Sikkerhet og sårbarhet i elektroniske samfunnsinfrastrukturer – refleksjoner rundt regulering og tiltak

Kjell Olav Nystuen og Håvard Fridheim

Forsvarets forskningsinstitutt (FFI)

29. mars 2007

FFI-rapport 2007/00941

1014

ISBN 978-82-464-1170-5

Emneord

Informasjonssikkerhet

Samfunnssårbarhet

Godkjent av

Håvard Fridheim	Prosjektleder
Jan Erik Torp	Avdelingssjef

Sammendrag

Rapporten tar utgangspunkt i arbeidet med en serie med analyser og studier som i hovedsak er gjennomført i BAS-prosjektserien på FFI. Arbeidet har i stor grad vært rettet inn mot å identifisere og analysere tiltak for å møte trusler mot samfunnets viktigste infrastrukturer, som telekommunikasjon, kraftforsyning og transport. Viktige utfordringer i disse arbeidene har vært å vurdere hvor sårbare ulike IKT-infrastrukturer i samfunnet er overfor ulike typer påkjenninger, og hvilke tiltak som er relevante for å øke sikkerheten og robustheten i dem.

Etter at disse prosjektene har levert sine resultater har det imidlertid vært stort fokus på de foreslåtte tiltakene som har vært lagt frem. Det har i langt mindre grad vært fokus og interesse for de bakenforliggende analysemetodene og prosessene som ble benyttet for å komme frem til tiltakene. Dette er et forhold som vi mener er uheldig. Særlig innenfor området sikkerhet innen IKT-infrastruktur skjer utviklingen så raskt at holdbarheten av slike anbefalinger er svært kort.

I rapportens første del skisseres en del forhold og utviklingstrekk rundt regulering av sikkerhet og robusthet i EKOM- og IKT-systemer de senere årene. Deretter beskrives en del utfordringer i forhold til sikkerhet og beredskap i en nasjonal kontekst. Her legges det vekt på sikkerhetspolitiske, markedsmessige og teknologiske utviklingstrekk de siste ti årene. Avslutningsvis drøftes myndighetenes mulige rolle innen IKT- og EKOM-sikkerhet.

Med dette utgangspunktet gis i rapportens siste del et innspill til innretning for et regime innen sikkerhet og sårbarhet i elektroniske infrastrukturer. Her beskrives en prosess med tre hovedpunkter som på tvers av sektorer og ansvarsområder kan gi nødvendig helhet og konsistens ved utvikling av strategier og tiltak. Hovedpunktene i prosessen er:

1. Det avklares hvilke utfordringer og trusselbilde sikkerhetsarbeidet skal rettes mot – hva er egentlig utfordringene for arbeidet med nasjonal IKT-sikkerhet?
2. Det bestemmes klare ambisjonsnivåer og målsettinger – hvor vil vi konkret med sikkerhetsarbeidet?
3. Det identifiseres hvilke virkemidler som basert på relevans og realisme kan bidra til å oppfylle målsettingen, og det måles hvilken effekt og kostnad disse har.

Det er sentralt at denne prosessen inneholder egenskaper for å gi sporbarhet av de beslutninger som tas. Som innledning til dette gis en kort vurdering av forhold rundt sikkerhet og beredskap innen EKOM-sektoren etter at BAS2-prosjektt la frem sine forslag i 1999.

English summary

This report is based on the work in the BAS project series at FFI. The BAS projects have primarily identified and analyzed measures to reduce vulnerabilities to threats against critical infrastructures, such as telecommunication, electrical power supply and transport services. Important challenges have been to assess how vulnerable different ICT infrastructures are against different types of threats, and which measures are relevant to increase security and robustness in the infrastructures in a holistic view.

After each project has delivered its results, much focus has been placed on the proposed measures. Unfortunately, there has been little or no interest in the underlying methods and processes used to reach the proposals. This is unfortunate, since ICT security issues are subject to rapid changes, and since the validity of the proposed measures are relatively short.

In the first part of the report, recent developments regarding security and robustness in telecommunication and ICT systems are discussed. Following this, a number of challenges for ICT security and emergency preparedness are discussed in a national context. Emphasis is put on challenges related to security policy, market-driven economies and technological developments the last ten years. Possible roles for the national authorities in the ICT security work are discussed.

The last part of the report proposes a new regime for security and robustness in electronic infrastructures. This regime consists of a process in three stages. The process ensures that strategies and measures for ICT security can be developed across different societal sectors and areas of responsibility, in a holistic and consistent way. The three stages are:

1. Identify the challenges and threats that the ICT security work shall counter. What are the challenges for the work with national ICT infrastructure security?
2. Determine clear ambitions, objectives and goals for the security work What are we trying to achieve?
3. Identify measures, that based on relevance and realism can contribute in a positive way to the main objectives with the security work. Effectiveness and cost of the measures has to be measured against set goals.

This process would ensure that decisions and measures for the national work on ICT infrastructure security will be robust, traceable and valid for set objectives and goals. To support this claim, a brief assessment of issues related to security and emergency preparedness in the national telecommunication sector the last years is given.

Innhold

Forord

Med utgangspunkt i de problemstillinger som er behandlet i BAS5-prosjektet og sett i lys av andre prosjekter med beslektet tema, ble det funnet et behov for å formidle noen refleksjoner rundt temaet sikkerhet og beredskap i IKT- og EKOM-tjenester og spørsmål knyttet til nasjonal regulering. Rapporten er ikke en forskningsrapport, men en oppsummering av erfaringer fra ulike studier gjennom en 10-årsperiode. Denne rapporten inngår formelt som del av sluttrapporteringen fra BAS5 prosjektet, selv om den ikke er et direkte resultat av en målsetting gitt av prosjektavtalen.

1 Innledning

Forsvarets forskningsinstitutt (FFI) har gjennom mange år arbeidet med ulike sider av sikkerhet og robusthet i IKT[1]-baserte infrastrukturer. Dette arbeidet har vært innrettet mot flere problemstillinger både innenfor sivil og militær sektor. Viktige utfordringer i arbeidet har vært å vurdere hvor sårbare ulike IKT-infrastrukturer i samfunnet er overfor ulike typer påkjenninger, og hvilke tiltak som er relevante for å øke sikkerheten og robustheten i dem.

For å svare på slike spørsmål, er det viktig å ha klarhet i følgende spørsmål:

- Hvilke typer utfordringer kan IKT-infrastrukturene bli utsatt for, og hvilke av disse skal være dimensjonerende for å kunne si at sikkerhet og robusthet er ivaretatt i tilstrekkelig grad?
- Hva skal ambisjonsnivået for sikkerhetsarbeidet være?
- Hvilke konkrete roller og oppgaver skal ulike aktører knyttet til IKT-sikkerhetsarbeidet ha?

Så lenge slike forhold er avklart, er det mulig å gjennomføre strukturerte analyser som bidrar til økt sikkerhet og robusthet i ulike typer IKT-infrastrukturer.

Denne rapporten tar utgangspunkt i en oppfatning av at forholdene som er presentert over *ikke* er godt nok avklart i dag. Dette skyldes ikke minst mangfoldet av sikