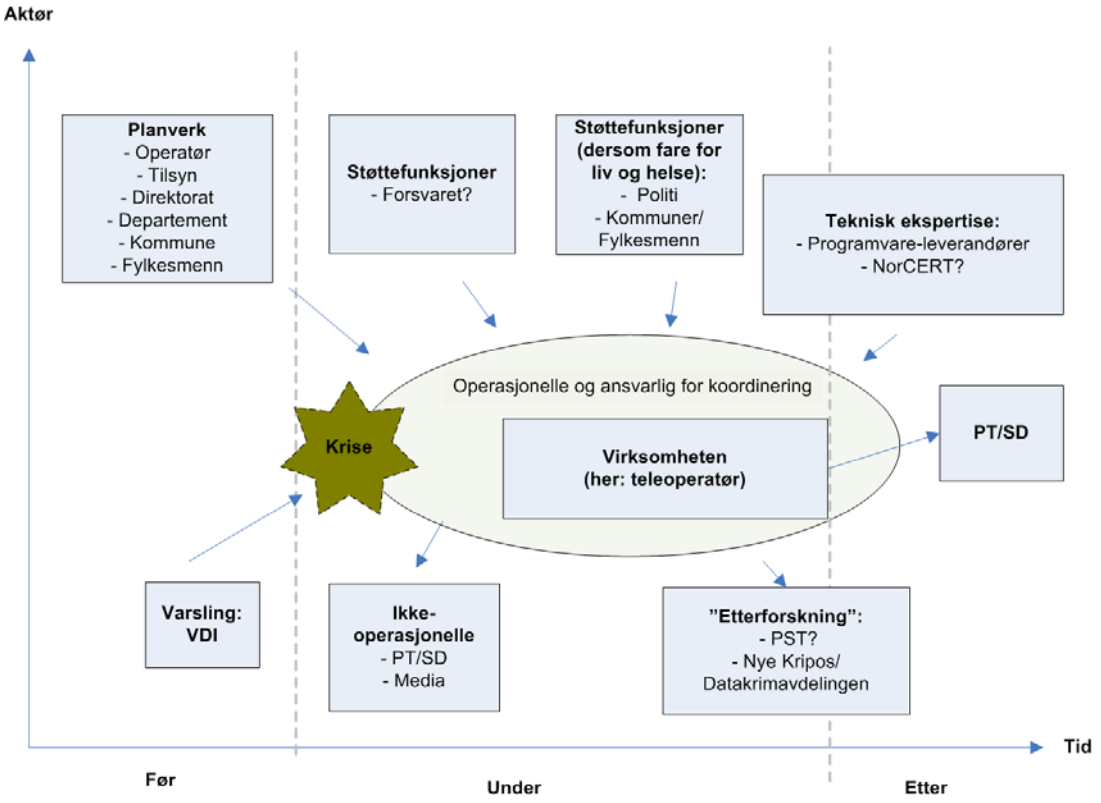
> ”Prosesskontrollsystemet for tjenesteproduksjon i bedriften settes helt eller delvis ut av spill. Tjenesteproduksjon lammes over lenger tid og et større område i Norge er uten tilgang på kommunikasjonstjenester. Årsak kan være både teknisk svikt (programvare) eller et villet angrep.”

Med ”lenger tid og et større område” menes for eksempel at en hel landsdel, eller flere fylker, har mistet tilgang på kommunikasjonstjenester i mer enn ett døgn. Når en slik hendelse inntreffer vil sannsynligvis ikke omfanget være helt klart til å begynne med, og i gjennomgangen av roller er det tatt hensyn til at hendelsen begynner som en bedriftsintern krise,

[8] Beskrevet i kapittel 2.2
[9] 5 millioner kroner, iflg. artikkel i VG 08.09.2005 (12)
[10] Ref. samtale Egil Andresen (Riksrevisjonen), 15.09.05. Rapporten vil bli tilgjengelig på http://www.riksrevisjonen.no , med tittelen ”Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur”.

som gradvis involverer flere aktører etter hvert som man oppfatter at omfanget av krisen øker.

For å konkretisere diskusjonen er scenariet avgrenset til å gjelde en telekommunikasjonsbedrift, der man snakker om bortfall i fastnettet over 2 dager. Figur 5.1 viser aktørene som kan bli involvert i en slik krise[11], og på hvilket tidspunkt av krisen de kommer inn i bildet.




*Figur 5.1 – Hendelsesforløp – scenario 1*

En forklaring og drøfting av figuren blir gitt i henhold til de tre fasene før, under og etter en krise.

### 5.1.1 Før krisen: varsling

Som vist til venstre i figuren bør det i forkant av en krise være to systemer på plass:

- et planverk for krisehåndtering på alle nivåer
- et etablert system for varsling i kriser.

*Planverk*

For å være mest mulig forberedt på en krise, bør alle virksomheter ha på plass en *beredskapsplan* for krisehåndtering. Som boksen øverst til venstre i figuren viser, bør det foreligge planverk på alle nivåer, fra operatør- og virksomhetsnivå til departementsnivå.

I en normalsituasjon er det klare linjer på hvem som skal føre tilsyn med hvem. Knyttet til

[11] Våre scenarier tar ikke med i betraktning hvordan andre kritiske infrastrukturer blir berørt, som for eksempel helse og finans etc.

elektronisk kommunikasjon har for eksempel Post- og Teletilsynet (PT) ansvar for å føre tilsyn med at Ekom-forskriften etterfølges av operatørene. PT har hjemmel for å pålegge virksomhetene å gjennomføre nødvendige tiltak, dersom de avdekker mangler. Det som ofte er tilfelle i forhold til beredskapsplaner er at tilsynsmyndigheten setter krav til *at* det skal være en plan på plass, men de sier ikke noe om hva den skal inneholde. Det kan derfor stilles spørsmål ved hvorvidt beredskapsplanene på alle nivåer er fullstendig oppdaterte til enhver tid.

*Varsling*
Det andre aspektet som kommer inn i forkant av en krise, er muligheten for å *varsle* den aktuelle virksomheten. Ved feil innenfra, eller som følge av teknisk svikt, vil virksomheten selv være den første til å avdekke feilen. Dersom det er snakk om angrep fra Internett, vil Varslingssystem for Digital Infrastruktur (VDI)[12] kunne observere unormal aktivitet på medlemsbedriftenes nett, og dermed være den første til å varsle virksomheten. Dette forutsetter at VDI har sensorer plassert ute i bedriften, slik at de kan foreta aktiv overvåkning. I dag er det kun et lite antall bedrifter som er knyttet opp mot VDI, og som dermed sikrer seg denne muligheten.

### 5.1.2 Under krisen: koordinering og operasjonelt ansvar

På dette tidspunktet er IKT-krisen et faktum, noe som illustreres ved hjelp av krisestjernen i figuren. Følgende aktører kan tenkes å bli involvert på dette stadiet:

- **Operasjonelt og koordinerende ansvar:** virksomheten
- **Mellomrapportering:** Post- og Teletilsynet (PT), Samferdselsdepartementet (SD)
- **Informasjon:** Media
- **Teknisk ekspertise:** Programvareleverandører, NorCERT
- **Etterforskning:** PST
- **Støttefunksjoner:** Politi, kommune, Fylkesmannen
- **Dersom eskalering:** Regjeringens kriseråd

Den første aktøren i listen er virksomheten selv som blir rammet av IKT-krisen, i dette tilfellet en teleoperatør. Virksomheten vil i utgangspunktet være fullt ansvarlig for å håndtere krisen selv.

*Mellomrapportering*
Virksomheten må reagere og vil på dette tidspunktet kontakte PT for å avgi en kort rapport om hva de tror har hendt og hvor stort omfanget er. PT vil rapportere videre til SD, slik at de er forberedt på å overta koordineringen av krisen i tilfelle eskalering.

*Informasjon*
Foreløpig ligger alt det operasjonelle og koordinerende ansvaret for å få kontroll over krisen hos virksomheten selv. Det er sannsynlig at media vil bli koblet inn på et tidlig tidspunkt, ettersom

[12] Enhet underlagt Nasjonal Sikkerhetsmyndighet (http://www.nsm.stat.no ), bestående av et representativt utvalg av deltagere med samfunnskritisk infrastruktur. Har i dag to typer deltagere: 1) medlemmer som har sensor plassert i virksomheten, og 2) ”observatører”, dvs. de har ikke sensor plassert hos seg, men mottar samme informasjon som de øvrige medlemmene. I tillegg ser VDI for seg en tredje type medlemmer, som har ”sovende” sensorer plassert hos seg, som i en krisesituasjon kan kobles inn for overvåking.

mange brukere har mistet tilgang på kommunikasjonstjenester. Media er definert i boksen ”ikke-operasjonelt”. Det betyr at de ikke vil ha noen innvirkning på å finne en løsning på krisen, men de vil ha en stor rolle i forhold til befolkningen. Det er gjerne media som stiller myndighetene til ansvar, ved å ta direkte kontakt med den instansen de ser det mest logisk å kontakte. Selv om nærhetsprinsippet tilsier at denne krisen skal håndteres hos virksomheten, kan SD som ansvarlig myndighet måtte komme med uttalelser. Media er i tillegg ofte de som setter standarden for hvorvidt noe blir definert som en krise eller ikke, men de kan også bidra til å forhindre at det sprer seg panikk blant befolkningen.

*Teknisk ekspertise*
Dersom virksomheten selv ikke er i stand til å håndtere krisen og finne løsning på den, vil de måtte søke råd fra teknisk ekspertise. Myndighetene har få virkemidler å sette inn i en slik IKT-krise, og virksomheten må derfor kontakte programvareleverandører eller underleverandører for å sikre seg hjelp. Eksterne leverandører av utstyret virksomheten anvender er naturlige kontaktpunkter. Muligens vil også NorCERT som en nasjonal enhet kunne bidra på dette stadiet i krisen[13].

Et samarbeid mellom teleoperatører i en krise blir sett på som en utfordring, hvis ikke en umulig oppgave, ettersom man benytter seg av ulike systemer og ulike underleverandører.

”*Etterforskning”*
I den grad scenariet kun innebærer teknisk og/eller driftsmessig svikt, vil virksomheten selv undersøke årsaksforhold i forbindelse med feilfinning og eventuelt sikre informasjon for senere årsaksanalyse og eventuelle regresskrav mot leverandør. Dersom det er mistanke om lovbrudd (i tilfelle ondsinnet angrep), vil virksomheten involvere politiet og eventuelt deres ekspertise for å sikre informasjon.

Manglende involvering av politi kan fort bli et problem på nasjonalt plan, ettersom man på denne måten mister muligheten til å si noe om det er et koordinert angrep. Forsinkelser her vil gjøre det vanskelig å sette inn mottiltak umiddelbart.

*Støttefunksjoner*
De aktørene som har blitt plassert i kategorien støttefunksjoner, vil kun komme på banen dersom det oppstår fare for liv og helse. I så fall vil politi, kommuner og Fylkesmannen få en rolle. I dette scenariet vil sannsynligvis ikke kommunen og Fylkesmannen bli involvert, ettersom det dreier seg om feil hos én operatør.

Post- og teletilsynet kan i gitte situasjoner bistå med vurdering av alternative sambandsløsninger, eventuelt gi andre tilbydere myndighetspålegg om bistand til å gjenopprette samband.

[13] I motsetning til VDI som kommer inn på *varslings*siden i en krise, vil NorCERT være en *respons*enhet, som kan koordinere tiltak på tvers av sektorer for å håndtere krisen.

Forsvaret har blitt nevnt av mange som en mulig støttefunksjon. På arbeidsseminaret ble det imidlertid sagt at det skal mye til for at Forsvaret settes inn. Dette skyldes delvis den nye ressurssituasjonen Forsvaret er i, både med tanke på økonomi og personell. Men Forsvarets kan også kun gi støtte til helt konkrete oppgaver der de kan tilby en ressurs som ikke er tilgjengelig på andre måter. Bistanden fra Forsvaret under flommen på Østlandet i 1995, med lokal ledelse, vakthold, bæring av sandsekker osv., er et eksempel på hvordan Forsvaret kan bidra overfor sivilsamfunnet. Utgiftene må dekkes av de som kommer med anmodning til Forsvaret om bistand.

På den annen side kan det nevnes at Forsvaret har et betydelig potensial til å etablere midlertidige digitale linjer via Forsvarets Deployerbare Kommunikasjonsmoduler/ "Multirolleradioer". Disse har både operatør- og ledelseselementer til å gjenopprette og etablere telefon- og internettforbindelser helt uavhengig av de kommersielle operatørene. Disse vil kunne transporteres til det stedet som trenger slikt samband i løpet av svært kort tid. Dette vil naturlig nok ikke dekke hele samfunnets behov for samband, men kan understøtte kriseledelsen.

*Hva skjer ved eskalering av krisen?*
Slik scenariet i utgangspunktet er beskrevet, dreier dette seg om en sektorkrise, der det er relativt enkelt å plassere ansvar. Krisen oppstår i telesektoren, og overordnet ansvar blir dermed plassert hos Samferdselsdepartementet. Men dersom store deler av teletjenestene blir borte over flere dager, vil dette berøre flere sektorer, og det kan bli aktuelt å kalle sammen koordineringsinstanser på høyere plan. Dette kan være sammenkalling av Regjeringens kriseråd, som det i et slikt scenario sannsynligvis vil være Samferdselsdepartementet som tar initiativ til. Ved eskalering av krisen vil det være sannsynlig at flere aktører kommer på banen, som for eksempel Forsvaret, ettersom de har mulighet til å understøtte *den kapasiteten* som blir borte (sambandet). En av deltakerne på arbeidsseminaret ved FFI uttalte at;

> ”Det å være uten samband *er* kritisk, og Regjeringens Kriseråd bør derfor settes inn”

På samme arbeidsseminar ble det også nevnt at hvorvidt Regjeringens kriseråd skulle tre sammen eller ikke ville bli diskutert ved Statsministerens Kontor. Det ble også sagt at man ikke helt sikkert kan si noe om hvorvidt Regjerings Kriseråd vil tre sammen eller ikke i dette scenariet, og at dette er noe som må vurderes fortløpende. Rollefordelingen vil endre seg ettersom krisen utvikler seg, og det er mer sannsynlig at Regjeringens Kriseråd settes inn hvis krisen er av en viss varighet, opp mot en uke. Dette kommer også an på hvor stort geografisk område som er rammet.

### 5.1.3 Etter krisen: gjenoppretting og oppfølging

Aktører som blir involvert i en ”etterfase” av scenario 1 er tilknyttet tre ulike kategorier:

- **Gjenoppretting:** Virksomheten, programvareleverandører, NorCERT
- **Etterforskning:** Datakrimavdelingen (Nye Kripos)
- **Rapportering:** Post- og Teletilsynet, Samferdselsdepartementet

Selv om dette i utgangspunktet startet med en IKT-krise, vil mange si at IKT-svikten i seg selv ikke er en krise. Det er ringvirkningene/konsekvensene for andre sektorer som vil definere hvor stort omfanget av krisen blir.

*Gjenoppretting*
Til gjenopprettingsfasen vil man i dette scenariet være mest avhengig av teknisk ekspertise for å få datasystemene opp å gå. Som beskrevet i "underfasen" vil dette kunne involvere programvareleverandører og NorCERT, når sistnevnte blir operativt. Disse aktørene vil sannsynligvis være sentrale aktører både under og etter krisen.

*Etterforskning*
Datakrimavdelingen (Nye Kripos) har ingen operativ rolle i krisen, men vil kunne bistå i etterforskning av elektroniske spor og datakriminalitet. Dette avhenger av at virksomheten selv tar kontakt. Datakrimavdelingen har i tillegg en rolle på forebyggingssiden, ved å gi råd til bedrifter om hvordan de selv kan håndtere hendelser, samt ved å stresse viktigheten av å rapportere og anmelde kriminelle forhold[14].

*Rapportering*
I etterkant av krisen er virksomheten pålagt å rapportere til Post- og Teletilsynet. Dette skjer gjennom en detaljert rapport, der virksomheten må gjøre rede for tekniske og organisatoriske forhold som førte til hendelsen. PT benytter slik informasjon til å bygge opp en erfaringsdatabase for å være rådgiver og initiere forebyggende tiltak (via tilskudd til operatører). PT vil gi rapporten videre til Samferdselsdepartementet.

### 5.1.4 Overføring av scenariet til andre sektorer

Hensikten med dette avsnittet er å vise kort hvordan scenario 1 ville sett ut dersom man antok at IKT-krisen oppstod i prosesskontrollsystemet til en kraftleverandør eller et oljeselskap, i stedet for i et teleselskap som nettopp beskrevet.

*Angrep/svikt på prosesskontrollsystem i kraftsektoren*
Forløpet ved en teknisk svikt eller et villet angrep mot et kraftselskap vil foregå ved at de først forsøker å rette det tekniske problemet de står over. Dersom dette ikke er mulig vil de bemanne trafostasjonene manuelt (så sant de har folk og kapasitet til å gjøre det) for å sørge for at kraftforsyningen kommer raskest mulig på plass. Deretter vil de avgi rapport til NVE om hendelsen. Det er også tenkelig at NVE på et tidligere tidspunkt kan komme inn og gi anbefalinger.

Ved et villet angrep vil selskapet varsle politiet, som sender rapport til PST. Selskapet sender kopi til NVE om at forholdet er anmeldt. I kraftsektoren skjer det små tekniske hendelser opptil 2 ganger i timen, og kun alvorlige feil rapporteres videre.

[14] Ref. samtale Torstein Schjerven, Datakrimavdelingen (Nye Kripos), 11.08.05.

NVE fører en oversikt over villede og tekniske feil, og de ser også på tidsperspektivet og omfanget av hendelsen, hvilket innebærer at tid og geografi er viktig.

*Angrep/svikt på prosesskontrollsystem i oljesektoren*
Hvis man lammer prosesskontrollsystemet i for eksempel et oljeselskap, vil dette varsle Petroleumstilsynet (Ptil), som igjen varsler Oljedirektoratet (OD). Ptil blir varslet av HMS-hensyn (helse, miljø og sikkerhet). OD blir varslet fordi produksjonen stopper, noe som vil gå ut over leveransen, og derigjennom norsk økonomi. OD er ikke operative, men mottar informasjon og videresender informasjon til Olje- og Energidepartementet (OED).

Operatørselskapene har gode rutiner for varsling. Oljeselskapene håndterer selv feil/brudd på oljeledninger. Men de har i tillegg Gassco, som er et offentlig selskap som styrer og koordinerer leveransen av gass. Det skal mye til for at OED får koordineringsansvar, og man snakker da om leveransesvikt på over 10 dager.

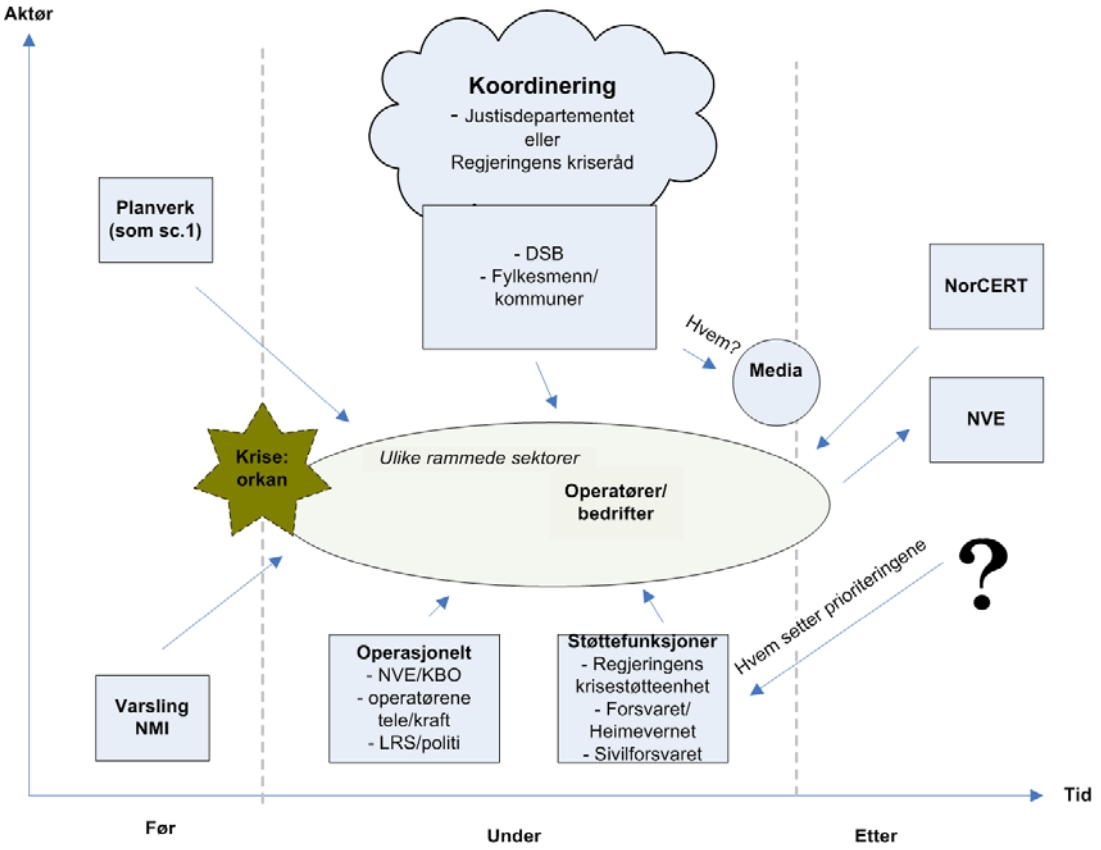
## 5.2 Scenario 2 - Krisesituasjon med ”naturlig årsak”

Scenario 2 er som følger:

> ”Sterk vind forårsaker brudd i kraftsystemet, som igjen forårsaker svikt i tele og IKT-systemer (kraftbrudd og nedblåsing av antenner etc.). Når kraft, tele og IKT faller ut oppstår det kaos og allmenn uro fordi grunnleggende rettigheter (strøm, varme, mat) og verdier (informasjon) rammes.”

Dette scenariet tar for seg en typisk naturkatastrofe, som rammer et større område. Her er det tatt høyde for de samme tids- og områdeavgrensingene som i scenario 1. På grunn av scenariets art, vil dette skille seg ut fra det første ved å ha utspring i et annet årsaksforhold, som kan påvirke hvilke aktører som blir involvert i krisehåndteringen. Scenario 2 lammer også flere aktører samtidig, ikke bare en virksomhet.

Figur 5.2 danner utgangspunkt for å diskutere aktørene og deres roller i dette scenariet.




*Figur 5.2 – Hendelsesforløp scenario 2*

### 5.2.1 Før krisen: varsling

På samme måte som beskrevet i kapittel 5.1.1 må et system for planverk og varsling være på plass. Planverket vil være av samme art som scenario 1, men varslingen vil initieres av værvarsling fra Det Norske Meteorologiske Institutt (DNMI). Et viktig punkt som vil inngå i planverket for kraftbransjen er å sørge for at man har nok personell tilgjengelig for å styre kraftsystemet manuelt, uten støtte fra driftssystemene. NVE kan sette kompetansekrav til virksomhetene om at de skal være i stand til dette, men det er selskapene selv som er ansvarlige for å sørge for at de har tilstrekkelige ressurser.

NVE kan ha en rolle i forbindelse med å varsle videre til virksomheter i kraftbransjen dersom de får beskjed om at naturkatastrofer er på vei. De har imidlertid ikke et formelt varslingsansvar, og virksomhetene vil selv motta værvarsel fra DNMI.

Noe som ikke ble nevnt i intervjuene eller på workshopen, men som kan tenkes å være en mulig oppgave i forbindelse med forutsette naturkatastrofer, er å sende ut en generell varsling til befolkningen, og særlig til de med kritisk infrastruktur. På denne måten vil man kunne forberede seg i forhold til reserveløsninger og alternative måter å fungere på, som for eksempel påfyll av

aggregater, utskrift av nyeste beredskapsplaner og alternative betalingsmåter[15].

### 5.2.2 Under krisen: koordinering og operasjonelt ansvar

Følgende aktører kan tenkes å bli involvert på dette stadiet:

- **Operasjonelt:** virksomhetene/operatørene som rammes, NVE/KBO, LRS/politi
- **Koordinering:** Regjeringens Kriseråd, JD og evt. DSB, Fylkesmenn/kommuner
- **Støttefunksjoner:** Regjeringens Krisestøtteenhet, Forsvaret/Heimevernet, Sivilforsvaret

*Operasjonelt*
De tekniske problemene må håndteres av operatørene selv, enten de tilhører tele- eller kraftbransjen[16]. Samarbeid mellom teleselskaper og kraftleverandører foregår på lokalt nivå. Telenor har for eksempel lokale kontakter med de ulike kraftleverandørene for å holde seg underrettet om hvor langvarig det er forventet at strømbruddet blir.

For å få løst kraftproblemet i denne krisen vil NVE ha en rolle. De har et tett samarbeid med Fylkesmannen, men samtidig en god oversikt over hele kraftbransjen. På denne måten kan de koordinere mellom fylker dersom flere fylker er involvert.

NVE sin rolle er å ansvarliggjøre enhetene nedover i Kraftforsyningens beredskapsorganisasjon (KBO)[17], som selv er ansvarlige for å utføre det fysiske reparasjonsarbeidet. Det skal mye til for at det formelle beredskapssystemet knyttet til KBO settes i gang, men i praksis vil man kunne følge mange av de samme prinsippene som ligger i KBO, som blant annet informasjonslinjer. NVE kan gi anbefaling til OED om å aktivere KBO-systemet, og dette skjer i så fall fort dersom det er et behov for det.

Dersom det er fare for liv og helse vil politiet ha fullmakt til å handle raskt og sette inn nødvendige ressurser. Det vil etableres en lokal redningssentral (LRS)[18], der Fylkesmannen får status som rådgiver under krisen. På det tidspunktet der faren for liv og helse er over, vil Fylkesmannen ta over etter Politiet. Dette skjer dersom krisen blir langvarig og det blir et behov for å omfordele ressurser.

Noe som ikke er tegnet inn i figuren er et eventuelt samarbeid til utlandet, dersom man har behov for supplerende utstyr. I *teorien* skal forespørsler om utstyr gå via Justisdepartementet til UD, som tar kontakt med tilsvarende departement i utlandet. I praksis finnes det snarveier her;

---

[15] Et generelt problem er at folk flest er lite informert om mulige konsekvenser, noe som ble vist med et eksempel fra DSB: mange *vet* ikke at mobilnettet slåes ut dersom strømmen går, og de har derfor ikke tenkt på alternative løsninger for kommunikasjon.
[16] Som et eksempel kan vi se på Statnetts mulige gjøremål i et slikt scenario. Statnett ville her forsøkt å sørge for manuell bemanning på trafostasjonene og sette inn reservemaster. Ettersom scenariet rammer flere fordelingsnett, ville Statnett kun kontaktet NVE som får rollen med å koordinere mellom kraftleverandører. NVE vil også ta seg av all kontakt mot politi og fylkesmann og andre som blir involvert. For Statnett isolert vil kontakten utad kun involvere NVE, i tillegg til at de må sørge for god intern organisering for å komme i orden.
[17] KBO (Kraftforsyningens beredskapsorganisasjon) er bygget med tanke på krigens krav, men kan tenkes å brukes i "sivile kriser". For mer informasjon om organiseringen i KBO – se http://www.nve.no/modules/module_109/publisher_view_product.asp?iEntityId=5802
[18] Terskelen for å opprette LRS i Oslo er svært høy, og det har ikke skjedd siden Scandinavian Star-ulykken i 1990.

eksempelvis har ulike tilsynsmyndigheter på norsk side etablert en direkte kontakt med tilsvarende myndigheter i Sverige.

*Koordinering*
I figuren ser man en sky av koordinerende myndigheter, heretter kalt "koordineringsskyen". I den øverste delen av skyen har man de mest overordnede koordineringsorganene som får ansvar på øverste hold, enten det blir JD eller lederdepartementet i Regjeringens kriseråd.

I boksen under koordineringsskyen er DSB og kommuner/fylkesmenn satt opp. Disse aktørene vil ha en rolle i denne krisen, uansett hvem som koordinerer på øverste nivå. DSB sin rolle vil være å fungere som en "kommunikasjonssentral" mellom JD og Fylkesmannen. DSB vil også ha en rådgivende rolle i forhold til JD, og vil ved behov delta i koordineringsarbeidet.

Fylkesmannen fungerer som et bindeledd mellom DSB og kommunene. Fylkesmannen har et samordningsansvar mellom kommunene og skal koordinere ressursbruken. Dette ansvaret vil imidlertid bli overført til JD dersom krisen får konsekvenser for flere enn ett fylke, eller dersom det utvikler seg til å bli et nasjonalt problem.

*Støttefunksjoner*
Regjeringens Krisestøtteenhet er satt opp som en støttefunksjon i en krisesituasjon[19]. Støttefunksjonene vil i dette bildet være nødvendige for å sørge for opprydning og muliggjøre gjenoppretting av systemene. Sivilforsvaret vil kunne bistå nød- og redningsetatene, med for eksempel evakuering og informasjonsarbeid[20]. Sivilforsvaret er direkte underlagt DSB, og DSB vil dermed få en rolle også her. Ettersom scenariet beskriver at det "er mye kaos og allmenn uro", vil Heimevernet kunne komme inn med støttefunksjoner, som for eksempel å dirigere trafikken. Forsvaret kan også få en rolle ifm. vakthold og sikring[21]. Post- og Teletilsynet kan som i scenario 1 bistå med vurdering av alternative sambandsløsninger.

For å kunne prioritere og dra nytte av støttefunksjonene, er det viktig at det foreligger klare ansvarslinjer på hvem som skal foreta nødvendige beslutninger. Hvem som foretar prioriteringene på ulike områder synes å være noe uklart. Et problem oppstår for eksempel ved sektorvis utkobling av strøm, på grunn av konkurrerende interesser og på grunn av hvordan infrastrukturen fysisk er bygget opp (de samme strømlinjene forsyner både private husholdninger og kritiske infrastrukturer, som for eksempel sykehus). Under workshopen ble det referert til en øvelse der det viste seg umulig å foreta prioritering av strøm innenfor Ring 2 i Oslo. For å få løst noen av disse utfordringene er det nødvendig å gjennomføre storskalaøvelser, som vil bli beskrevet nærmere i diskusjonskapittelet.

For telesektoren vil PT ha myndighet til å prioritere ressurser hos teleoperatørene, for å sikre samsvar med prioritering gitt av overordnet myndighet (i dette scenarioet via SD).

[19] For mer info om Regjeringens Krisestøtteenhet se tidligere beskrivelse i kapittel 4.
[20] Det er etablert fem sivilforsvarstiltak: Varsling, tilfluktsrom, krigsutflytting/evakuering, hjelpestyrker, informasjon. For mer informasjon, se www.sivilforsvaret.no
[21] Dette skjedde blant annet i Sverige under kraftbruddet ved Gudrun-stormen tidligere i år.

*Media*
Som beskrevet i scenario 1 vil media ofte være med på å definere krisen. I et scenario som dette vil flere sektorer være involvert i krisen, og dermed mange aktører. Hvem som får ansvar for å håndtere media avhenger av om Regjeringens kriseråd trer sammen eller ikke. Når dette rådet er fullt operasjonelt, vil det ha en egen kriseinfoenhet som får mediaansvar. Per i dag ligger dette informasjonsansvaret hos JD. Medias rolle med å få informasjon ut til befolkningen vil i et slikt scenario bli redusert vesentlig, på grunn av manglende strøm. Dette vil imidlertid kun gjelde de områdene som er berørt av krisen, og for alle andre vil media fortsatt ha en sentral rolle.

### 5.2.3 Etter krisen: gjenoppretting og oppfølging

De enkelte virksomhetene som har blitt rammet av orkanen, vil selv være ansvarlig for å sørge for opprydning og gjenoppretting av systemene, samt for å rapportere til tilhørende myndighet.

*Gjenoppretting av datasystemer*
Når strømmen har vært borte over lang tid, viser det seg at man kan få problemer med å gjenopprette datasystemene. Virksomhetene og deres tjenesteleverandører vil primært ha et ansvar for gjenoppretting. I tillegg kan det være overordnede problem med prioritering av rekkefølge for gjenoppretting, for eksempel hos ISPer med tjenesteleveranser til to eller flere autonome virksomheter. PT har her samme mulighet til myndighetspålegg rettet mot tilbydere av offentlige datakommunikasjonsnett på linje med de offentlige telenett. En nasjonal koordineringsfunksjon som NorCERT kan bistå i den forutgående prioritering innen offentlig sektor. Et eksempel på slik bistand kan være å hjelpe til med å koordinere mellom ISPer hvis de har problemer, eller assistere i prioriteringen av systemer (f.eks. internettnoder) som skal gjenopprettes.

*Rapportering*
På samme måte som i scenario 1, vil kraftleverandørene måtte rapportere til NVE i etterkant av krisen. Dette på grunn av gjennomgang av regelverk, for å se om noe bør endres på. Kraftbransjen er veldig avhengig av samband og har derfor et eget reservesamband som er uavhengig av kommersielle nett. Likevel ser de en trend mot økt bruk av mobiltelefoni, ettersom dette er mer lettvint. Ettersom mobilnettet ved strømstans vil bli utilgjengelig etter kort tid, gjør de seg også mer sårbare.

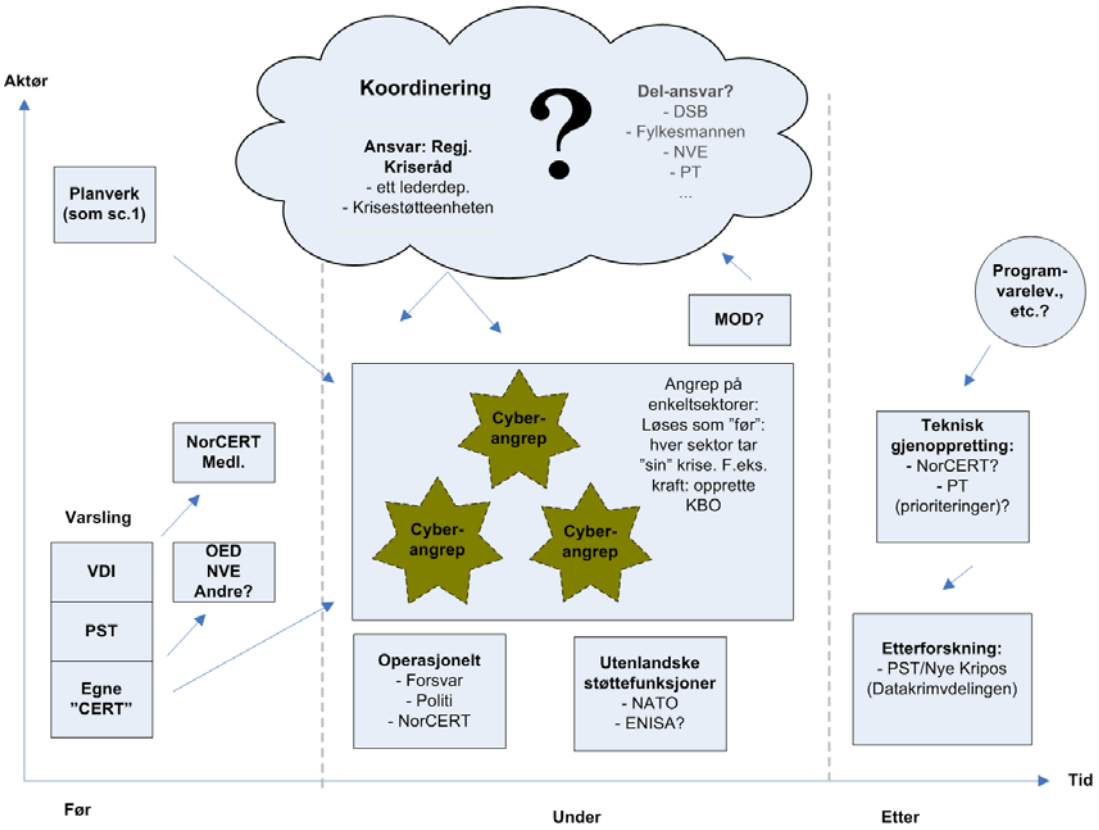
I telesektoren vil driftsavbrudd som følge av kraftutfall og linjebrudd i stor skala utløse samme rapportering til PT og SD som beskrevet for scenario 1 ovenfor.

## 5.3 Scenario 3 - Sikkerhetspolitisk krise

Scenario 3 er som følger:

> ”Det er stortingsvalg i Norge om to måneder. Norge har sendt 1500 soldater til den internasjonale sikkerhetsstyrken i Afghanistan (ISAF). Det gjennomføres gjentatte og rullerende angrep på enkeltsektorer med bruk av ulike midler:
>
> - Et cyberangrep initieres mot Jernbaneverket klokken 1600 en ukedag og slår ut togtrafikken ca 1 - 2 timer. Angrepet gjentas de påfølgende dagene til samme tid, og skaper frykt og uro.
> - Cyberangrep dels kombinert med angrep på de fysiske kommunikasjonsveiene mot Oslo kontrollsentral Røyken. Kommunikasjon med omverdenen settes ut av drift i lenger perioder.
> - Også i kraftsektoren oppdages det gjentatte tilfeller av cyberangrep
> - Trussel på Internett om at det er plassert masseødeleggelsesvåpen på norsk grunn som vil bli benyttet dersom Norge ikke trekker de militære styrkene ut av Afghanistan.”

Figur 5.3 danner utgangspunkt for å diskutere aktørene og deres roller i dette scenariet.




*Figur 5.3 – Hendelsesforløp scenario 3*

Scenario 3 er et typisk eksempel på en situasjon der mange sektorer blir involvert på samme tid. Her gjennomføres det cyberangrep som lammer ulike samfunnsfunksjoner i perioder, og med gjentatte angrep på mange sektorer.

### 5.3.1 Før krisen: varsling

På varslingssiden kan det komme inn flere mulige aktører, som vist til venstre i figur 5.3. VDI vil kunne ha en viktig rolle, ettersom de kan detektere koordinerte angrep (mot flere sektorer/aktører), så sant de har sensorer plassert i de virksomhetene det skjer angrep. VDI vil sammen med NorCERT varsle tilknyttede medlemsbedrifter. De vil samtidig forsøke å finne kilden og sjekke om det har vært lignede angrep på virksomheter i samme eller andre sektorer.

PST vil gi en vurdering om gjeldende trusselnivå i Norge til aktører som blant annet OED og NVE. I tillegg kan enkelte virksomheter ha etablert egne ”CERT-er”, eller være knyttet til kommersielle varslingstjenester.

### 5.3.2 Under krisen: koordinering og operasjonelt ansvar

Det overordnede problemet i dette scenariet er å definere hvem som *eier* krisen. Likevel henviser flere av aktørene som har blitt intervjuet til at hvert cyberangrep skal håndteres i den sektoren det oppstår. Scenariet i seg selv er stort og uoversiktlig, men ved å bryte det ned kan man plassere ansvar for håndtering der de ulike krisene inntreffer. Følgende aktører kan tenkes å bli involvert på dette stadiet:

- **Operasjonelt:** de enkelte virksomhetene som rammes, NorCERT, Forsvar, Politi.
- **Koordinering:** Regjeringens Kriseråd
- **Del-ansvarlige:** NorCERT, DSB, Fylkesmannen, NVE, PT
- **Utenlandske støttefunksjoner:** NATO, ENISA

*Operasjonelt*
Som beskrevet i de to foregående scenariene vil virksomhetene selv forsøke å løse problemene etter hvert som de oppstår. Politiet og Forsvaret vil kobles inn på samme måte som i scenario 1 og 2, selv om det her kan forventes at Politiet vil komme raskere på banen. NorCERT vil også kunne bistå med teknisk bistand, blant annet via sitt kontaktnettverk internasjonalt[22].

*Koordinering*
Dette er et scenario der man kan forvente at Regjeringens kriseråd vil tre sammen, og at dette vil skje tidlig dersom man skjønner at det er snakk om målrettede angrep som kan knyttes til utplasseringen av styrker i Afghanistan. Utfordringen blir imidlertid å utpeke et lederdepartementet, ettersom krisen er sektorovergripende. Under workshopen på FFI ble det hevdet at dette sannsynligvis ville ende opp i en diskusjon mellom JD og FD om når JD ikke lenger skal eie krisen, dvs. at det forventes en omfattende dialog mellom det militære og sivile. JD vil i utgangspunktet få dette ansvaret pga. deres samordningsansvar på sivil side under kriser.

[22] Se diskusjon under kap. 5.1.2

Et spørsmål er hvilken rolle Moderniseringsdepartementet (MOD) vil ha i forhold til JD og Regjeringens kriseråd. Dette er en diskusjon som like gjerne kunne vært plassert under scenario 1 eller 2, men på grunn av at dette mest direkte berører cyberangrep og kriser via Internett, er det relevant å inkludere denne diskusjonen her. MOD var kun så vidt nevnt i forkant av workshopen, ved at enkelte aktører trodde de ville ha en rolle med å håndtere IKT-kriser på grunn av sin rolle med å koordinere nasjonal IT-politikk. Andre mente at det ikke ville være naturlig at MOD kommer inn her:

> ”I dette scenariet er det terror som er problemet, og ikke IKT; man gir ikke ansvaret til de som lager sprengstoff selv om en bombe eksploderer”

Dersom det blir aktuelt at Regjeringens kriseråd trer sammen, kan likevel MOD få en rådgivende funksjon i rådet.

I forhold til trusselen om masseødeleggelsesvåpen ble det også reist spørsmål om tiltak i Sivilt beredskapssystem vil bli satt i verk. Dette vil være avhengig av hvor konkret trusselen er. Dersom det foreligger konkret etterretningsinformasjon på hvor trusselen kommer fra, vil dette kunne skje.

*Delansvarlige*
På lavere koordineringsnivå kan man forvente at KBO blir opprettet. I så fall vil det foregå et tett samarbeid mellom NVE og systemansvarlig Statnett. De øvrige selskapene vil vente på ordre.

PT har ikke hatt en operativ rolle i de tidligere scenariene, men vil få det dersom Sivilt Beredskapssystem (SBS) tas i bruk. DSB og Fylkesmannen vil ha tilsvarende roller som i de to foregående scenariene.

*Utenlandske støttefunksjoner*
Ettersom det her blir snakk om en sikkerhetspolitisk krise, vil det være sannsynlig at det trekkes inn mange ressurser, både fra inn- og utland. Forsvaret vil komme inn på et tidlig stadium, og NATO er en ressurs som kan bli trukket inn dersom det er snakk om et *angrep* på Norge. I henhold til Washington-traktatens artikkel 5 er det mulig for et medlemsland som er angrepet av et tredjeland, å påkalle de andre medlemmenes støtte (13). Dette har kun skjedd én gang tidligere (USA etter terrorangrepene 11. september 2001). Mer sannsynlig er det at man vil benytte seg av den ekspertise og informasjonssamling som kan ligge i NATO CIRC (Computer Incident Response Capability), og benytte dette materialet til en sammenlikning for å få bukt med angrepets utspring.

Utenriksdepartementets (UD) ansvarsområde er begrenset til å beskytte nordmenn overfor utenlandske myndigheter, personer og institusjoner (14). I tilfeller av terrorvirksomhet, spionasje og sabotasje foreligger det en trussel mot nasjonale sikkerhetspolitiske interesser og befolkning (15), og det kan være naturlig at Utenriksdepartementet får en rolle som

kommunikasjonskanal mot det landet eller institusjonen(e) som er ansvarlig(e) for en slik handling, så langt dette er mulig å fastsette. UD har også fast plass i Regjeringens kriseråd. På arbeidsmøtet ble en eventuell rolle for UD ikke videre kommentert, men i intervjuer kom det frem at UD bør ha en rolle i scenario 3 dersom masseødeleggelsesvåpen på noen måte er involvert.

EUs ENISA (European Network and Information Security Agency)[23] vil kunne få en rolle i en IKT-krise *på sikt*, om ikke annet som et informasjonsknutepunkt for varslingssystemer og standarder og med oversikt over tilgjengelig teknisk assistanse som befinner seg i medlemslandene i EU. ENISAs rolle vil sannsynligvis være mer fremtredende med tanke på tekniske innspill til EU-kommisjonen om nye forordninger og direktiv med hensyn til for eksempel beredskapsplaner og minimumsstandard på sikkerhet. ENISA vil slik kunne påvirke medlemslandenes lovgivning indirekte.

### 5.3.3 Etter krisen: gjenoppretting og oppfølging

I en gjenopprettingsfase vil PT kunne styre tilbydere innen post- og telesektoren i en myndighetsrolle med koordinering og prioritering. Dersom flere sektorer er involvert, må andre aktører involveres, for eksempel Fylkesmannen. PT har øvd på å ha en operativ rolle. Erfaringer fra en tidligere øvelse viser at PT kan være hensiktsmessig som koordineringsorgan for alle teleoperatørene i en gjenopprettingsfase. Dette kan da skje via en eventuell ”TERT” (Telecom Emergency Response Team) for telesektoren.

NorCERT og Politiet, ved PST og Datakrimavdelingen, vil komme inn med samme rolle som beskrevet tidligere, og i tillegg vil programvareleverandører/ underleverandører være sentrale i arbeidet med å få systemene til å fungere igjen.

## 5.4 Oppsummering

En felles problemstilling for alle scenariene er å avgjøre på hvilket tidspunkt myndighetene (på departementsnivå) griper inn og koordinerer. En av deltakerne på arbeidsseminaret uttrykte at:

> ”Tiltakene (mottiltakene mot angrepene etc.) starter anarkisk – *etter hvert* vil man koordinere”

Dette tilsier at det er vanskelig å peke på absolutte kriterier som gjør at departementene blir involvert. Dette kan avhenge av flere forhold, for eksempel antall sektorer som berøres, hvor stor del av befolkningen som er rammet og om krisene er akutte. Det vil si at man må vurdere opprettelse av for eksempel Regjeringens Kriseråd fra situasjon til situasjon.

I scenario 2 og 3 vil det sannsynligvis gå kortere tid før departementene ser behovet for å koordinere seg, ettersom flere sektorer blir involvert. Jo større omfang det er på krisen, desto

[23] ENISA ble opprettet i 2004 for å samordne og fremme IKT sikkerhet for EU-institusjonene og medlemslandene, og vil også ha en rolle ovenfor private og offentlige bedrifter. Se for øvrig kapittel 5.3 og utover.

flere aktører vil bli involvert i håndteringen av denne. I scenario 1 som har blitt betegnet som en sektorkrise, vil myndighetene i større grad bli ”tilskuere”. Først dersom krisen eskalerer vil myndighetene gripe inn og få et koordineringsansvar, noe NVE[24] uttrykte ved følgende eksempel:

> ”I scenario 1 og 2 vil bransjen måtte håndtere det selv på best mulig måte. NVE vil fungere som rådgiver, men problemene vil løses av selskapene selv. Ved scenario 3 vil NVE ta over styringen, og man kan forvente at KBO formelt blir etablert som system. I et slikt scenario kan man ikke forvente at aktørene selv skal kunne håndtere dette. Det enkelte selskap er ikke dimensjonert for cyberangrep av en slik skala.”

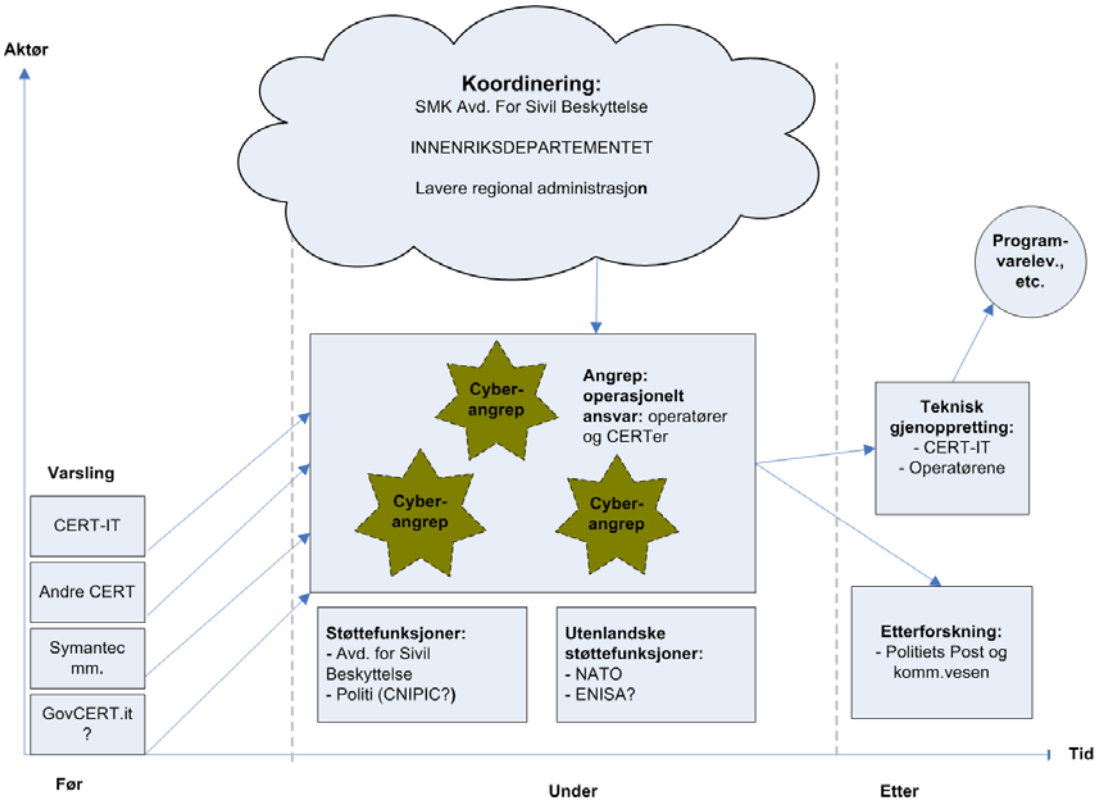
Under arbeidsseminaret på FFI ble det uttrykt bekymring rundt underleverandører til virksomheter med samfunnskritiske funksjoner, ettersom én og samme underleverandør ofte bidrar med systemer til mange kritiske funksjoner. Dermed vil feil hos én underleverandør kunne påvirke mange ulike sektorer. Det er derfor et stort behov for å identifisere og følge opp slike viktige underleverandører, og hvilke beredskapsrutiner som eksisterer i disse. Dette er særlig et problem i forbindelse med outsourcing. Et eksempel som ble nevnt var outsourcing av kraft, der det kan ende opp med at alle e-verk benytter tjenester fra de samme underleverandørene.

Generelt for alle scenariene er at Forsvaret normalt ikke vil ha noen rolle før dette vedtas av Regjeringen. Forsvaret har ingen mulighet til å på eget initiativ tre inn i det sivile systemet, og det er derfor veldig viktig at det foreligger en beslutning fra høyt hold. På IKT-siden kan Forsvaret i noen grad være med å understøtte den kapasiteten som blir borte, som for eksempel bistå med samband. Det må likevel understrekes at slik støtte kun kan gis til et fåtall brukere, typisk blant ledelsesapparatet på sivil side.

## 6 PRAKSIS FOR IKT-KRISEHÅNDTERING I ANDRE LAND

Det er ulik praksis for organiseringen av IKT og sikkerhet i de europeiske land. I mange land er det et eget innenriksdepartement som er ansvarlig for nasjonal sikkerhet, og i noen land er kriseberedskapen samlet under Statsministerens Kontor. I dette kapittelet vil vi se på hvordan en IKT-krise på nasjonalt nivå vil bli taklet i andre europeiske land, nærmere bestemt Italia og Frankrike. Det tas utgangspunkt i en ”scenario 3”- type krise for å sammenlikne håndteringen i disse landene med gjeldende praksis i Norge. Se forøvrig figur 6.1 for en skisse over aktører og roller.

[24] Ref. møte med NVE, 26.07.05




*Figur 6.1 Håndtering av IKT-krise i Italia*

Forskjellene i håndteringen av IKT og kriseberedskap i de europeiske landene gjenspeiles i utfordringen med å enes om en felles europeisk standard i EU. En oversikt over EUs initiativ innen IKT-beredskap vil derfor bli presentert i avslutningen av kapittelet. Innledningsvis vil ulike aktørers rolle i en krisesituasjon presenteres. For bakgrunns- og tilleggsinformasjon om de ulike aktørene, se appendiks A.2 og A.3.

I underkapittelet om Italia presenteres et sannsynlig handlingsmønster og relevante aktører i tilfelle en IKT-krise rammer Italia på nasjonalt nivå. Det pekes på noen områder der italiensk organisering kan gi innspill til norsk organisering av IKT-beredskap. Avslutningsvis nevnes Italias håndtering av Tsunamikatastrofen i Sørøst-Asia i 2004 som et eksempel på velorganisert kriseberedskap, om enn på et annet område enn IKT.

## 6.1 Hva skjer ved en IKT-krise i Italia?

### 6.1.1 Før krisen: varsling

I dag kommer det meste av varsling via italienske CERT-er, eller via bedriftens egen innsamling av informasjon fra for eksempel Trend, Microsoft og Symantec. De ulike CERT-ene er foreløpig ikke organisert i en nasjonal CERT. I dag benytter offentlig administrasjon og private aktører seg i hovedsak av den statsautoriserte *CERT-IT*, opprettet ved Universitetet i Milano i 1994 som en non-profit organisasjon[25]. Politiet og Forsvaret har også egne CERT-er som

[25] *CERT-IT* ledes av Professor Danilo Bruschi, og arbeidet med datainnsamling utføres av studenter ved universitetet"Politecnico di Milano".

overvåker trafikk på Internett og gir anbefalinger til mottiltak, og det er en egen CERT for akademia og forskningsmiljøene[26].

To initiativ er i ferd med å realiseres: for det første er det i ferd med å bli etablert en nasjonal CERT (*GovCERT.IT*[27]) underlagt minister uten portefølje Lucio Stanca[28], og samtidig arbeides det innen Innenriksdepartementet med å sette opp et eget senter for beskyttelse av kritisk infrastruktur, som også vil få en varslingsfunksjon for IKT.

Det er foreslått at den nasjonale CERT-en, GovCERT.IT, skal ha en bred varslingsfunksjon på sikt og at overvåking (aktiv og passiv) skal utføres hos offentlige myndigheter og andre utvalgte aktører (16). Enheten er tildelt et budsjett og vil i henhold til planen utvides fra seks til 15 ansatte i løpet av "kort tid"[29]. Det diskuteres om *GovCERT.IT* bør etableres som et eget direktorat, fordi det da vil være i tråd med trenden i EU og at det vil bli lettere å få tildelt ressurser samt å kunne utvide arbeidsområdet til å inkludere for eksempel simulerte øvelser[30]. Det eksisterer ikke noe formelt samarbeid mellom offentlig og privat sektor per i dag, men dette er satt opp som ett av GovCERT.IT's foreslåtte mål[31].

Politivesenet, underlagt Innenriksdepartementet, er siden 1992 ansvarlig for cyberkriminalitet, og deres "avdeling for post og kommunikasjon" ("Servizio Polizia postale e delle communicazioni") skal i løpet av september 2005 sette opp et "Nasjonalt senter for beskyttelse av kritisk infrastruktur" (CNIPIC[32]). Senteret skal representere alle kritiske infrastrukturer, deriblant IKT, og skal både overvåke, varsle og nøytralisere cyberangrep og andre villede angrep (terrorisme og sabotasje)[33].

Det kan diskuteres hvordan forholdet vil bli mellom GovCERT.IT og CNIPIC når begge organene blir operative, og det hevdes at det er en viss maktkamp mellom Statsministerens Kontor (SMK) og Innenriksdepartementet når det gjelder hvilken enhet som skal være den nasjonale varslings- og responsenheten[34]. Privat sektor har tradisjonelt sett ikke vært opptatt av IKT-sikkerhet, og det er uklart om dette vil bedres ved opprettelsen av en nasjonal

---

[26] For mer informasjon om de ulike CERT'ene i Italia, se utfyllende informasjon i appendiks A.2 om aktørene i Italia.
[27] Det skal presiseres at navnet til den nye nasjonale CERT'en ennå ikke er offisielt.
[28] Minister uten portefølje Lucio Stanca er ansvarlig for området Teknologi og Innovasjon i regjeringen. GovCERT.IT vil ligge organisatorisk under senteret for IKT i offentlig administrasjon, (Centro Nazionale per l'Informatica nella Pubblica Amministrazione, CNIPA), som er underlagt Minister Stanca.
[29] Ref. telefonintervju med Claudio Manganelli, CNIPA og Nasjonal Teknisk Komité for IKT i offentlig sektor, 30.08.05.
[30] Ref. telefonintervju med Claudio Manganelli, CNIPA og Nasjonal Teknisk Komité for IKT i offentlig sektor, 30.08.05.
[31] Ref. telefonintervju med Alessandro Bonomi (ISCOM), 2.08.05.
[32] CNIPIC: "Centro Nazionale di Protezione delle Infrastrutture Critiche". Senteret er formelt innstiftet men ikke operativt ennå. Ref Telefonintervju Roberto Setola, (Arbeidsgruppe for Beskyttelse av Kritisk IKT-infrastruktur), 1.09.05.
[33] Telefonintervju med Dr. Caroselli, Politiets Post og Kommunikasjonsvesen, 18.08.05.
[34] Ref. telefonintervju med Claudio Manganelli, CNIPA og Nasjonal Teknisk Komité for IKT i offentlig sektor, 30.08.05.

varslingsenhet, og om det vil føre til et bedre samarbeid mellom offentlig og privat sektor[35].

### 6.1.2 Under krisen: koordinering og operasjonelt ansvar

*Koordineringsansvar*
Det er i hovedsak Innenriksdepartementet som er ansvarlig i tilfelle nasjonal krise[36]. Dersom krisen er svært alvorlig og går ut over befolkningens liv og helse vil Avdeling for Sivil Beskyttelse under SMK raskt kunne tre sammen og ta over koordineringsansvaret.

I en nasjonal IKT-krise vil det være sannsynlig at Innenriksdepartementet, etter hvert ved Politivesenets nye CNIPIC-senter, kan ta på seg en rolle som "operasjonssenter"; et forum for samordning av de videre trinn i krisehåndteringen[37]. Dersom IKT-krisen eskalerer, og det er fare for liv og helse, vil Avdelingen for Sivil Beskyttelse under SMK[38] ta over det generelle koordineringsansvaret under krisen. Det er denne avdelingen som utpeker lederdepartementet, som så delegerer ansvar nedover. Selve operasjonene delegeres raskt ned til lavest mulig nivå etter nærhetsprinsippet.

Nærhetsprinsippet tilsier at den som har hovedansvaret for sivilt beredskap på laveste organisatoriske nivå, det vil si kommunens ordfører, skal ta ansvar for operasjonene lokalt. Ordføreren organiserer kommunale ressurser etter forhåndslagte planer for kriseberedskap. Erfaring fra naturkatastrofer i Italia tilsier at det raskt blir avklart om man er i stand til å håndtere krisen lokalt, om man må involvere høyere nivå (regionen og fylket) eller ta det opp på nasjonalt nivå. Det politiske ansvaret taes direkte av Statsministeren[39].

*Operasjonelt ansvar*
Det operasjonelle ansvaret i en krise ligger i første omgang hos operatørene selv. CERT-ene er i Italia som regel både varslings- og responsenheter, og vil kunne assistere operatørene og de rammede aktørene med teknisk kunnskap og ressurser. CNIPIC-senteret planlegger å kunne være delaktig i den operasjonelle delen av en krise, og har som politienhet fått utvidet mandat gjennom den nye "anti-terrorloven" av 27 juli 2005[40].

Rollen til SMK Avdeling for Sivil Beskyttelse er *bredere* enn den som vil gjelde CNIPIC. Professor Danilo Bruschi, leder av CERT-IT og medlem i Nasjonal teknisk komité for beskyttelse av kritisk IKT infrastruktur, poengterer at CNIPIC vil ta spesifikt hensyn til de *kritiske infrastrukturer*, mens Avdeling for Sivil Beskyttelse har fokus på beskyttelse av *liv og*

---

[35] Offentlig sektor kan se ut til å være bedre organisert enn privat sektor på grunn av erfaringer med nasjonal og internasjonal terrorisme. Det er generelt utvist liten påpasselighet med hensyn til å sette sikkerhetskrav når man outsourcer tjenerster eller privatiserer bedrifter. Se appendiks A.2 om aktørene i Italia for andre kommentarer, samt rapporten ISCOM (2005) *"La Sicurezza delle Reti: dall'analisi del rischio alle strategie di protezione"*, side 86.
[36] Elektronisk kommunikasjon fra Danilo Bruschi, leder av CERT-IT og medlem i blant annet Nasjonal teknisk komité for beskyttelse av kritisk IKT infrastruktur, 4.08.05.
[37] Telefonintervju med Dr. Caroselli (Politiets Post og Kommunikasjonsvesen), 18.08.05
[38] Statsministerens Kontor er i Italia ikke bare en rent administrativ enhet underlagt Statsministeren. Det finnes også tverrsektorielle grupper og avdelinger organisert under SMK som arbeider med spesifikke og begrensede tema.
[39] SMK Avdeling for Sivil Beskyttelse, http://www.protezionecivile.it/sistema/index.php
[40] Innenriksdepartementet (2005): *"decr.legge 144/24 juli 2005, art. 7bis"*

*helse*. Det kan diskuteres hvorvidt Avdelingen for Sivil Beskyttelse i det hele tatt kan spille en rolle i den operasjonelle delen av en IKT-krise, på grunn av krisens tekniske karakter. SMK Avdeling for Sivil Beskyttelse er tidligere kun benyttet i forbindelse med naturkatastrofer som jordskjelv og epidemier, men det er sannsynlig at de kan opptre med en støttefunksjon dersom IKT-krisen fører til kaos og tilstander der det for eksempel er behov for rydding av veier og skinneganger[41].

Avdelingen for Sivil Beskyttelse er i dag i ferd med å gå gjennom en omstilling for å bedre kunne ta høyde for andre typer scenarier, så som en IKT-krise og dens mulige konsekvenser[42]. Omstillingen kommer som et resultat av økt bevisstgjøring etter strømutfallet 28. september 2003, der kritiske samfunnsfunksjoner ble satt ut av spill. En blackout med utspring i Sveits forårsaket store problemer i hele Italia, med unntak av Sardinia. Kommunikasjonssektoren ble hardt rammet da nødstrømskapasiteten ikke strakk til over tid, og det ble tatt i bruk satellittelefoni og manuell utkjøring av personale for å gjenopprette kommunikasjonssystemet[43].

Det italienske forsvaret vil ha en rolle dersom et militært angrep er årsaken til IKT-krisen.

### 6.1.3 Etter krisen: gjenoppretting og oppfølging

*Gjenoppretting*
Gjenopprettingen etter en nasjonal IKT-krise vil i første rekke være operatørenes ansvar, med assistanse fra CERT-ene og eventuelt fra CNIPIC når dette blir operativt. Dersom krisen rammer befolkningen, kan Avdelingen for Sivilt Beredskap få en rolle.

Organiseringen av frivillige har tradisjonelt spilt en stor rolle i Italia. Siden 1960-tallet har kvinner og menn frivillig organisert seg for å "gi en hjelpende hånd" under kriser. Italia har vært rammet av flere alvorlige ulykker, så som snøskred og jordskjelv. 2.500 organisasjoner er listet blant Avdelingen for Sivilt Beredskaps ressurser, og til sammen teller de over 1.300.000 mennesker[44]. Sivilt beredskap benytter seg av de frivillige først og fremst dersom det inntreffer naturkatastrofer som krever at mange deltar i f.eks. opprydning. Det er mer usikkert hvordan myndighetene og de frivillige stiller seg i tilfelle et villet terroranslag mot IKT-sektoren.

*Oppfølging*
Det er Politiets post- og kommunikasjonsvesen som står for innsamling av bevismateriale og etterforskning av cyberkriminalitet. De har hatt en utfordring i at det ikke har vært lovpålagt å beholde en datalogg over tid, i motsetning til reglene for telefoni. Dette er nå endret, slik at Politiet har større tilgang til datalogger[45]. Politiets post- og kommunikasjonsvesen nyter

[41] Ref. telefonintervju med Claudio Manganelli, CNIPA og Nasjonal Teknisk Komité for IKT i offentlig sektor, 30.08.05
[42] Ref. telefonintervju med Roberto Setola, (Arbeidsgruppe for Beskyttelse av Kritisk IKT-infrastruktur), 1.09.05
[43] AEEG (2004) *"Resoconto dell'Attività Conoscitiva in Ordine alla Interruzione del Servizio Elettrico Verificatasi il 28 Settembre 2003"*.
[44] De frivillige arbeider gratis, men Staten oppmuntrer til deltakelse gjennom å kompensere for tapt arbeidslønn dersom de blir utkalt. http://www.protezionecivile.it/volontariato/index.php
[45] OECD (2003) *"Survey on the Implementation of the OECD guidelines for the security of Information systems and Networks: Towards a culture of Security"*

utvidede fullmakter i etterforskning etter den overnevnte ”antiterrorloven” av 2005.

### 6.1.4 Innspill fra den italienske IKT-organiseringen

I Italia er det så langt ikke tatt i bruk *øvelser* som metode for å påpeke mangler ved dagens organisering, og dette er noe som etterlyses blant annet av senteret underlagt SMK, CNIPA, som er ansvarlig for bruk av IKT i offentlig administrasjon. Enkelte hevder likevel at rene IKT-øvelser er mindre interessant, og at eventuelle IKT-øvelser under planlegging i dag uansett har blitt nedprioritert til fordel for øvelser som går på andre typer terroranslag[46].

Mangelen på analyser av holdninger til og kunnskap om IKT-sikkerhet blant brukerne av kritisk infrastruktur kan bli en utfordring som Italia må ta tak i snarest. EU har varslet om at de om kort tid ønsker å gjennomføre en undersøkelse i alle medlemsland som går på kunnskap og fokus på sikkerhet, spesielt med hensyn til risikohåndtering og kontinuerlig tjenesteleveranse[47]. Italienske aktører er allerede i ferd med å sette opp planer for tjenesteleveranse (”Business Continuity Plans”), og det arrangeres kurs og opplæring for kompetanseheving. Det skal bemerkes at denne undersøkelsen kun vil gå på privat sektor, og ikke på offentlig administrasjon. En relatert bekymring er det offentliges avhengighet av RUPA (”Rete Unitaria per la Pubblica amministrazione”), det felles nettverket for all offentlig administrasjon. Et slikt felles nettverk øker sikkerhetsrisikoen dersom man ikke tar høyde for mulige angrep og svakheter i systemet, og spesielt dersom kunnskap og bevissthet omkring IKT er svak[48]. RUPAs tekniske senter er nå underlagt CNIPA, noe som muligens kan forenkle tilgangen til teknisk assistanse når GovCERT.IT også blir operativt under CNIPA, og man er i ferd med å omorganisere RUPA[49].

Av de mer positive erfaringene som kan trekkes fra italiensk organisering av IKT, er blant annet opprettelsen av den nasjonale CERT-en. En slik enhet kan vise seg å være svært viktig fordi det er en massiv oppblomstring av CERT-er og ”Incident Respons Teams” innen offentlig administrasjon og privat sektor[50]. Det er behov for en sentralisert enhet som kan sammenfatte og rådgi de ulike CERTene, og som kan ha oversikt over situasjonen på nasjonalt plan. På den annen side er det ennå uvisst når denne enheten vil bli fullt operativ, og oppgavene er ennå ikke fullstendig fastlagt[51].

Et område man er i ferd med å ta nærmere i betraktning i Italia er *kritisk infrastruktur*, der IKT vil komme inn som en naturlig del[52]. CNIPICs rolle vil kunne bli av betydning for den videre utviklingen av IKT kriseberedskap i Italia både på varsling og på det koordinerende plan.

---

[46] Ref. telefonintervju med Claudio Manganelli, CNIPA og Nasjonal Teknisk Komité for IKT i offentlig sektor, 30.08.05

[47] ISCOM (2005) *”La Sicurezza delle Reti”*, side 88

[48] Ref. telefonintervju med Claudio Manganelli, CNIPA og Nasjonal Teknisk Komité for IKT i offentlig sektor, 30.08.05

[49] RUPA skal lages som et system der to av de seks italienske telekom-operatørene skal ha ansvaret for tjenesteleveransen; ”Sistema Pubblica di Connettivitè” (SPC), ref Claudio Manganelli, se note ovenfor.

[50] ISCOM (2005) *”La Sicurezza delle Reti”*, side 146, samt elektronisk kommunikasjon med Prof. Danilo Bruschi, 4.08.05

[51] For ytterligere informasjon om GovCERT.IT og andre varslings- og responsenhetene, se vedlegg 1.

[52] Se for eksempel den konkluderende rapporten fra Gruppo di lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate (2004)*”Protezione delle infrastrutture critiche informatizzate”*.

Senteret vil få et nedslagsfelt som går utover IKT, i og med at det skal håndtere *all* kritisk infrastruktur, men kan gi nyttig erfaring til håndteringen av de gjensidige avhengigheter som finnes på tvers av sektorene. En utfordring kan her ligge i den tidligere nevnte rivaliseringen og uklare arbeidsfordelingen mellom SMK og Innenriksdepartementet.

Koordinering av IKT kan bli gjort enklere dersom "Nasjonal teknisk komité for beskyttelse av kritisk infrastrukturs" forslag til ny modell for IKT vedtas[53]. Forslaget ble fremmet i 2004, men har ikke tatt hensyn til kostnader, slik at det fremstår til en stor grad som en idealmodell. Så langt har man kun opprettet GovCERT.IT som utgår fra forslaget, mens resten av modellen skal opp til diskusjon i Regjeringen i løpet av høsten 2005.

På det operasjonelle plan er det interessant å se på omstillingen av SMK Avdeling for Sivil Beskyttelse. Dersom omstillingen lykkes vil det bety at man i en krisesituasjon vil kunne ha over én million mennesker som kan være tilgjengelige for innsats. På den annen side er en IKT-krise av en slik teknisk karakter at Avdelingens rolle sannsynligvis vil fortsette å være begrenset. Sivil beskyttelse kan være nyttig i en fase hvor man behøver opprydning og menneskelige ressurser som en *konsekvens* av en IKT-krise som har pågått over tid og som har utløst dominoeffekter i samfunnet for øvrig, slik erfaringen fra strømutfallet i 2003 viste.

### 6.1.5 Erfaringer fra tidligere hendelser: Italias kriseberedskap for utland og erfaringene fra Tsunamien i Sørøst-Asia, desember 2004

Det italienske Utenriksdepartementets kriseenhet[54]overvåker det internasjonale trusselbildet på daglig basis, og er opprettet for å ivareta italienske interesser og sikkerhet utenlands. Enheten opererer både i fredstid og under en krise. Under normale omstendigheter samler den informasjon om risiko for italienske interesser og italiensk befolkning i utlandet fra sine diplomatiske forbindelser (ambassader og konsulat), og de samler informasjon om situasjonen, spesielt om kommunikasjonssamband, transport og italienske innbyggere i de landene som befinner seg i en risikosone. I en krisesituasjon skal enheten drive analyse, planlegging og utføring av operasjoner, så som å sende militærpersonell, imøtekomme grunnleggende behov, foreta redningsoperasjoner samt evakuering.

Kriseenheten har flere virkemidler og ressurser til rådighet. Blant annet kan de stille med kommunikasjonssystemer som satellittelefoner og radio[55] til de diplomatiske utsendte, bringe nødvendig mat og utstyr til de italienske rammede, sende ut militært personell for å beskytte diplomater og utføre operasjoner for å beskytte italienske borgere, så som evakuering. Under høyrisikoforhold kan det være aktuelt å også redde ut andre EU-borgere og tredjelandsborgere. Videre organiserer de inspeksjoner utført av sikkerhetseksperter på steder der italiensk bosetting finnes, og de samarbeider med turistselskap om kontroll av steder der det ikke finnes italiensk

[53] Comitato tecnico nazionale
[54] Utenriksdepartementets Kriseenhet "Unità di crisi", http://www.esteri.it/ita/5_31.asp
[55] Ulike kommunikasjonselement som er tilgjengelige for Kriseenheten er bl.a. 75 VHF/UHF nødradionett, over 150 satellittelefoner (fast- og mobile), 1.350 håndholdte og mobile radioapparat med mer. http://www.esteri.it/ita/5_31_83.asp.

ambassade eller konsulat.

*Tsunamien 2004 og Italias reaksjon*
I forbindelse med tsunamien 26. desember 2004, gjorde Italia seg bemerket på grunn av sin profesjonelle håndtering av krisen. Samarbeidet mellom Avdelingen for Sivil Beskyttelse og UDs kriseenhet, med en klart hierarkisk struktur og tydelig lederskap, er noe av forklaringen på Italias vellykkede håndtering.

Regjeringen varslet først Avdeling for Sivil Beskyttelse om naturkatastrofen[56]. To timer etter skjelvet var den operative komiteen for sivilt beredskap samlet. Komiteen bestod av alle enheter som ble regnet som viktige for å håndtere krisen: fra forsvarets flyvåpenet og hæren, telekommunikasjonsoperatørene (både mobilnett og fastnett), og til de sivile flyselskapene. Utenriksministeren ble holdt kontinuerlig informert, og han samlet Sivil Beskyttelses kriseenhet hos seg. Kriseteam fra Sivil Beskyttelse var de første som kom frem til flere av de rammede områdene. Dr. Caroselli fra italiensk Politivesen henviser til at pyramideorganiseringen av ansvar og ledelse i Avdelingen for Sivil Beskyttelse på stedet for katastrofen, gjorde at håndteringen gikk så bra.

En flybro ble opprettet ved hjelp av sivile og militære fly allerede den 27. desember, og innen tredje januar var alle italienske statsborgere brakt hjem. 4.308 passasjerer (italienske og andre) ankom italienske flyhavner i denne perioden. Italienske myndigheter tok også i bruk to Canadair CL415 til bruk på stedet for å transportere personell, mat og annet materiale til katastrofeområdene.

God organisering, ekspertise, ressurser og støtte fra frivillige gjorde at katastrofen ble håndtert på en tilfredstillende måte. Kritikken som har vært rettet mot italienske myndigheter i etterkant av krisen gikk i hovedsak på manglende publisering av navnene på de savnede og omkomne. Årsaken lå i at det var vanskelig å si med sikkerhet hvem som var savnet og hvem som faktisk var identifisert som omkommet. Det var til slutt en ung italiensk gutt som la ut en liste på Internett, hvor man kunne korrigere opplysningene dersom status endret seg. Eksempelet ble deretter etterfulgt av andre organisasjoner, før den italienske staten til sist publiserte en offisiell liste over avdøde.

## 6.2 Håndtering av en IKT-krise i Frankrike

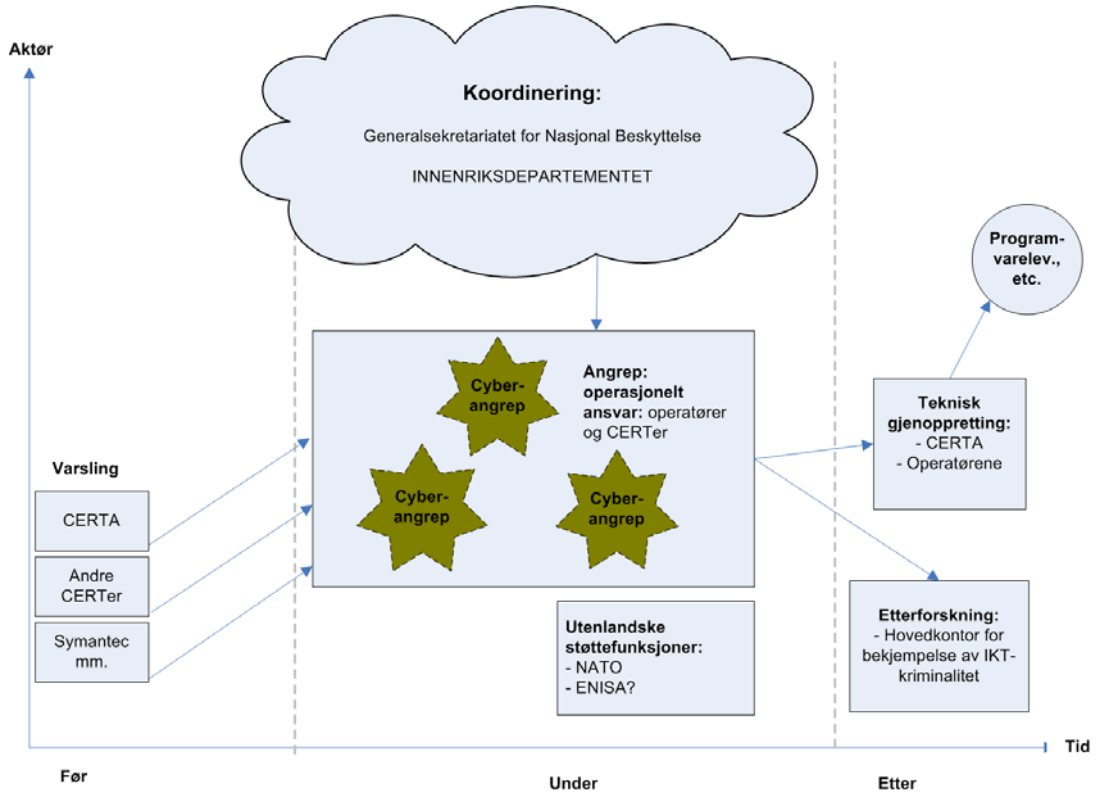
I underkapittelet om Frankrike følger en presentasjon av hvilke aktører som blir involvert dersom en IKT-krise rammer Frankrike, og hvilken rolle de vil ha. Det skal bemerkes at denne fremstillingen er basert i hovedsak på en internettstudie, og at det derfor kan foreligge mangler.

Fransk nasjonal strategi baserer seg på OECDs retningslinjer og prinsipper for informasjons-sikkerhet, det vil si prinsippene om bevisstgjøring, ansvar, reaksjon, etikk, demokrati,

[56] Informasjon fra Avd. for Sivil Beskyttelse:
http://www.protezionecivile.it/cms/view.php?dir_pk=52&cms_pk=2401

risikoanalyse, sikkerhet, håndtering og kontinuerlig evaluering. Disse prinsippene følges opp blant annet av nasjonale planverk for sikkerhet i informasjonssystem[57]. Det opereres også med en ”sjekkliste” for små og mellomstore bedrifter for å se til at de oppfyller disse retningslinjene.

Organiseringen av IKT som sikkerhetselement er i Frankrike fordelt mellom Statsministerens Kontor (SMK) og departementene, da i hovedsak Innenriksdepartementet. Hovedaktøren underlagt SMK er Avdelingen for sikkerhet i informasjonssystemer (”Direction centrale de la sécurité des systèmes d'information”, DCSSI), under Generalsekretariat for nasjonal beskyttelse (”Sécretariat Générale de la défense nationale”, SGDN).




*Figur 6.2 Håndtering av IKT-krise i Frankrike*

### 6.2.1 Før krisen: varsling

Det er ikke mange eksempler på samarbeid mellom offentlig og privat sektor innen IKT, verken når det gjelder varsling eller felles standard på planverk. Siden 2003 er det organisert et antall arbeidsmøter der man har forsøkt etablere ”best practice” på enkelte områder innen IT sikkerhet, så som kryptering, autentisering og produktkvalifisering[58].

På bedriftsnivå og i offentlig sektor er det i hovedsak de ulike CERT-ene som kan varsle om et cyberangrep. Disse samler informasjon fra for eksempel Microsoft og Symantec og videreformidler til bedrifter og offentlig sektor. CERT for offentlig administrasjon er samordnet

[57] ADELE (2004) *”Plan de renforcement de la sécurité”* , samt DCSSI (2004) *”Guide pour l’élaboration d’une politique de sécurité.*
[58] ENISA oversikt: www.enisa.eu.int/country_pages/

i *CERTA* (”Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques”), lansert under DCSSI i 1999, etter utarbeidelse og forslag av en tverrsektoriell komité. CERTA overvåker nett og sårbar infrastruktur, og både varsler og assisterer ved behov[59]. CERTA ser seg selv som et ”tillitsorgan” både for offentlig administrasjon og andre administrative organiseringer, og selv om den er opprettet for å varsle og bistå offentlig etater, kommer varslene ut til befolkningen ”bare noen dager etter”[60]. Det finnes også en egen CERT[61] for industri- og servicenæringene, en kommersiell CERT[62] samt en CERT forbeholdt brukerne av telekommunikasjonsnettverket Renater[63].

På nasjonalt plan vil man benytte seg av terrorvarsel via Vigipirate-planen[64] av 2004 når man innser at det er et koordinert angrep.

### 6.2.2 Under krisen: koordinering og operasjonelt ansvar

*Koordineringsansvar*
Koordinering av en IKT-krise vil avhenge av krisens omfang. Dersom krisen er av svært alvorlig grad vil den håndteres av Generalsekretariatet for Nasjonal Beskyttelse, under Statsministerens Kontor, og det operasjonelle koordineringsansvar vil ligge hos et spesialsenter under sekretariatet kalt COSSI (”Centre Opérationnel de la Sécurité des Systèmes d'Information”), et tverrsektorielt operativt sekretariat. COSSI vurderer og koordinerer arbeidsgrupper og tilknyttede organ som arbeider med ulike viktige samfunnsfunksjoner, så som innenriks- og forsvarsrelaterte emner. COSSI har gjennomført to øvelser for å teste organiseringen i 2003.

Dersom krisen er av et noe mer begrenset omfang vil det være Innenriksdepartementets Hovedkontor for bekjempelse av IKT-kriminalitet (”Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication”, OCLCTIC) som får koordineringsansvaret. En ”Brigade” for bekjempelse av informasjonskriminalitet ble opprettet allerede i 1994, og ble beriket med OCLCTIC i 2000. Hovedkontoret er både operasjonelt og strategisk i arbeidet med å gi teknisk assistanse samt opplæring av offentlig ansatte.

*Operasjonelt ansvar*
I hovedsak er det operatørene som må ta ansvar for den operasjonelle fasen. Dersom en krise rammer Frankrike og man vurderer terrorrisiko mot ”rødt” og ”purpurfarget” i henhold til Vigipirate-planen, vil det få konsekvenser for det operasjonelle ansvar. I henhold til ”Plan for

[59] Det skal bemerkes at CERTA assisterer privat sektor kun i den grad det er aktører som representerer samfunnskritiske funksjoner. Ref Elektronisk kommunikasjon med funksjonær i SGDN, 1.09.05.
[60] DCSSI (2004), *”Mise en oeuvre en France des lignes directrices de l'OCDE”* , side 2.
[61] CERT-IST, opprettet i 1999 av fire store bedrifter; Alcatel, CNES, ELF og France Télécom. Det er per i dag kun France Télécom, Sanofi Synthelabo og Alcatel-gruppen som har adgang til alle tjenester, mens andre medlemmer får adgang til utvalgte deler., www.cert-ist.com/francais/presentation/presentation2_fr.htm
[62] LEXSI, “Laboratoire d’Expertise en Sécurité Informatique”, http://www.lexsi.fr/
[63] CERT-RENATER, www.renater.fr/Securite/CERT_Renater.htm
[64] ”Vigipirate” gir de nasjonale mål på trusselnivået fra gul til oransje, deretter rød og purpur; http://www.premier-ministre.gouv.fr/information/fiches_52/plan_vigipirate_50932.html

styrking av beredskapssikkerhet i informasjonssystemene i offentlig sektor" skal det settes opp operativsentre med bemanning 24/7 i SGDN og i de berørte departementer[65].

Det er også opprettet en "tema-server"[66] til nytte for brukere, både private og offentlige, der en har samlet det meste av informasjonen som er relevant for IKT-sikkerhet.

### 6.2.3 Etter krisen: gjenoppretting og oppfølging

*Gjenoppretting*
Operatørene med støtte i CERTene har hovedansvaret for gjenoppretting, med teknisk assistanse fra CERTene.

*Oppfølging*
Det er Hovedkontor for bekjempelse av IKT-kriminalitet som tar seg av etterforskning og oppfølging av kriminelle handlinger begått ved bruk av Internett.

## 6.3 IKT og utvikling i den Europeiske Union

Den Europeiske Union har allerede opplevd konsekvensene av den økende gjensidige avhengigheten i systemer på tvers av landegrensene. Strømbruddet som blant annet rammet flere europeiske land i september 2003 synliggjorde at ulik standard og mangel på interoperabilitet er en utfordring for tjenesteleveranse innen IKT og et utall andre sektorer. Medlemslandene er pliktige å gjøre hva de kan for at tilgjengelighet til offentlige nett opprettholdes i tilfelle en krise forårsaket av en naturkatastrofe eller annet[67]. Problemet med et stadig økende antall gjensidig avhengige nett gjør at man ikke kjenner den reelle graden av (u)sikkerhet som finnes i IKT-sektoren[68].

Det er altså grunn til å se nærmere på utviklingen i EU for å se hva medlemslandene ser på som ønskelig samarbeid (og ikke) for IKT-relaterte tjenester og regelverk. Opprettelsen av et europeisk byrå for nettverks- og informasjonssikkerhet ("European Network and Information Security Agency", ENISA) vil blant annet kunne gi tekniske innspill til den Europeiske Kommisjonen med hensyn til lovgivning. Det er til dels sterke nasjonale interesser som berøres, noe som fører til at enkelte medlemsland er mindre villige til å enes på unionsnivå, men tre initiativ er i startgropen og vil farge debatten på disse områdene den nærmeste fremtiden. I det følgende presenterer kort dagens situasjon i EU, før det gis en oversikt over initiativene:

- et felles byrå for informasjonssikkerhet (ENISA),
- et program for kritisk infrastruktur ("European Programme for Critical Infrastructure Protection", EPCIP)
- et felles varslings- og informasjonsnettverk for kritisk infrastruktur ("Critical Infrastructure Warning Information Network", CIWIN).

---

[65] ADELE (2004), *"Plan de renforcement de la sécurité*".
[66] Serveur Thématique sur la sécurité des systèmes d'information, http://www.ssi.gouv.fr/fr/index.html
[67] I henhold til Direktiv 97/33/CE og 98/10/CE.
[68] ISCOM (2005)*"La Sicurezza delle Reti"*, side 53

### 6.3.1 IKT i EU i dag

På europeisk nivå finnes det i dag lite samordning og koordinering i tilfelle en krise skulle inntreffe i IKT-sektoren. Det nyopprettede ENISA skal ha som et mål å sette opp en beredskapsplan for kritisk IKT-infrastruktur[69].

På europeisk nivå er det lite samarbeid mellom private og offentlige aktører, selv om det er foreslått et utvidet samarbeid i standardiseringsorganet CEN[70]. I kraftsektoren er et slikt samarbeid i utforming i disse dager[71], og i elektrisitetssektoren har organet UCTE[72] foreslått en felles "sikkerhetspakke" for overføringsoperatører som ble obligatorisk for medlemmene fra 1. juli 2005. Innen energi- og transportsektoren er det flere enheter som allerede har startet opp arbeider med IKT-relaterte problemer[73]. Det hele forblir relativt sektororientert, og det er lite eller ikke noe samarbeid mellom kraft- og kommunikasjonssektoren[74]. Sikkerhet er et nøkkelord i det foreslåtte syvende rammeprogram[75], noe som kan gjøre det enklere å få finansiell støtte til initiativ som omhandler sikkerhet.

### 6.3.2 Samarbeidsinitiativ i EU

**ENISA** er i ferd med å bli operasjonsdyktig. Cirka 30 personer skal tilsettes ved hovedkontoret i Heraklion på Kreta. Dette er et begrenset antall personer, og det opprinnelige mandatet er kun for fem år, men ENISA kan regnes som et første skritt mot en felles EU-strategi for informasjonssikkerhet. Byråets oppgaver blir å rådgi og koordinere Kommisjonen og medlemslandene i nettverks- og IKT-spørsmål, analysere data, høyne kunnskap og invitere til økt samarbeid mellom offentlige og private sektorer. Byrået skal også promotere risikoanalyser og vil publisere studier av beredskap i både offentlige og private organisasjoner.

**EPCIP** er et resultat av samarbeid mellom flere av Kommisjonens generaldirektorat (Directorates-General), Ministerrådet, Europaparlamentet og alle medlemland, og også Norge er med. Neste møte mellom medlemslandene i ENISA er i september 2005, og man regner med at programmet vil bli akseptert innen slutten av året[76].

Hovedoppgavene vil være kritisk infrastruktur generelt ("all-hazards approach"), men programmet skal også utarbeide en spesifikk beredskapsplan for IKT-kriser innen EU, samt legge bedre til rette for samarbeid mellom offentlige og private aktører. Foreløpig er det meningen at hvert land setter opp en rangering av kritisk infrastruktur etter følgende foreslåtte

---

[69] Ref. elektronisk kommunikasjon med Marcelo Masera, JRC, 28.07.05
[70] "Comité Européen de Normalisation", CEN BT/WG 161 (Arbeidsgruppe) "Protection and Security of the Citizen" fremmer standardisering innen blant annet kritisk infrastruktur og CBRN-hendelser (chemical, biological, radiological og nuclear), som kan være til skade for befolkningen.
[71] IEC standard TC57
[72] "Union for the Co-ordination of Transmission of Electricity" UCTE inter-TSO (Transmission System Operator) Multilateral avtale; http://www.ucte.org/pdf/News/20050701_MLA_in_force_v5.pdf
[73] Ref. Marcelo Masera, se fotnote 69.
[74] Ref. Marcelo Masera, se fotnote 69.
[75] Framework Programme 7 (2007-2013) [ennå ikke vedtatt] er EUs hovedinstrument for å finansiere forskning og teknologisk utvikling, og for å arbeide mot oppnåelse av Lisboa-målene om konkurransedyktighet.
[76] Ref. Marcelo Masera, se fotnote 69.

kriterier: nedslagsfelt (geografisk område som berøres), størrelse (tap av liv, økonomisk-, miljømessig-, eller politisk innvirkning), og tidsaspekt (hvor lenge kritiske effekter varer)[77]. EPCIP vil få en rolle i konsolideringen av disse rangeringene. Kritikere hevder programmet vil bli vanskelig å gjennomføre på grunn av problemer med fordelingen av kostnader, samt at det er vitale, nasjonale interesser som berøres av et slikt program.

Europakommisjonen ønsker også å sette opp varslingsenheten **CIWIN**, på samme tid som EPCIP[78]. CIWIN vil bygge på erfaringene fra den tilsvarende organisasjonen i USA, CWIN[79]. Hva denne europeiske enheten konkret skal gjøre, og om den vil videreutvikles til å bli en del av et Europeisk CERT, er ennå ikke bestemt. Fordi det representerer et sensitivt tema for bedrifter og nasjoner ser man for seg en krevende videreutviklings- og beslutningsprosess.

Det finnes også initiativ utenom den Europeiske Union, som har som mål å forbedre samarbeidet og informasjonsdelingen mellom landene. NorCERT er nylig blitt offisielt medlem i **EGC-gruppen** (European Government CERTS-group), et samarbeidsorgan av CERTer med forankring på myndighetsnivå. Så langt omfatter EGC-gruppen sju medlemsland[80], og er per i dag NorCERTs mest relevante internasjonale samarbeidsenhet for krisehåndtering.

### 6.3.3 Utfordringer for EU

Opprettelsen av et byrå for informasjonssikkerhet og de andre initiativene på europeisk plan er tegn på at en viss harmonisering og standardisering anses som nødvendig, men det betyr ikke at det er en likefrem oppgave. Nasjonale interesser og sikkerhetshensyn er med på å trenere prosessen for å komme frem til felles løsninger, og det er en grad av mistillit og skepsis til samarbeid om så viktige områder som kritisk infrastruktur. Tendensen er at de europeiske landene foretrekker at nasjonalstaten er ansvarlig for å lage avtaler om samarbeid, fremfor at det skal organiseres på overnasjonalt nivå. Som en funksjonær i et medlemsland uttalte under intervjuet:

> *"ENISA vil ikke ha en stor rolle i IKT-kriser. Det beste er at krisen handles nasjonalt, eventuelt bilateralt".*

---

[77] Ref. Marcelo Masera, se fotnote 69.
[78] EurActive, 22 august 2005; *"Dossier: Critical Infrastructure"*, http://www.euractiv.com/Article?tcmuri=tcm:29-140597-16&type=LinksDossier .
[79] CWIN I USA: Cyber Warning and Information Network, for mer informasjon se US-CERT: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf .
[80] De andre medlemslandene er Sverige, Finland, Storbritannia, Frankrike, Nederland og Tyskland, utenom Norge. EGC-gruppen er en videreutvikling av bilateralt samarbeid mellom disse landene.

# 7 RESULTATDISKUSJON

Etter en inngående beskrivelse av håndtering av IKT-kriser i Norge og andre europeiske land, vil dette kapittelet oppsummere resultatene sett i lys av hverandre. Strukturen på kapittelet følger problemstillingene beskrevet i kapittel 2. En diskusjon av hvordan andre land har organisert seg vil inkluderes mot slutten i kapitlene 7.1-7.3.

## 7.1 Hvem har ansvar i en krisesituasjon?

I forhold til ansvarsavklaring uttrykte en intervjuet person at:

> ”Det vil uansett være slik at det departementet som har flest ”aksjer” i krisen må håndtere den”.

Som scenariene har vist vil plassering av ansvar være avhengig av hvilken sektor krisen oppstår i. Ved en IKT-krise får man imidlertid et problem, ettersom IKT er sektorovergripende, og derfor kan være vanskelig å knytte til en enkelt sektor.

Som det kom frem av gjennomgangen av scenario 3, vil det ikke være sannsynlig at MOD blir ilagt en rolle i en krise. Moderniseringsministeren har imidlertid tatt initiativ til å få en struktur på kommandolinjer etc. ved en IKT-krise, etter at det blir opprettet et nasjonalt CERT[81]. Fordelen med et nasjonalt CERT vil være å få samlet oversikt over kompetansen og ha et felles kontaktpunkt mot utlandet. På operativt nivå vil ansvaret for å løse IKT-problemene ligge på den enkelte virksomhet, og de må selv sørge for å ha etablerte kontakter med underleverandører for å sikre seg hjelp i tilfelle kriser.

Om Regjeringens kriseråd skal tre sammen eller ikke kan være avhengig av antall brukere som berøres. Som nevnt vil det også være slik at ansvaret i en krise vil kunne overføres til eller mellom departementer, avhengig av krisens omfang. Dette kan være vanskelig å avgjøre når krisen inntreffer. Katrina-orkanen i USA 29. august viste nettopp at man ofte ikke innser omfanget av krisen før etter en stund, og at det tar tid før det nasjonale beredskapsapparatet settes inn:

> ”Supermakten mobiliserer, etter å ha virket som lamslått de første par dagene”[82]

[81] Det skal nedsettes en interdepartemental arbeidsgruppe - ledet av MOD - som gjennomgår nåværende koordinerings- og sektoransvar på IT-sikkerhetsområdet. Dersom gruppen avdekker tvilstilfeller forutsettes det at arbeidsgruppen foretar de nødvendige presiseringer slik at de involverte myndigheter ikke er i tvil om grenseoppgangen. Forhåpentligvis foreligger det en rapport fra arbeidsutvalget i begynnelsen av desember d.å.

[82] Artikkel i Aftenposten, 1.09.05: ”Lamslår supermakten”, av Nils Morten Udgaard.

Det kan oppfattes som et problem i dag at ”man mener og *tror* det er slik eller slik”, og at ingen kan si noe sikkert om hva som egentlig skjer på ulike tidspunkt. Igjen kan dette skyldes at det finnes liten praktisk erfaring med å håndtere større IKT-hendelser.

Diskusjonen om ansvarsplassering ender ofte opp i hvorvidt det ville vært på plass med et eget ”superdepartement” for sikkerhet. Flere mener dette er nødvendig for å få klarhet i ansvarsforhold på øverste hold og mellom sektorer:

> ”[…] vil gjøre sektorjobben lettere, fordi noen på høyere nivå kan tenke strategisk og legge føringer. De på sektornivå kan konsentrere seg om detaljer og om å utføre det de skal. I dag er det sånn at myndighetene ”rir på hver vår sektor”. Med et superdepartement vil man kunne koordinere mellom sektorer. Det er viktig at hver enkelt sektor ansvarliggjør bransjen og det enkelte selskap; det er disse som sitter på mest kompetanse om systemene.”

En interessant observasjon i forhold til hvorvidt Regjeringens kriseråd vil tre sammen eller ikke er at man på lavere administrative nivå tror og forventer at Regjeringens kriseråd vil opprettes. Når man imidlertid spør på departementsnivå, er de mer usikre og mener det vil avhenge av flere faktorer. Man har enda ikke testet ut Regjeringens kriseråd i nasjonale kriser, som kan gjøre at dette er vanskelig å uttale seg helt sikkert om.

Det viser seg at det ikke bare er i Norge man er i gang med omfattende analyser og undersøkelser i forbindelse med ansvar og IKT. Intervju og rapporter fra Frankrike og Italia viser at de er i gang med en storstilt omstilling, noe som gir seg utslag i et tilsvarende uklart bilde av hvordan organiseringen vil komme til å se ut på sikt. Sommeren 2005 opprettes det i Italia en egen enhet for beskyttelse av kritisk infrastruktur (inklusiv IKT) under politiet og innenriksdepartementet, man forsøker omorganisere nasjonal beredskap for å være forberedt på en IKT-krise, og man etablerer en nasjonal CERT.

I Italia kan utformingen av et CNIPIC-senter for beskyttelse av kritisk infrastruktur, underlagt Innenriksdepartementet (se kap. 6.1) gjøre det nødvendig med en ny avklaring av roller. Innenriksdepartementets senter oppfattes som en ”utfordrer” til Statsministerens Kontor, Avdelingen for Sivil Beskyttelse, spesielt fordi sistnevnte *også* er i ferd med å omorganisere seg for bedre å håndtere en IKT-krise. En ”maktkamp” mellom disse to nivåene i ansvarsfordelingen er i stor grad forårsaket av IKT-sektorens tekniske og tverrsektorielle karakter, og en løsning på dette i Italia vil kunne gi nyttige erfaringer også for Norge.

Omorganiseringen av det italienske sivile beskyttelsesapparatet baseres på erfaringene fra strømbruddet som rammet Italia via Sveits i 2003, som har gjort dem mer oppmerksomme på gjensidige avhengigheter og behovet for å være beredt på

dominoeffekter av en IKT-krise. Der man i Norge først nå er i ferd med å opprette Regjeringens kriseråd, har dette vært praksis i Italia i en årrekke - mest fordi det har vært flere tilfeller av nasjonale (natur) kriser. I Norge vil krisehåndteringen tas hånd om av det departement som "eier" krisen, eventuelt av Justisdepartementet dersom ingen andre kan utpekes. I Italia er det Innenriksdepartementet som har ansvar ved en nasjonal krise, og ansvaret overføres til høyere hold (Avdeling for Sivil Beskyttelse) i det øyeblikk krisen medfører fare for liv og helse.

Etableringen av en nasjonal CERT i Norge stiller seg på linje med utviklingen i Italia, selv om oppgavene til de to er noe forskjellige. Både i Frankrike og i Italia er den nasjonale CERTs oppgaver *både* varsling og respons, mens den i Norge per i dag er en responsenhet, der varsling overlates til et eget organ. I Frankrike har man hatt en nasjonal CERT i flere år, men der er hovedutfordringen at den ikke varsler privat sektor. Erfaringene fra Frankrike, og i mindre grad Italia, tilsier at man *forsøker* å oppnå en tillit mellom sektorene, men bedriftenes konkurransehensyn motarbeider et slikt initiativ. Det kan synes som om dette er en utfordring i flere europeiske land, og blant annet har man i Nederland etterlyst en lovhjemmel som kan gjøre det obligatorisk for konkurrerende selskap til å samarbeide dersom en krise oppstår, noe som anses som nødvendig for å opprettholde tjenesteleveransen til den rammede aktøren[83]. I så måte kan man si at situasjonen i Norge, der samarbeid og tillit mellom offentlige og private aktører er utbredt, er spesiell[84].

At man i EU er opptatt av IKT og kritisk infrastruktur kommer også frem i utviklingen på mellomstatlig nivå, med opprettelsen av et byrå for nettverks- og informasjonssikkerhet, der også Norge er representert. Det som er hovedutfordringen for arbeidet på Europeisk nivå er at det er nasjonale interesser og sårbarhetsaspekter med i betraktningen, noe som kan hemme samarbeidet. I tillegg kan det være ulikt fokus i de forskjellige landene, slik at det som regnes som kritisk i ett land ikke nødvendigvis er det samme i et annet. Der man i Norge fremdeles vurderer om man skal se på IKT som et *eget* område, eller om det er en sektorovergripende utfordring, utviser man for eksempel i Italia og Frankrike en mer pragmatisk holdning. Dersom man har et cyberangrep mot en (hvilken som helst) sektor vil det være Innenriksdepartementet som får det koordinerende hovedansvaret, så fremt det ikke er fare for liv og helse.

## 7.2 Hvilke virkemidler har myndighetene i en krisesituasjon?

Under de innledende intervjuene i Norge ble det sagt at myndighetenes rolle består i å lage et veldekkende konkret regelverk, føre tilsyn med at det etterfølges, ta strategiske beslutninger og bevilge penger. Det mest virkningsfulle virkemiddelet kommer inn i

[83] Ref. Intervju med funksjonær i nederlandsk offentlig sektor, august 2005.
[84] Samarbeid mellom private og offentlige aktører er spesielt synlig blant annet hos VDI sine medlemmer, der sikkerhetsinformasjon (alt fra trusselbilde ned til enkelthendelser) er tilgjengelig medlemmene i mellom.

forkant av en krise, ved å styrke beredskapen gjennom planverk og gjennomføring av beredskapsøvelser. Det er i Norge ennå ikke avholdt mange øvelser som går spesifikt på IKT, og flere aktører i Norge uttrykte behovet for å gjennomføre en storskalaøvelse, ved blant annet å sjekke kompatibilitet og effektivitet mellom det sivile og militære systemet.

*Lovverk*
Det vil være stor forskjell på kriser i fred og krise i krig, ved at det i en krigssituasjon foreligger et lovverk. Alle våre scenarier foregår i fredstid, men scenario 3 kan tenkes å få "krigslignende" tilstander.

Flere har kritisert at det ikke finnes et lovverk som setter påbud om beredskapsplaner for viktige samfunnsfunksjoner. Per i dag eksisterer det kun for virksomheter med ansvar for helse- og sosialtjenester, sykehus, vannverk og næringsmiddelkontroll. Behovet for å ha tilsvarende lovverk i kraft og telesektoren er nødvendig for å sikre god beredskap[85].

I kraftbransjen eksisterer KILE-systemet (Kvalitetsjusterte inntektsrammer ved ikkelevert energi). Dette ble innført av NVE i 2001, og gjør at nettselskapenes inntekter er avhengig av leveringspåliteligheten i nettet[86]. Ved strømbrudd blir nettselskapene pålagt et straffegebyr for hvert minutt de ikke leverer strøm. Dermed vil det være et incentiv for selskapene å sørge for god beredskap, herunder vedlikehold av IKT-baserte driftssystemer.

På den annen side bør diskusjonen om *nytten* av beredskapsplaner settes i sammenheng med hvem som utarbeider disse planene, og det er ikke selvsagt at slike planer nødvendigvis vil kunne lette krisehåndteringen i det den inntreffer. I så måte er det kanskje mer nyttig med en utstrakt bruk av *øvelse*, noe som også ser ut til å passe med aktørenes formening:

> "Planverk er bra – øvelser er morsommere"

*Hvem betaler?*
Det er myndighetene som i mange ledd bevilger penger i krisesituasjoner, og for mange operasjoner (for eksempel dersom Forsvaret skal trekkes inn) kreves det at beslutninger tas på et høyt nivå.

Hvert departement har et budsjett på 1 million kroner som kan brukes umiddelbart i kriser, utover dette kreves det ekstrabevilgninger og nødvendige fullmakter. Alle private aktører må bruke egne midler i kriser, noe myndighetene ikke tror et problem, ettersom det vil være i deres egeninteresse å få systemene opp og driften i gang igjen.

---

[85] fra ROS-analyse utarbeidet av Fylkesmannen i Oslo og Akershus, 4.12.03.
[86] For mer informasjon, se: www.nve.no

Følgende sitat er betegnende for de fleste aktørene vi har intervjuet:

> ”I en krisesituasjon vil det ikke bli spørsmål om penger. Mentaliteten er: Bygg opp! Finn penger til det etterpå”.

En generell oppfatning er at alle vil mobilisere i en krise, og ikke være redde for å stille opp. Økonomien er ikke det man tenker på. Et av argumentene for dette er at man ved store kriser uansett ikke vil ha budsjettert nok midler på forhånd. Det ble også nevnt at det er ”lett” å få penger til håndtering av krisen når den har inntruffet, men kostnader knyttet til beredskap er det verre med.

Av en annen aktør ble det nevnt at økonomi kan bli et problem, og at personer som blir sentrale i krisehåndteringen er nødt til å ha fullmakter avklart i forkant av en krise. Dersom dette ikke er gjort, kan man få tilfeller der enkelte velger å ikke bruke penger i det hele tatt, av frykt for å få kritikk i etterkant av krisen.

I utenlandsstudien kommer det frem at mens man i Norge og i Frankrike allerede har gjennomført øvelser som i det minste omhandler IKT som en *del* av et krisescenario, er dette noe som mangler fullstendig i den italienske organiseringen. Det er i dag snakk om at Italias nye enhet for beskyttelse av kritisk infrastruktur skal kunne drive øvelsesvirksomhet og simulering, men dette er ennå ikke utprøvd. I tillegg er det både i Italia og i Norge uttrykt ønske om å gjennomføre øvelser som går spesifikt på *IKT*-kriser, med den tilleggsutfordringen i Italia at en ren IKT-øvelse hevdes å kunne bli nedprioritert i forhold til øvelser som går på andre typer terroranslag. I Frankrike ligger svært lite informasjon om øvelser tilgjengelige på Internett, noe som gjør det vanskelig å kommentere graden av nytte og vellykkethet.

I tillegg til planverk og øvelser på virksomhetsnivå, bør det også vurderes hvilken rolle myndighetene har i forhold til opplæring av befolkningen. Bare ett år før det faktiske terrorangrepet på London, ble det i 2004 vist en dokumentar på BBC som tok for seg et scenario der London ble angrepet[87]. I dokumentaren var en rekke av landets fremste eksperter på sikkerhet samlet for å gi sin vurdering på hva som kom til å skje i de ulike fasene av angrepet, og hva de trodde kom til å bli de største utfordringene. Det ble påpekt at myndighetenes viktigste rolle vil være forberedelse og opplæring i krisehåndtering. Dette inkluderer ikke bare myndigheter og virksomheter, men også befolkningen generelt. Et sett med ”do’s and dont’s” i tilfelle kriser kan gjøre hele befolkningen mer forberedt på hvordan de skal opptre i en krisesituasjon.

## 7.3 Håndteres kriser forskjellig avhengig av hvilken type det er?

Innledningsvis prøvde vi å definere begrepet krise, og i praksis ser det ut til at man skiller på *graden* av en krise for å avgjøre hvilket apparat som skal involveres. På

[87] ”London under attack”, BBC, 16.mai 2004.

operativt nivå ser det ut til at aktørene vil ha samme rolle uansett om det dreier seg om en IKT-krise eller en annen krise. Høyere opp i systemet vil spørsmålet bli *om* det skal etableres et Regjeringens kriseråd eller ikke. Når systemet først er etablert, vil rollen være den samme. Enheter som har koordineringsroller i kriser, ser ut til å ha samme rolle uansett, som for eksempel DSB sin koordineringsrolle mellom JD og Fylkesmannen.

I alle scenariene kan det tenkes at et nasjonalt CERT kan få en rolle. Blant aktørene på workshopen ble det nevnt at det vil være en umulig oppgave å samle all kunnskap i en generell ekstern "ekspertgruppe", på grunn av forskjellene som ligger i systemene hos de enkelte virksomhetene. Det vil derfor være et behov for sektorvise CERTer i tillegg[88]. Dette er blitt foreslått som et viktig tiltak av flere aktører, for å få til en god informasjonsutveksling mellom alle relevante virksomheter innen en sektor. Innenfor de ulike CERT-ene bør det også tas stilling om CERT-ene skal være både varslings- og responsenheter, slik praksis er i andre land.

Hva er forskjellen på håndtering av IKT-kriser og andre kriser? Og er det mulig å snakke om en ren IKT-krise? Det flere er enige om er at *konsekvensene* fort blir de samme, men ettersom årsaken til krisen i de ulike scenariene er forskjellige, må de håndteres ulikt. Erfaringene fra arbeidsseminaret resulterte i noen synspunkter, på hva som er spesielle utfordringer med IKT-kriser:

> "Sette navnelappen på: hvem eier den?"
> "Alt stopper opp – ingenting styres manuelt lenger"
> "Dersom det er snakk om fare for liv og helse har man et klart definert lovverk – for det andre er det litt mer ullent"

I forhold til IKT-kriser kan man skille på (minst) to faktorer:

1. Den opprinnelig årsak til krisen er en naturkatastrofe, som dermed rammer IKT-systemene.
2. Årsaken til krisen er angrep mot/teknisk svikt direkte i IKT-systemene, som dermed gir konsekvenser for en rekke andre funksjoner. Her kan man ved angrep skille på to nye faktorer:
    a. Angrep mot én sektor
    b. Koordinerte angrep mot flere sektorer

En av aktørene under workshopen hadde en godt beskrivende kommentar til forskjellen mellom disse to faktorene. Dersom det første tilfellet fører til strømbrudd, vil SCADA-systemene bryte sammen, med den konsekvensen at man bare må vente til strømmen er tilbake igjen. Inntil da er *dataene* i systemet utilgjengelige, men de vil fortsatt være de samme som før strømmen gikk (dvs. tilgjengeligheten er svekket, men integriteten er i takt). Ved angrep på datasystemene får man en ny

[88] Som for eks. egen CERT for oljenæringen, telebransjen etc.

problemstilling; man vet ikke lenger om man kan stole på de dataene man får, ettersom noen kan ha endret på dem. Tilfelle 2) skaper dermed en stor grad av usikkerhet, ettersom integriteten i dataene er påvirket i tillegg til tilgjengeligheten av dem.

Det ble også kommentert at det ved feil på datasystemer ofte er veldig vanskelig å få oversikt, og at man ikke vet om det er en fysisk eller logisk bombe. Dette er ofte noe man finner ut i etterkant når problemet er løst.

Erfaring fra Netcom-hendelsen i sommer[89] viser at bortfall av mobiltelefoni i seg selv ikke trenger å være en krise, ettersom de fleste har tilgang til alternative samband i stedet. Diskusjonen om prioriteringer i telenettet kom opp på nytt, der det fra flere hold ble påpekt at PT bør ha en slik samlet oversikt, for dermed å kunne fungere som et bindeledd mot Fylkesmannen og andre relevante aktører. Som flere har nevnt i samtaler vil det stadig tilbakevendende temaet være; hvilket verktøy bruker man i gjenopprettingsfasen når mobiltelefoni ikke fungerer? Og dersom kriseplanene ligger på en pc man ikke får skrudd på? Dette peker igjen tilbake på myndighetenes rolle for å sørge for tilstrekkelig regelverk som sikrer god beredskap i forkant av kriser.

I Italia og Frankrike er det i hovedsak faren for liv og helse som bestemmer om krisen skal håndteres annerledes. I enklere scenarier vil det være naturlig å løse krisen på operatørnivå, og en nasjonal CERT vil kunne tenkes å ha en rolle tilsvarende den i Norge. Unntaket er i så måte at franske og italienske CERT-er er både varslings- og responsenheter, og som en tilleggsutfordringen i Italia er den nasjonale CERT-en ennå ikke operativ. Den franske CERTA er noe bedre stilt, siden det har vært operativt siden 2000, men enheten er i hovedsak et responssenter kun for offentlige organer. Det savnes en mer nyansert holdning til krisehåndtering for IKT spesielt, for i dag blir en IKT-krise oppfattet mer som en hvilken som helst krise. Som Claudio Manganelli uttalte, settes IKT-sikkerhet ikke akkurat i høysetet i Italia i dag[90].

## 8 KONKLUSJON

Målet med denne rapporten er å si noe om hvordan en IKT-krise kan håndteres i Norge. Dette har blitt gjort ved hjelp av samtaler med både norske og utenlandske aktører, der erfaringene fra utlandet har blitt brukt for å få innspill på andre måter å organisere sikkerhetsarbeid på. Vi har kommet frem til hvilke aktører som er involvert i håndteringen av krisen, samt hvilken rolle det kan tenkes at disse har. I det følgende vil vi trekke ut de mest interessante konklusjonene, for å påpeke noen av utfordringene som eksisterer i dag.

---

[89] 12. og 13.juni 2005: 3000 bedrifter og over en million kunder ble rammet

[90] *"La sicurezza ICT viene messa nel camerino, non esattamente nel salone"*, Ref. Claudio Manganelli, Se note 46.

## 8.1 Forbedringsmuligheter i Norge

Tittelen for rapporten er håndtering av *IKT-kriser* i Norge, men erfaringer[91] har vist at det har vært vanskelig å avgrense diskusjonen til å kun gjelde IKT, og at man i stor grad faller tilbake på "tradisjonell" krisehåndtering. Dersom krisen oppstår som en ren IKT-krise som beskrevet i scenario 1 havner diskusjonen fort på hvilke *konsekvenser* dette får for andre sektorer. Ved en krise tilsvarende scenario 2 vil IKT-problemer inntreffe som en følge av strømsvikt, og dermed ender diskusjonen fort opp med at "vi må fikse strømmen", så ordner IKT-problemene seg etter hvert.

Erfaringene viser at det eksisterer klare linjer på hvem som skal håndtere *konsekvensene* av en IKT-krise, men problemet kommer når man skal definere hvem som eier selve IKT-krisen. Ettersom IKT-problemene uansett må løses på laveste nivå, kan man diskutere hvorvidt *eierskapet* til IKT-krisen er et reelt problem. Utfordringen i dag ligger i å tenke på IKT som sektorovergripende, isteden for å bruke ressurser på å "lete" etter en eier til krisen. Dette krever at man løfter blikket opp fra sektorprinsippet og begynner å tenke mer helhetlig.

I en krisesituasjon vil det være helt nødvendig å ha på plass klare ansvarsavklaringer. I Italia vil Innenriksdepartementet være ansvarlige for krisehåndteringen, inntil krisen eskalerer og det blir fare for liv og helse. På det tidspunktet overføres ansvaret til Statsministerens Kontor. På denne måten vil det være en helt klar rollefordeling uavhengig av hva slags krise det er, selv om ansvarsfordelingen aldri har vært utprøvd ved hjelp av øvelser.

For selve håndteringen av kriser, viser det seg at en enkel sektoravgrenset krise ikke er noe problem, ettersom dette knyttes opp til det ansvarlige sektordepartementet. Problemet oppstår når krisen eskalerer og dominoeffekten mot andre sektorer kommer til syne; hvem skal da koordinere? Figurene som ble vist i kapittel 4, har samlet myndighetene i en "koordineringssky". Under workshopen reiste en av deltakerne spørsmålet om det egentlig er noe problem at myndighetene fremstår som en "ulldott". Kanskje ansvarsforholdene ikke trenger være så mye mer klare enn de er i dag? Det har blitt nevnt at myndighetene har få konkrete virkemidler å sette inn ved slike kriser. Det koker ned til at det operative ansvaret vil ligge på hver enkelt virksomhet. Myndighetenes viktigste rolle blir således å sikre at bedriften selv har gode rutiner på plass. Dette involverer både planverk og beredskapsøvelser.

En suksessfaktor for all krisehåndtering er forberedelse lokalt, og det blir viktig med et grundig og dekkende planverk, samt bruk av øvelser. Det ser ut til at det foretas en rekke nasjonale øvelser, som i stor grad er begrenset geografisk eller sektorvis. Det som mangler er gjennomføring av storskalaøvelser, som tar hensyn til større geografiske områder, flere sektorer, og med større fokus på sivilmilitært samarbeid.

[91] Fra workshop 23.8.05 og samtaler med relevante myndigheter i tidsrommet 15.juli-15.august

Det er enda ikke gjennomført rene IKT-øvelser, men IKT har vært del av andre beredskapsøvelser, som i forbindelse med forberedelse til år 2000[92].

Erfaringene fra arbeidet med denne rapporten viser at man ved ”fare for liv og helse” har et godt etablert system, noe som skyldes at denne faren har eksistert lenge, og at man har erfaring fra tidligere ulykker og katastrofer. Problemet med IKT-kriser er at dette inneholder et nytt element, ”IKT”. Det kan være en tendens til å tro at dette området er noe veldig nytt, som krever helt nye tenkemåter. Løsningen ligger muligens i å se på dette i forhold til erfaringene man har gjort seg på området ”liv og helse”, og at det dermed kan være tilstrekkelig med mindre tilpasninger. Den største utfordringen ligger muligens på regelverksiden, noe vi forhåpentligvis kan få orden på gjennom Koordineringsutvalget for IT-sikkerhet[93].

Ved å studere krisehåndtering i andre land, har vi kommet frem til at det er mye som ser bra ut på papiret, med for eksempel etablering av ny nasjonal CERT og planer for samarbeid mellom offentlig og privat sektor. Vi vet imidlertid lite om hvordan dette vil fungere i praksis, og landene selv har etterlyst øvelser og testing. Denne studien har ikke gitt noen ”bevis” på hvordan man vil være i stand til å håndtere IKT-kriser. Et fellestrekk for landene er at organiseringen følger nærhetsprinsippet, og at en IKT-krise i hovedsak kan sies å bli oppfattet som en hvilken som helst annen krise.

## 8.2 Videre arbeid

Utarbeidelsen av denne rapporten har skjedd med begrenset tid til rådighet, og de følgende punktene viser noen områder som er interessante å følge opp i tilknytning til rapporten.

*Roller og ansvar på myndighetsnivå*
Som nevnt i kapittel 4 foretar Riksrevisjonen i disse dager en studie av myndighetenes arbeid med å sikre IT-infrastruktur. Denne beskriver alle myndighetene som har en rolle i dette arbeidet, og hva slags rolle de har. Rapporten vil gi nyttig bakgrunnsinformasjon for det videre arbeidet med BAS5. Det kan også være interessant å følge med på hva som skjer i Regjeringens Kriseråd, når dette er operativt.

*Beredskapsplaner*
Vår rapport har inkludert en ”før”-fase i scenariene, der planverk er en sentral del. Denne studien har imidlertid verken gått inn i planverket på virksomhets- eller forvaltningsnivå. Ettersom myndighetene i stor grad henviser til nærhetsprinsippet i kriser, kunne det vært interessant å studere planverket til eiere med kritisk

[92] Ref. møte med Fylkesmannen i Oslo og Akershus, 3.08.05.
[93] Utvalget har nedsatt en arbeidsgruppe som skal jobbe med forenkling av regelverket. For mer informasjon, se www.kis.stat.no.

infrastruktur (selv om disse ikke er klart definert enda) for å se i hvilken grad det er etablert planer for hva de skal gjøre i tilfelle en IKT-krise. Hvorvidt kommunene i Norge har beredskapsplaner og gjennomfører øvelser med tanke på en IKT-krise i kommunen, ville også vært interessant i en slik sammenheng.

*Internasjonalt arbeid av interesse for Norge*

- Det skal ferdigstilles en rapport fra OECD (Organisasjonen for økonomisk samarbeid og utvikling) i august 2005 som bruker Norge som en case i et studie av IKT-sikkerhet[94].
- Det skjer mye arbeid i forbindelse med organisering av IKT-sikkerhet, som blant annet opprettelse av nasjonale og andre CERT.er. Det kan være nyttig å se videre på hva som skjer i land som i utgangspunktet har en annen organisasjonsstruktur enn Norge.
- Satsing på kritisk infrastruktur kan vise seg å sette IKT i et annet søkelys, og om man i utlandet finner at IKT bør behandles separat eller som en del av en generell beskyttelse av kritisk infrastruktur, vil være av interesse for videre norsk organisering.

*Krisehåndtering i andre land*

Som følge av terrorangrepene i London 7. og 21. juli i år, samt orkanen Katrina i USA 29. august, kan det tenkes at det vil bli utarbeidet erfaringsrapporter fra krisehåndteringen. I motsetning til scenariene beskrevet i denne rapporten, er dette hendelser som faktisk har skjedd på storskalanivå, hvor man kan forvente at det vil komme mye nyttig informasjon.

*Informasjonsarbeid*

Erfaringer fra Gudrun-stormen i Sverige[95] tilsier at det bør være klare retningslinjer for informasjonsarbeid på myndighetsnivå i forbindelse med en krise. Dette kan være spesielt utfordrende i en IKT-krise på grunn av den åpenbare vanskeligheten med å nå ut med relevant informasjon, når telekommunikasjonssystemer er ute av drift.

[94] Ref samtale med Ronald van der Luit 9.08.05
[95] Svenska Kraftnät Beredskapsstaben, *"Erfarenheter av krisehanteringsarbetet efter Gudrun"*, PM 25.04.2005

# A APPENDIKS

## A.1 FORKORTELSER

| | | |
|---|---|---|
| BAS | - | Beskyttelse av samfunnet |
| CERT | - | Computer Emergency Response Team |
| CIRC | - | Computer Incident Response Capability |
| DSB | - | Direktoratet for samfunnssikkerhet og beredskap |
| EU | - | Den Europeiske Union |
| FD | - | Forsvarsdepartementet |
| FSA | - | Forsvarets Sikkerhetsavdeling |
| IKT | - | Informasjons- og kommunikasjonsteknologi |
| JD | - | Justis- og politidepartementet |
| KBO | - | Kraftforsyningens Beredskapsorganisasjon |
| KIS | - | Koordineringsutvalg for informasjonssikkerhet |
| LRS | - | Lokal Redningssentral |
| NSM | - | Nasjonal Sikkerhetsmyndighet |
| NVE | - | Norges vassdrags- og energidirektorat |
| MOD | - | Moderniseringsdepartementet |
| OECD | - | Organisation for Economic Co-operation and Development |
| OD | - | Oljedirektoratet |
| PST | - | Politiets sikkerhetstjeneste |
| PT | - | Post- og Teletilsynet |
| Ptil | - | Petroleumstilsynet |
| SD | - | Samferdselsdepartementet |
| SIS | - | Senter for Informasjonssikring |
| SMK | - | Statsministerens kontor |
| UD | - | Utenriksdepartementet |
| VDI | - | Varslingssystem for Digital Infrastruktur |

## A.2 IKT-organisering i andre land

### A.2.1 IKT-organisering i Italia

*Offentlig sektor versus privat sektor*
Offentlig sektor ser ut til å være bedre organisert enn privat sektor, med hensyn til IKT og sikkerhetstenkning[96]. Noe av årsaken kan ligge i at italienske myndigheter har erfart illegal bruk av IKT. Ett slikt eksempel er da Internett ble benyttet som informasjonskanal av nasjonale terrorister, da de politisk radikale "Røde Brigadene" tok livet av professor Marco Biagi i Bologna i 2002. I tillegg er det i den senere tid avslørt funn som tyder på at internasjonale terrornettverk har sterk tilknytning til Italia, og én av de mistenkte bombemennene fra London-eksplosjonen tidligere i år ble nylig arrestert i Italia[97]. Finansiering og planlegging av terroraksjonene i USA i 2001 har blitt knyttet til terrororganisasjonens undergrupper i Italia[98].

*Energi og IKT*
Det er en klar sammenheng mellom IKT og energi. Dersom den elektriske kraften forsvinner medfører det bortfall av viktig IKT-infrastruktur innen relativt kort tid. Italia importerer bortimot en fjerdedel av elektrisiteten til nasjonalt bruk fra sine naboer, noe som medfører at den nasjonale IKT-sikkerheten er avhengig, ikke bare av tilgang til strøm i deres eget land, men også av leverandørenes tilgang[99]. Denne avhengigheten ble synliggjort av hendelsene 28. september 2003, der store deler av Italia ble mørklagt pga. en feilsituasjon i Sveits. Kommunikasjonssektoren ble hardt rammet da nødstrømskapasitetet etter hvert ble tappet, og det ble tatt i bruk satellittelefoni og manuell utkjøring av personale for å gjenopprette kommunikasjonssystemet[100].

*Holdninger til IKT*
Det er foreløpig ikke gjennomført noen helhetlig analyse av holdning til, og kunnskapen om, IKT-sikkerhet blant brukerne av kritisk infrastruktur i Italia. Rapportene baserer seg på generaliseringer og deduksjoner ut fra for eksempel hvor mange som er ansatt til å ta vare på sikkerhet[101]. Forskning på IKT er fremdeles i stor grad sektorfokusert[102], noe som gjør det vanskeligere å sammenlikne graden av sikkerhet i IKT system på tvers av sektorene og i forholdet mellom offentlige og private aktører. Privatisering og outsourcing er et område i ekspansjon også i Italia, og forskning viser at det er utvist lite påpasselighet med å tydeliggjøre minimumskrav til sikkerhet dersom IKT-relaterte tjenester overlates til

[96] Corrado Maria Daclon (2004), intervju med Vincenzo Merola.
[97] Det er snakk om Hamdi Issac Adus (og hans bror) som stod bak det mislykkede angrepet på Londons undergrunn 21.juli 2005, ref. Innenriksdept. (2005b) "Lo stato della sicurrezza in Italia", side 58.
[98] La Repubblica (2003), *"Italia avamposto dei terroristi"*.
[99] Import til Italia: ENEL (2004) *"Energia e Ambiente"*
[100] AEEG (2004) *"Resoconto dell'Attività Conoscitiva in Ordine alla Interruzione del Servizio Elettrico"*.
[101] ISCOM (2005)*"La Sicurezza delle Reti"*, side 87.
[102] Ref. intervju med Vincenzo Merola, note 96.

underleverandører[103].

*Gjensidige avhengigheter*
Teknisk svikt i en begrenset del av IKT-systemet får store konsekvenser. Den 2. januar 2004 skjedde det en teknisk feil i luftanlegget til en telefonsentral i Roma, hvilket førte til at hele telekommunikasjonssystemet ble satt ut av spill i flere timer. Over 5 000 bankfilialer og 3 000 postkontor ble uten Internettkontakt, og 70% av check-in-deskene på hovedstadens flyplass ble paralysert. I tillegg til risiko for teknisk svikt, er det en økende fare for at kritisk infrastruktur i Italia kan rammes av cyber-angrep, fordi folk flest ikke er oppmerksomme nok på risikoen som følger med avhengigheten av IKT-systemer i alle sektorer[104]. En omfattende holdningskampanje[105] pågår i denne perioden, og myndighetene (Nasjonal Teknisk Komité spesielt) er pådriver for utarbeidelse av en "Business Continuity Plan" (BCP) for alle sektorer. BCP skal ta høyde for ulykker og angrep (naturkatastrofer, teknisk svikt, menneskelig feil, sabotasje og terror) på IKT-sektoren for at tjenesteleveranse skal kunne fortsette i best mulig grad[106]. I denne planen er det også forespeilet øvelser for å teste dens funksjonalitet. Det mest vanlige virkemiddel for å garantere tjenesteleveranse innen IKT i Italia, er å sikre redundans ved hjelp av alternering av tilgjengelighet samt duplisering av infrastruktur[107].
Et villet cyberangrep på kritisk IKT-infrastruktur ble sett på som "utenkelig" bare for få år siden, men det regnes i dag som "sannsynlig" at man vil få en større hyppighet av denne typen angrep[108].

Historisk fokus på terror, avhengighet av energikilder fra naboland, en problematisk sikkerhetskultur blant brukere av IKT samt en økt bevisstgjøring på gjensidig avhengighet som følge av strømutfall danner bakteppet for IKT-organiseringen i Italia. Vi ser i det følgende nærmere på aktørene og deres funksjoner.

*De viktigste aktørene i organiseringen av IKT i Italia*
Her følger en introduksjon til de ulike aktørene fra Statsministerens Kontor til departementene, med deres respektive underorgan, samt andre aktører som har en rolle i håndteringen av IKT under såkalt "normale" omstendigheter.

Statsministerens Kontor (SMK)[109] er Italias øverste myndighet og leder blant annet Avdelingen for Innovasjon og Teknologi, Nasjonalt Senter for IKT i Offentlig Administrasjon (CNIPA) samt Avdelingen for Sivil Beskyttelse. De to førstnevnte har ikke et definert operativt ansvar i en IKT-krise, men spiller først og fremst en rolle i utformingen av strategier og beredskap.

---

[103] ISCOM (2005)*"La Sicurezza delle Reti"*, side 86.
[104] Ref. intervju med Vincenzo Merola, note 96.
[105] En slik bevisstgjøring (sensibilisering) foregår ved bruk av for eksempel opplæring av personell i offentlig administrasjon, informasjonskampanjer samt oppmuntring til å opprette egne eller sektorvise CERT'er.
[106] CNIPA (2004)*"Proposte concernenti le strategie in materia di sicurezza informatica e delle telecommunicazioni per la pubblica amministrazione"*, side 36.
[107] CNIPA (2004) *som ovenfor*,side 59.
[108] Ref. intervju med Vincenzo Merola, note 96.
[109] Statsministerens Kontor: "La Presidenza del Consiglio dei Ministri", http://www.governo.it/index.asp

SMK Avdeling for Innovasjon og Teknologi[110] har tilknyttet en Arbeidsgruppe samt en Teknisk Komité med IKT og kritisk infrastruktur som hovedtema.

Arbeidsgruppen for Beskyttelse av Kritisk IKT-infrastruktur[111] ble etablert i 2003, av minister uten portefølje for Innovasjon og Teknologi, Lucio Stanca. Gruppen består av representanter fra alle statlige departement, samt offentlige og private aktører som har en rolle i håndtering av kritisk infrastruktur, så som Innenriksdepartementet, Kommunikasjons-departementet, private operatører så som GRTN, RFI, Snam Rete Gas, Telecom Italia og Wind, samt ressurspersoner fra akademia og forskningsmiljø[112].

Også en Nasjonal Teknisk Komité for Beskyttelse av Kritisk IKT-infrastruktur[113] hører inn under Avdelingen for Innovasjon og Teknologi. Komiteen ble opprettet etter initiativ fra Minister for innovasjon og teknologi og Kommunikasjonsdepartementet i juli 2002, og plassert under ledelse av Regjeringen. Komiteen fikk blant annet som oppgave å utarbeide en nasjonal plan for IKT-sikkerhet i offentlig administrasjon, samt fremlegge et forslag til en ny organisatorisk IKT-modell. Komiteen skal videre foreslå sertifisering og drive evaluering av offentlig administrasjons fremskritt innen IKT-sikkerhet, lage retningslinjer for personell, rådgi i IKT-sårbarhetsreduksjon og være med på å garantere offentlig informasjons tjenesteleveranse og integritet. Komiteen fremla i mars 2004 et vidløftig forslag til IKT-organisering i Italia. Forslaget tar ikke med i betraktning finansielle utfordringer eller budsjettposter, og har heller ikke blitt implementert i henhold[114]. Forslaget[115], som baserer seg på et eget Nasjonalt Senter for Informasjonssikkerhet (CNSI), har i praksis kun blitt iverksatt gjennom den formelle opprettelsen av en nasjonal CERT (GovCERT.IT, se under). CNSI-strukturen er foreslått å bestå av: en koordineringsenhet, en IKT-krisehåndteringsenhet og senter for Early Warning, en utdanningsenhet, lokale, operative enheter av teknisk karakter samt et forskningssenter. I tillegg var det tenkt et nettverk av relasjoner mellom nasjonale og internasjonale organ som har kompetanse på området, samt samarbeid med politi, datatilsyn og sertifiseringsorgan[116].

---

[110] Avdelingen for Innovasjon og Teknologi: "Dipartimento per l'innovazione e le tecnologie", hjemmeside: http://www.innovazione.gov.it/

[111] Arbeidsgruppe for Beskyttelse av Kritisk IKT-infrastruktur: "Gruppo di lavoro sulla protezione delle infrastrutture critiche informatizzate".

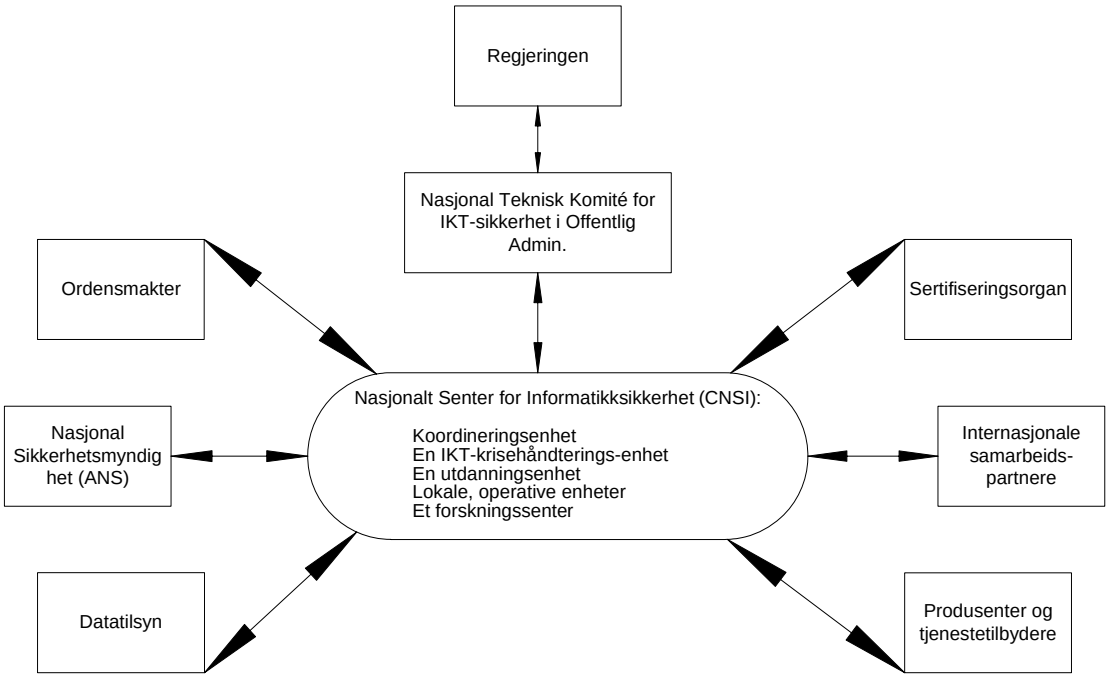
[112] Ref. intervju med Vincenzo Merola, note 96.

[113] Nasjonal Teknisk Komité for Beskyttelse av Kritisk IKT-infrastruktur: "Comitato tecnico nazionale per la sicurezza ICT": http://www.innovazione.gov.it/ita/normativa/allegati/dm_240702.pdf og http://www.cnipa.gov.it/site/it-IT/Attivit%c3%a0/Servizi_per_la_PA/Govcert.it/

[114] Ref. telefonintervju med Claudio Manganelli, CNIPA og Nasjonal Teknisk Komité for IKT i offentlig sektor, 30.08.05.

[115] *"Forslag til strategi for IKT-sikkerhet i Offentlig Administrasjon"*, CNIPA, mars 2004 www.governo.it/GovernoInforma/Dossier/sicurezza_informatica/proposte.pdf

[116] Se modell over forslaget fra Komiteen i enden av vedlegget




*Figur A.8.1 – Forslag til strategi for IKT-sikkerhet i Offentlig Administrasjon, CNIPA, mars 2004 (Kilde: [www.governo.it/GovernoInforma/Dossier/sicurezza_informatica/proposte.pdf](www.governo.it/GovernoInforma/Dossier/sicurezza_informatica/proposte.pdf) - oversatt fra italiensk)*

Forslaget er optimistisk i organisering, og så også i mål:

- Beskyttelse: høyne beskyttelsesnivået på IKT-systemer, spesielt i offentlig sektor
- Kontroll og varsling: overvåking av nett samt analyse av datainnsamling
- Reaksjon og gjenoppretting: sette inn mottiltak dersom angrep mot offentlig administrasjon, reparere skade påført offentlig sektors IKT-systemer

Så langt er det kun GovCERT.IT, en del av mål nummer to, som er formelt etablert, selv om CERT'en ikke er operativ per september 2005.

Hva som skjer videre med forslaget er vanskelig å si. Det skal gjøres opp status medio september 2005, men det er ikke så langt utsikter til økte midler som er nødvendig for at en slik organisering skal settes ut i livet[117].

SMK Avdeling for Sivil Beskyttelse[118] er organisert i ulike under-enheter. Her finner vi blant annet en egen Enhet for Risikoanalyse, en for Krisehåndtering samt en Frivillighets-enhet[119].

[117] Ref. telefonintervju med Claudio Manganelli, CNIPA og Nasjonal Teknisk Komité for IKT i offentlig sektor, 30.08.05.
[118] SMK Avdeling for Sivil Beskyttelse: "Dipartimento per la protezione civile", hjemmeside: http://www.protezionecivile.it/
[119] Organisasjonskart over Avdeling for Sivil Beskyttelse: http://www.protezionecivile.it/download/organigrammadpc.pdf

Siden 1992 har sivilt beredskap vært en del av nasjonal beredskap, og den er direkte underlagt Regjeringen. En spesiell karakteristikk ved italiensk sivilt beredskap er at den tar opp i seg representanter for hele statsorganisasjonen: fra departementene ned til de minste kommunene og til frivillige organisasjoner og deres medlemmer. Årsaken til denne organiseringen kan finnes i det karakteristiske ved italiensk territorium: regionalisme, fokus på lokal ansvarliggjøring og desentralisering har vært høyt verdsatt i Italia siden grunnloven av 27. desember 1947[120]. Sivil beskyttelse har i hovedsak vært aktiv med tanke på naturkatastrofer og andre hendelser som krever at man har mulighet til å kalle inn flere frivillige, for eksempel til opprydning etter jordskjelv og flom. Grunnlaget for en slik organisering er subsidiaritetsprinsippet (nærhetsprinsippet).

"Nasjonalt senter for IKT i offentlig administrasjon" (CNIPA[121]) ble opprettet i juli 2003, som et organ direkte underlagt Statsministerens Kontor[122]. Delegert myndighet over CNIPA ble gitt ved resolusjon av 6. mai 2005 til Minister uten portefølje, Lucio Stanca[123], og CNIPAs medlemmer utnevnes av Regjeringen[124]. CNIPA sørger for teknisk støtte til Minister for innovasjon og teknologi, og leder arbeidet i disse dager med å utarbeide en nasjonal CERT for offentlig administrasjon (GovCERT-IT: se nedenfor), etter oppdrag fra Nasjonal Teknisk Komité. Andre hovedoppgaver er PKI, elektroniske signaturer, IKT-awareness og e-government[125].

*Departementenes rolle i organiseringen av IKT i Italia*
Her følger en kort beskrivelse av departementenes rolle i IKT-hensyn, og hvert departement med tilknyttede organ blir presentert. Ikke alle har en operativ rolle i en krise, men flere driver tilsyn i for- og etterkant.

Kommunikasjonsdepartementet[126] regner seg som "svært involvert i IKT-sikkerhet", fordi IKT-infrastruktur regnes å være en kritisk infrastruktur, sammen med energi og transportsektoren. IKT-infrastruktur er essensiell med tanke på preventive tiltak og gjenoppbygging. Kommunikasjonsdepartementet fører tilsyn med post, finans og telesektoren. Departementet regulerer, koordinerer og kontrollerer implementeringen av lover[127].
Tilknyttet organ: Institutt for kommunikasjon og informasjonsteknologi: ISCOM[128]. ISCOM er et teknisk-vitenskapelig institutt underlagt Kommunikasjonsdepartementet[129]. Instituttet er til teknisk støtte for departementet, andre bedrifter samt brukerne, i utarbeidelsen av IKT standarder, rådgivning, forskning og utdanning. Det er så sent som i 2005 opprettet et eget

[120] http://www.protezionecivile.it/sistema/index.php
[121] CNIPA hjemmeside: http://www.cnipa.gov.it/site/it-IT/
[122] Ref. IDABC European Commission (2005a) og Kommunikasjonsdepartementet (2005) Resolusjon.
[123] Kommunikasjonsdepartementet (2005) Resolusjon.
[124] CNIPA struktur, http://www.cnipa.gov.it/site/it-IT/Il_Centro_Nazionale/Struttura/
[125] ENISA, http://www.enisa.eu.int/country_pages/italy/index_en.htm
[126] Kommunikasjonsdepartementet: "Il Ministero delle Communicazioni", hjemmeside: http://www.comunicazioni.it/it/.
[127] Kommunikasjonsdepartementet: http://www.comunicazioni.it, samt ENISA: http://www.enisa.eu.int/country_pages/italy/index_en.htm
[128] ISCOM, http://www.iscom.gov.it/
[129] Opprinnelig opprettet under "Dept. for Post og Telegrafi" (Ministero delle Poste e Telegrafi)

organ for sikkerhetssertifisering: OCSI[130], innenfor rammen av instituttet ISCOM. OCSI er beregnet å konsentrerer seg spesielt om IKT-sektorens system og produkt, men den er ikke operativ per august 2005. De skal sertifisere IKT-relevante produkter og tjenester til offentlig administrasjon samt utarbeide felles standarder.

Minister uten portefølje (for Innovasjon og Teknologi)[131] er en stilling som ble opprettet i juli 2001. Minister Lucio Stanca har fått delegert myndighet til å legge føringer på området innovasjon og utvikling av informasjonssamfunnet[132], samt at han er blitt tillagt ledelsen av "Nasjonalt senter for IKT i offentlig administrasjon", CNIPA.

Innenriksdepartementet[133] har ansvar for politivesen (Polizia di Stato) og sivil beskyttelse. Politiet fikk tildelt ansvaret for cyber-kriminalitet allerede i 1992, og et eget organ, Politiets post- og kommunikasjonsvesen (se under), ble utnevnt til å ta hånd om det.
Tilknyttet organ: Politiets post- og kommunikasjonsvesen[134] består av tjenestefolk som er høyt spesialisert innen IKT og jus. Organet er delt opp i 19 regionale avdelinger og 76 seksjoner på lokalt nivå. Denne avdelingen er også G8's 24/7 operative kontaktpunkt i forbindelse med internasjonal datakriminalitet[135]. Post og Kommunikasjonsavdelingen opererer på ulike IKT-områder. De overvåker og registrerer tilfeller av hacking, overvåker politisk ekstremisme i landet, ser på lovbrudd innen e-handel, illegale handlinger innen post og telefoni, kontroll av kopiering samt tiltak mot online pedofili. Politiet fikk nye retningslinjer i 1998 som åpnet for utvidede etterforskningsmetoder med hensyn til IKT. Overvåking av nett er i den senere tiden blitt intensivert i et forsøk på å få bukt med mulige cyberangrep og bruk av nett til å organisere terrorvirksomhet. En egen enhet for analyse av forbrytelse innen IKT (UACI) er satt sammen for å fokusere på cyber-crime[136]. Politiets Post og Kommunikasjonsvesen samarbeider med Kommunikasjonsdepartementet og med private aktører som har IKT som spesialområde[137].

Påvirket av hendelsene i USA 9.11.2001, og etter press mot egne myndigheter, er det nå i ferd med å bli opprettet et eget "Nasjonalt senter for beskyttelse av kritisk infrastruktur", CNIPIC[138] som skal holde til i Roma. Det utløsende element for denne opprettelsen er den nye "anti-terrorloven" av 27. juli 2005[139]. Senteret er formelt sett innstiftet, men vil ikke være operativt før slutten av september 2005[140]. Det skal representere både telekommunikasjon,

---

[130] OCSI, http://www.iscom.gov.it/ocsi.htm Organet har sin hjemmel i resolusjon av 2003, men provisoriske retningslinjer for hvordan organet skal operere ble ikke satt før i februar 2005.
[131] Minister Stanca har ikke et eget departement, men har ansvaret for området "innovasjon og teknologi". ("Ministro per l'Innovazione e le Tecnologie"), http://www.innovazione.gov.it/
[132] Kommunikasjonsdepartementet (2005) Resolusjon.
[133] Innenriksdepartementet: "Ministero dell'Interno", hjemmeside: http://www.interno.it.
[134] Politiets post-og kommunikasjonsvesen: "Servizio Polizia postale e delle communicazioni".
[135] ENISA, http://www.enisa.eu.int/country_pages/italy/index_en.htm.
[136] UACI, http://www.poliziadistato.it/pds/informatica/attivita.html.
[137] Vulpiani, Domenico, (2002)*"L'esperienza italiana nel contrasto al crimine informatico"*.
[138] Nasjonalt senter for beskyttelse av kritisk infrastruktur (CNIPIC): "Centro Nazionale di Protezione delle Infrastrutture Critiche".
[139] Innenriksdepartement (2005a) *"decr.legge 144/24 juli 2005, art. 7bis"*.
[140] Telefonintervju med Dr. Caroselli, Politiets Post og Kommunikasjonsvesen, 18.08.05.

elektrisitetssektoren, bank, post og andre som regnes blant de kritiske infrastrukturer. Rollen blir å detektere samt nøytralisere og spore kilden til trusler og angrep, både cyber og ”vanlige”. CNIPIC skal også være et slags ”operasjonssenter” der man samarbeider for å komme frem til videre strategier. CNIPIC er nå i ferd med å opprette bilaterale avtaler om planverk og beredskap med offentlige og private enheter som innehar samfunnskritiske funksjoner, så som jernbane, flyplasser og departementene. Arbeidet med å sette opp slike avtaler er forenklet ved at det nå er lovpålagt for de som innehar slike funksjoner å ha egne planverk og beredskap[141]. I forhold til en nasjonal CERT, vil CNIPIC få en overordnet rolle[142], og den nasjonale CERT’en vil da være klient under et slikt Senter.

*Tverrsektorielle organ*
Permanent arbeidsgruppe (”observatorium”) for nettverks- og telekommunikasjons-sikkerhet[143] ble etablert i 1998, som et samarbeid mellom Innenriksdepartementet, Kommunikasjonsdepartementet og Justisdepartementet. Undergruppen ”Internet subgroup” arbeider med etterforskning og juridiske utfordringer knyttet til Internett[144]. Arbeidsgruppen er organisatorisk underlagt Kommunikasjonsdepartementet[145].

*Andre aktører*
Italiensk ”Datatilsyn”[146] er organet for beskyttelse av personlige data.

*Italienske varslings- og responsenheter:*
Det er kun én operasjonell autorisert CERT på nasjonal skala per i dag, og det er CERT-IT[147]. Den vil bli supplementert på sikt med en nasjonal CERT som mest sannsynlig vil bli kalt ”GovCERT.IT”.

CERT-IT[148] er en non-profit organisasjon med støttefunksjon for sluttbrukere av ”.it”-domenet samt for nye CERT’er som settes opp i for eksempel offentlig administrasjon. CERT-IT ble opprettet ved Universitetet i Milano i 1994, og er den første italienske CERT som ble medlem av FIRST (internasjonalt ”Forum of Incident Response and Security Teams”). Varsling av angrep registreres av studentene tilknyttet universitetet ”Politecnico di Milano” og arbeider ledes av professor Danilo Bruschi. CERT-IT er autorisert av myndighetene til å drive denne virksomheten. GARR-CERT[149] er en CERT for forskningsmiljø og akademia: de varsler, tester mottiltak og assisterer i tilfelle angrep på medlemmenes system.

---

[141] Telefonintervju Roberto Setola, (Arbeidsgruppe for Beskyttelse av Kritisk IKT-infrastruktur), 1.09.05.
[142] Elektronisk kommunikasjon fra Danilo Bruschi, CERT-IT, 4.08.05
[143] Permanent arbeidsgruppe for nettverks- og telekommunikasjonssikkerhet, ”Osservatorio permanente sulla sicurezza delle reti e delle telecommunicazioni”, http://www.comunicazioni.it/it/index.php?Mn1=4&Mn2=114
[144] ENISA, http://www.enisa.eu.int/country_pages/italy/index_en.htm
[145] Roberto Setola kan fortelle at arbeidet som ble startet av Observatoriet i 1998 er blitt videreført under instituttet ISCOM. Telefonintervju Roberto Setola, se note 141.
[146] Italiensk ”datatilsyn”: ”Garante per la protezione dei dati personali”, http://www.garanteprivacy.it/garante/navig/jsp/index.jsp
[147] Ref. telefonintervju med Alessandro Bonomi, ISCOM, 2.08.05
[148] CERT-IT hjemmeside: http://idea.sec.dsi.unimi.it/
[149] GARR-CERT, http://www.cert.garr.it/

Forsvarets CERT[150] (CERT.DIFESA.IT) overvåker og informerer Forsvaret om trusler og virusangrep fra nett, og tilbyr teknisk assistanse til sine egne enheter. De overvåker jevnlig operativsystemer for å avdekke nye sårbarheter, og kommuniserer dem via et elektronisk nyhetsblad "Bollettino di Sicurezza Informatica". Forsvarets CERT samarbeider med andre nasjonale og internasjonale CERT'er.

GovCERT.IT skal bli den nasjonale CERT'en. Den er ikke operativ per august 2005, men skal "innen kort tid" etablere seg i beskyttede lokaler med 24/7 tilgjengelighet[151]. Den utpekte lederen er Gianluigi Moxedano fra CNIPA, og CERT'en vil være underlagt CNIPA ved opprettelsen. Denne CERT'en skal i utgangspunktet informere og støtte offentlig administrasjon i forebyggende arbeid. Etter hvert skal den også ta opp i seg oppgaver som varsling og datainnsamling via organet CERT-PA (P.A. står for Pubblica Amministrazione [offentlig administrasjon]), samt utdanning via et "Senter for utdanning og bevisstgjøring (sensibilisering)", i samarbeid med foreningen Ugo Bordoni. GovCERT.IT vil utføre sine oppgaver i tett samarbeid med Politiets Post og Kommunikasjonsavdeling.
GovCERT skal bli en enhet med ca 15 medarbeidere[152]. Per i dag er GovCERT.IT kun bestående av seks personer, men er allokert et to-årig budsjett på til sammen 5 millioner Euro[153]. Det foregår i dag en diskusjon blant CNIPA-medlemmer og regjeringen om hvorvidt GovCERT.IT bør gjøres om til en del av et eget direktorat ("Agenzia"), og det hevdes fra CNIPAs side at et direktorat vil være med i tråd med trenden i EU, samt at det vil forenkle finansiering og allokering av personell og andre ressurser i forhold til nasjonalt budsjett. Samtidig ville et direktorat kunne ta på seg flere viktige oppgaver, så som å arrangere øvelser, noe som ikke eksisterer per i dag.

### A.2.2 IKT-organisering i Frankrike

*De viktigste aktørene i organiseringen av IKT i Frankrike*
Organiseringen av IKT som sikkerhetselement er i Frankrike fordelt mellom Statsministerens Kontor (SMK), ved Generalsekretariatet for nasjonal beskyttelse samt departementene, da i hovedsak Innenriksdepartementet.

[150] Forsvarets CERT, http://www.difesa.it/NR/exeres/DF1CEE63-DC2B-49F8-9857-1E991A6EED59.htm
[151] Ref. telefonintervju med Alessandro Bonomi, note 162, samt http://www.cnipa.gov.it/site/it-IT/Attivit%c3%a0/Sicurezza_informatica/
[152] CNIPA (2004)*"Proposte concernenti le strategie in materia di sicurezza informatica e delle telecommunicazioni per la pubblica amministrazione"*, side 26
[153] Ref. telefonintervju med Claudio Manganelli, Se note 128.

Statsministerens Kontor[154], Generalsekretariat for Nasjonal Beskyttelse[155] (SGDN) er et tverrsektorielt sekretariat som vurderer og koordinerer arbeidsgrupper og tilknyttede organ som arbeider med ulike viktige samfunnsfunksjoner, så som innenriks- og forsvarsrelaterte emner. Tilknyttet organ: Direktorat for Sikkerhet i Informasjonssystemer[156] (DCSSI) er rådgivende i regulering, operasjoner, forskning og utvikling av sikkerhet i informasjonssystemene. Underlagt DCSSI finnes også et Sertifiseringsorgan[157] siden 1995, og et Utdanningssenter for offentlige ansatte[158] siden 1986. Utdanningssenteret tilbyr dagskurs og trainee-opphold på alt fra et par dager til to år. Tilknyttet DCSSI finnes også CERTA, den nasjonale CERT'en i Frankrike, som blir videre utdypet nedenfor.

ADAE[159], Byrå for Utvikling av Elektronisk Administrasjon (det såkalte ADELE programmet), er et tverrsektorlig organ opprettet i februar 2003. ADAE skal arbeide for utvikling av informasjonssystemene i offentlig administrasjon for bedre å kunne dekke befolkningens behov. Fire avdelinger tar for seg strategisk utvikling, relasjoner til befolkningen, relasjoner til offentlig administrasjon og en kommunikasjonsavdeling. Byrået skal etter bestemmelse av juni 2005 stille til disposisjon for Ministeren ansvarlig for Budsjett og Administrativ Reform, underlagt Departementet for Økonomi, Finans og Industri[160]. Strategien for eGovernment i Frankrike er en del av ADELE-programmet.

*Innenriksdepartementet*

Innenriksdepartementet Politiavdeling, Underavdeling for økonomi og finans, ble beriket med en egen Brigade for bekjempelse av Informasjonskriminalitet i 1994[161]. På denne basis er det opprettet et nytt spesialisert kontor i mai 2000: Hovedkontor for bekjempelse av IKT-kriminalitet (OCLCTIC)[162]. OCLCTIC er både operasjonell og strategisk, og skal både gjennomføre undersøkelser på høyt teknisk nivå, gi teknisk assistanse i straffesaker som for eksempel pedofili, og samtidig være med på opplæring og koordinering av andre avdelinger som behandler lovbrudd innen IKT. OCLCTIC er også det nasjonale kontaktpunkt for G8, Interpol og Europol.

Økonomi, Finans og Industridepartementet (MINEFI), Avdelingen for bedrifter og virksomheter (DGE)[163], skal støtte opp under innovasjon og anvendt forskning, garantere tilgjengelighet og

---

[154] Statsministerens Kontor (SMK) "Bureau du Premièr Ministre", http://www.premier-ministre.gouv.fr/en.
[155] Generalsekretariatet for nasjonal beskyttelse SGDN, "Sécretariat Générale de la défense nationale".
[156] Direktorat for Sikkerhet i Informasjonssystemer (DCSSI) " Direction centrale de la sécurité des systèmes d'information" http://www.ssi.gouv.fr/fr/dcssi/index.html.
[157] SSI, Sertifiseringssenteret med nytt mandat av 2002; http://www.ssi.gouv.fr/en/confidence/evalcertif.html.
[158] Utdanningssenter; Centre de formation à la sécurité des systèmes d'information, CFSSI
[159] Byrå for utvikling av elektronisk admin. (ADAE) www.adae.gouv.fr/article.php3?id_article=1
[160] IDABC European Commission eGovernment Observatory (2005b),"*eGovernment in France*".
[161] Brigade for bekjempelse av Informasjonskriminalitet "La Brigade Centrale de Répression de la Criminalité Informatique" (B.C.R.C.I.), http://www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic/presentation
[162] Hovedkontor for bekjempelse av IKT-kriminalitet "L'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication", http://www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic
[163] Avdelingen for bedrifter og virksomheter, "Direction Générale des Entreprises" (DGE) www.telecom.gouv.fr/presentation/presentation.htm

standarden på post og elektronisk kommunikasjon, utvikle informasjonssamfunnet og overvåke sikkerheten i industri med tanke på eksplosivt materiale, trykkluft med mer.

*Andre aktører*

Det uavhengige reguleringsbyrået for Post- og Telekommunikasjon, ARCEP[164], er en utvidelse av ART, byrået for telekommunikasjon av1996. Når postvesenet fortsetter den gradvise liberaliseringen fra januar 2006[165], vil også denne sektoren ha behov for kontroll og overvåkning via reguleringsbyrået. ARCEP skal blant annet gjennomføre markedsanalyser, tilrettelegge for fritt konkurransemarked, overvåke tilgang på kommunikasjonsteknologi (ADSL med mer), og overvåke prissetting og tilgjengelighet av tjenestene. Det føres tilsyn med ARCEP fra det franske Parlamentet, deres bestemmelser kan prøves foran en rett (le 'Cour d'appel de Paris' samt 'le Conseil d'Etat'), og Europakommisjonen kontrollerer markedsandelene.

CNIL, det franske "Datatilsynet"[166] ble opprettet ved lov av 6 januar 1978.

*Varslings- og responsenheter i Frankrike*

CERT for offentlig administrasjon er samordnet i CERTA[167]. CERTA ble lansert under Statsministerens Kontor i 1999, etter utarbeidelse og forslag av en "Tverrsektoriell komité for Informasjonssamfunnet" (CISI). CERTA, operativ siden 2000, overvåker nett og sårbarheter, og både varsler og assisterer ved behov. CERTA ser seg selv som et "tillitsorgan" både for offentlig administrasjon og andre administrative organiseringer, og selv om den er opprettet for å varsle og bistå offentlig etater, kommer varslene ut til befolkningen "bare noen dager etter"[168].

Andre CERT'er i Frankrike er Cert-IST[169] for industri, service- og tertiærnæringene (IST). Den ble opprettet i 1999 av fire store bedrifter; Alcatel, CNES, ELF og France Télécom. Det er per i dag kun France Télécom, Sanofi Synthelabo og Alcatel-gruppen som har adgang til alle tjenester, mens andre medlemmer får adgang til utvalgte deler. Cert-IST skal være objektiv, garantere konfidensialitet og inneha overblikk over sikkerhetssituasjonen til enhver tid. LEXSI[170] er en kommersiell CERT, mens CERT-RENATER[171] er forbeholdt de over 600 brukerne av telekommunikasjonsnettverket Renater, det vil si teknologibedrifter, utdanningsinstitusjoner og forskningsmiljø som er medlemmer av GIP-RENATER[172].

---

[164] Reguleringsbyrået for Post-og Telekommunikasjon "Autorité de régulation des communications électroniques et des postes", www.arcep.fr
[165] Lov 2005-516, 20 mai 2005, Publisert i *JO21.05.2005*
[166] Fransk "datatilsyn", "Commissione Nationale pour l'Informatique et la Libertée", http://www.cnil.fr/
[167] CERTA, www.certa.ssi.gouv.fr/certa/certa.html
[168] Dokument fra Direktoratet DCSSI (SGDN), publisert på: http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf/viewHtml/index/$FILE/fiche%20application%20lignes%20directrices%20-%20mars%202004.pdf, side 2.
[169] CERT-IST, www.cert-ist.com/francais/presentation/presentation2_fr.htm
[170] LEXSI, "Laboratoire d'Expertise en Sécurité Informatique", http://www.lexsi.fr/
[171] CERT-RENATER, www.renater.fr/Securite/CERT_Renater.htm
[172] GIP-RENATER "Reseau National de télecommunications pour la Technologie, l'Enseignement et la Recherche".

## A.3 IKT-aktører med kontaktinformasjon: Italia, Frankrike og EU

### A.3.1 IKT-aktører Italia

| | |
|---|---|
| Kommunikasjons-Departementet (Il Ministero delle Communicazioni) | http://www.comunicazioni.it/it/<br>Ing. *Luisa Franchina*, Direzione generale per la regolamentazione e la qualità dei servizi,<br>Tel. +39 06 54442191, luisa.franchina@comunicazioni.it<br><br>Også: Ing. *Franco Guida*<br>Ing. *Perucchini*, (Fondazione Ugo Bordoni) chini@fub.it |
| ISCOM (Institutt til teknisk støtte) | http://www.comunicazioni.it/it/index.php?Mn1=9<br>Dr. *Alessandro Bonomi*:<br>Tel. +39 0654 444082, alessandro.bonomi@istsupcti.it<br>Fax: +39 06 59 13 536<br><br>Dr. *Giovanni Desirò*<br>Tel: +39 06 54 44 23 24, desiro.giovanni@istsupcti.it |
| OCSI (Organ for sertifisering, underlagt ISCOM) | http://www.ocsi.gov.it/<br>Direktør *Luisa Franchina* (Kommunikasjonsdept.) |
| Politiet (Polizia Postale e delle Communicazioni) | http://www.poliziadistato.it/pds/informatica/index.htm<br>*Dr. Caroselli*: +39 06 46 53 01 12<br>(”Servizio Polizia Postale e delle Communicazioni”) |
| Minister uten portefølje for Innovasjon og Teknologi (Ministro per l’Innovazione e le Tecnologie) | http://www.innovazione.gov.it/<br>Minister: *Lucio Stanca* |
| Nasjonalt senter for informatikk i offentlig administrasjon (CNIPA) | http://www.cnipa.gov.it/<br><br>President: *Livio Zoffoli*, Tel. +39 0685264206<br>segreteriapresidente@cnipa.it<br><br>Direktør: *Carlo D’Orta*, Sentralbord: Tel.+39 06852641<br>segreteriadirettore@cnipa.it<br><br>Kontaktperson: *Claudio Manganelli*, Sentralbord: Tel.+39 06852641 manganelli@cnipa.it |

| | |
|---|---|
| | Manganelli er også President i ”Nasjonal Teknisk Komité for IKT i offentlig administrasjon” siden 2003 |
| *Arbeidsgruppe* for Beskyttelse av Kritisk IKT-infrastruktur (Gruppo di lavoro) | *Vincenzo Merola*, Koordinator<br>Tel. +39 06 84 56 34 32<br>Mobil: +39 347 3539 425<br>v.merola@governo.it<br><br>*Roberto Setola*<br>r.setola@governo.it<br>Mobil: +39 329 4308445 |
| Nasjonal Teknisk Komité for Beskyttelse av Kritisk IKT-infrastruktur (Comitato tecnico nazionale) | President: *Claudio Manganelli*, Sentralbord: Tel.+39 6852641<br>manganelli@cnipa.it<br><br>Medlem: *Danilo Bruschi*, Tel. +39 0250 316260<br>bruschi@dico.unimi.it<br>Medlem: *Vincenzo Merola* v.merola@governo.it |
| Italiensk ”Datatilsynet” (Garante per la protezione dei dati personali) | http://www.garanteprivacy.it/garante/navig/jsp/index.jsp<br><br>*Luigi Montuori*<br>Tel: +39 06 696771 |
| CERT-IT | http://idea.sec.dsi.unimi.it/<br><br>*Danilo Bruschi*<br>Tel. +39 0250 316260<br>bruschi@dico.unimi.it<br>Bruschi sitter også i den Nasjonale Tekniske komiteen (se over) |
| GOVCERT.IT (nasjonalt CERT) | http://www.cnipa.gov.it/site/it-IT/Attivit%c3%a0/Servizi_per_la_PA/Govcert.it/<br><br>Leder: *Gianluigi Moxedano* sicurezzaICT@cnipa.it<br>Tel sentralbord (CNIPA): +39 06852 641<br>Tel direkte: +39 06852 472 |
| Garr-CERT (forskning og akademia) | http://www.cert.garr.it |

### A.3.2 IKT-aktører Frankrike

| | |
|---|---|
| DCSSI (underlagt SGDN; Generalsekretariat for Nasjonal Beskyttelse) | http://www.ssi.gouv.fr/fr/dcssi/index.html<br><br>*Matthieu Grall* Tel. +33 171 7584 33<br>communication.dcssi@sgdn.pm.gouv.fr<br><br>Tel. sentralbord: (33) 01 41 46 37 00 |
| ADAE (Byrå for Utvikling av Elektronisk Administrasjon) | www.adae.gouv.fr/article.php3?id_article=1<br><br>Direktør: *Jacques Sauret*<br>jacques.saurat@pm.gouv.fr |
| OCLCTIC (Hovedkontor for bekjempelse av IKT-kriminalitet) | www.interieur.gouv.fr<br><br>Tel +33 149 27 49 27 |
| ARCEP (Reguleringsbyrået for Post- og Telekommunikasjon) | www.arcep.fr<br>courrier@art-telecom.fr<br><br>Tel sentralbord + 33 1 40 47 70 00 |
| CNIL (”Datatilsynet”) | http://www.cnil.fr/<br><br>Tel. Sentralbord +33 1 53 73 22 22 |
| CERTA | www.certa.ssi.gouv.fr/certa/certa.html<br>certa-svp@certa.ssi.gouv.fr<br><br>Tel. Sentralbord :+33 1 71 75 84 50 |
| DGE (Avdelingen for bedrifter og virksomheter/ Økonomi, Finans og Industridepartementet) | http://www.telecom.gouv.fr/<br>presentation/presentation.htm<br><br>Tel. Sentralbord +33 1 44 87 17 17 |

### A.3.3 IKT-aktører EU

| | |
|---|---|
| ENISA | *Andrea Servida*<br>andrea.servida@cec.eu.int<br><br>ENISA-direktør: *Andrea Pirotti*<br>+32 2299 3969 |
| JRC Joint Research Centre | *Marcelo Masera*<br>Tel. +39 0332 789238<br>marcelo.masera@jrc.it<br><br>*Alberto Stefanini*<br>alberto.stefanini@jcr.it |

## A.4 Generelt informasjonsgrunnlag

### A.4.1 Bøker, rapporter o.l.

ADELE (2004), *"Plan de renforcement de la sécurité des systèmes d'information de l'Etat (2004-2007)"* (PRSSI), [Plan for styrking av beredskapssikkerhet i informasjonssystemene i offentlig sektor], 10.03.2004 SMK/ ADELE, Frankrike
http://www.ssi.gouv.fr/site_documents/PRSSI/PRSSI.pdf

AEEG (2004), *"Resoconto dell'Attività Conoscitiva in Ordine alla Interruzione del Servizio Elettrico Verificatasi il 28 Settembre 2003"* , Rapport, AEEG Autorità per l'energia elettrica e il Gas [Gass- og energimyndighetene], 9 juni 2004,
www.autorita.energia.it/com_stampa/index.htm

BBC (2004): "Panorama: London under attack", tv-program sendt 16. mai 2004

Buzan, B., Waever, O., de Wilde, J. (1998), *Security: A New Framework for Analysis*, Lynne Rienner Publishers

CNIPA (2004)*"Proposte concernenti le strategie in materia di sicurezza informatica e delle telecommunicazioni per la pubblica amministrazione"* [Forslag til strategi for IKT-sikkerhet i Offentlig Administrasjon]", mars 2004 Italia
www.governo.it/GovernoInforma/Dossier/sicurezza_informatica/proposte.pdf

CRN (2004), *International CIIP Handbook – An Inventory and Analysis of Protection Policies in Fourteen Countries*, tilgjengelig på
http://www.isn.ethz.ch/crn/_docs/CIIP_Handbook_2004_web.pdf

Daclon, Corrado Maria (2004), intervju med Vincenzo Merola, *Analisi Sicurezza*, Nr. 47/48, juli-august 2004, www.analisidifesa.it/articolo.shtm/id/4375/IT

DCSSI (2004) *"Guide pour l'élaboration d'une politique de sécurité de système d'information"* [Guide til en politisk strategi for sikkerhet i informasjonssystem], SMK/SGDN/DCSSI,
http://www.ssi.gouv.fr/fr/confiance/documents/Methodes/PSSI-Section4-ReferencesSSI-2004-03-03.pdf

DCSSI (2004), "Mise en oeuvre en France des lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information adoptées le 25 juillet 2002", Retningslinjer,
http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf/viewHtml/index/$FILE/fiche%20application%20lignes%20directrices%20-%20mars%202004.pdf

ENEL (2004) "*Energia e Ambiente"*, Rapport 2004
http://www.enel.it/attivita/ambiente/energiaelettrica/doc/tab_dipendenza_importazioni.pdf

Gruppo di lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate (2004), [Permanent arbeidsgruppe] *"Protezione delle infrastrutture critiche informatizzate"*, Rapport, mars 2004 (rapporten kan fåes ved å kontakte Roberto Setola, r.setola@governo.it)

Hagen, J. og Fridheim, H. (2005), *Hva er kritisk infrastruktur?*, FFI/notat-2005-00363

IDABC European Commission eGovernment Observatory (2005a),*"e-Government in Italy"*, Periodisk Rapport juni 2005, http://www.innovazione.gov.it/ita/ministro/dpcm_050506.shtml

IDABC European Commission eGovernment Observatory (2005b),*"eGovernment in France"*, Periodisk Rapport juni 2005, http://europa.eu.int/idabc/servlets/Doc?id=21009

Innenriksdepartement (2005a) *"decr.legge 144/24 juli 2005, art. 7bis"*, Italia http://www.interno.it/legislazione/pages/pagina.php?idlegislazione=648

Innenriksdepartementet (2005b),*"Lo stato della sicurrezza in Italia"* [Sikkerhetstilstanden i Italia], Rapport, 16.08.2005, http://www.interno.it/assets/files/8/20058141464.pdf

ISCOM (2005)*"La Sicurezza delle Reti: dall'analisi del rischio alle strategie di protezione"*, mars 2005, Roma, Italia

Johansen, I. (2004), *Cyberspace som slagmark: Refleksjoner omkring Internett som arena for terrorangrep*, FFI/Rapport 2004/01666

Kjølberg, A. (2003), *Når Religionen Blir Truet: årsaker til og konsekvenser av islamistiske gruppers sikkerhetisering av religion*, FFI/Rapport 2003/00330

Kommunikasjonsdepartementet (2005), Resolusjon av 6 mai 2005, http://www.innovazione.gov.it/ita/ministro/dpcm_050506.shtml

La Repubblica (2003), *"Italia avamposto dei terroristi"*, 3 april 2003 http://www.repubblica.it/online/politica/italiairaqtredici/frattini/frattini.html

OECD (2003) *"Survey on the Implementation of the OECD guidelines for the security of Information systems and Networks: Towards a culture of Security"*, Undersøkelse, DSTI/ICCP/REG(2003)8/FINAL, juli 2003, nedgradert juni 2004 http://webdominio1.oecd.org/COMNET/ST/IccpSecu.nsf?OpenDatabase

Perrow, C. (1984), *Normal Accidents – living with high-risk technologies*, Basic Books, Inc., Publishers, New York

St.meld. nr. 17 (2001-2002), *Samfunnssikkerhet – veien til et mindre sårbart samfunn*, Det Kongelige Justis- og Politidepartement.

St.meld. nr. 37 (2004-2005), *Flodbølgekatastrofen i Sør-Asia og sentral krisehåndtering*, Det Kongelige Justis- og Politidepartement.

St.meld. nr. 39 (2003-2004), *Samfunnssikkerhet og sivilt-militært samarbeid*, Det Kongelige Justis- og Politidepartement.

Svenska Kraftnät Beredskapsstaben (2005), *"Erfarenheter av krisehanteringsarbetet efter Gudrun"*, PM 25.04.2005

Vulpiani, Domenico, (2002) Direktør (”Dirigente”) i italiensk Politi og Direktør for Politiets Post-og Kommunikasjonsvesen, *”L’esperienza italiana nel contrasto al crimine informatico”*, Innlegg, Internasjonal konferanse om Cyberkriminalitet, Palermo, Italia, oktober 2002

### A.4.2 Intervjuer

*Norske aktører*

Direktoratet for Samfunnssikkerhet og Beredskap, 21.juli 2005

Forsvarets Sikkerhetsavdeling (telefon), 11.august 2005

Forsvarsdepartementet, 12.august 2005

Fylkesmannen Oslo og Akershus, 1.august 2005

Hafslund, 18.august 2005

Justisdepartementet (telefon), 2.august 20005

Moderniseringsdepartementet (telefon), 10.august 2005

NorCERT, 15.juli 2005

Norges Vassdrags- og Energidirektorat, 26.juli 2005

Nye Kripos/Datakrimavdelingen (telefon), 11.august 2005

Oljedirektoratet (telefon), 12.august 2005

Politiets Sikkerhetstjeneste (telefon), 12.august 2005

Post- og Teletilsynet, 9.august 2005

Samferdselsdepartementet, 9.august 2005

Statnett, 10.august 2005

Telenor (telefon), 3.august 2005

Varslingssystem for Digital Infrastruktur, 15. juli 2005

*Utenlandske aktører*

Anonym funksjonær, offentlig sektor, Nederland, august 2005

Bonomi, Alessandro, (ISCOM), Italia, 2.08.05 og 5.09.2005

Bruschi, Danilo (CERT-IT) Italia, 4.08.05 (Elektronisk kommunikasjon)

Dr. Caroselli (Politiets Post og Kommunikasjonsvesen), Italia, 18.08.05.

Ferrazza, Marcellino (Kommunikasjonsdepartementet), Italia, 19.08.05

Grall, Matthieu (DCSSI/SGDN, SMK Bureau Conseil), Frankrike, 01.09.05

Luisa, Franchina (Kommunikasjonsdepartementet), Italia, 3.08.05

van der Luit, Ronald (Ministry of Economic Affairs), Nederland, 9.08.05

Manganelli, Claudio (CNIPA og Nasjonal Teknisk Komité for IKT i offentlig sektor), Italia, 30.08.05.

Masera, Marcello (JRC) Italia, 28.07.05

van Merkom, Simon (Ministry of Economic Affairs), Nederland, 19.08.05

Servida, Andrea (ENISA), 25.08.05

Setola, Roberto (Arbeidsgruppe for Beskyttelse av Kritisk IKT-infrastruktur), Italia, 1.09.05.

## Litteratur


(1) CTV.CA: http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1121363949740_36/?hu

(2) Justis- og politidepartementet (2002): Stortingsmelding 17 - "Samfunnssikkerhet – Veien til et mindre sårbart samfunn"

(3) DSB (2005): http://www.dsb.no/article.asp?ArticleID=1033&Rank=1&SubRank=3

(4) Hagen J, Fridheim H (2005): Hva er kritisk infrastruktur?, FFI/NOTAT-2005/00363, Forsvarets forskningsinstitutt

(5) Bjørgo T, Hovden J, Olsen O E (2005): Økt sikkerhet krever kunnskap, Kronikk i Aftenposten 3/8-2005

(6) Buzan B, Waever O, de Wilde J (1998): Security - A New Framework for Analysis, Lynne Rienner Publishers, 1998

(7) Neumann I B, Offerdal K (2003): Kortinfo fra DNAK 7, 2003, side 2: http://www.atlanterhavskomiteen.no/publikasjoner/andre/kortinfo/2003/pdf/Kortinfo7_2003.pdf

(8) Perrow C (1984): Normal Accidents – living with high-risk technologies, Basic Books Inc. Publishers, New York, 1984

(9) Albrechtsen E (2005): Forelesningsnotater i etterutdanningskurset ”Sikkerhet – analyse og ledelse”, NTNU 28.april 2005

(10) Telecom Italia: http://www.comunicazioni.it/it/index.php?Mn1=4&Mn2=121

(11) ODIN: http://odin.dep.no/jd/norsk/aktuelt/nyheter/012101-990637/dok-bu.htm

(12) VG (2005): Artikkel 8. september, http://www.vg.no/pub/vgart.hbs?artid=107232

(13) NATO (1949): North Atlantic Treaty, Washington 4 april 1949, http://www.nato.int/docu/basictxt/treaty.htm

(14) ODIN: http://odin.dep.no/ud/norsk/dep/ansvar/bn.html

(15) Sikkerhetsloven: http://www.lovdata.no/all/hl-19980320-010.html

(16) CNIPA (2004): " Proposte concernenti le strategie", side 19

(17) Evalueringsutvalget (2005): "Rapport fra evalueringsutvalget for flodbølgekatastrofen i Sørøst-Asia”, http://www.evalueringsutvalget.no

(18) Justis- og politidepartementet (2000): Et sårbart samfunn, NOU 2000:24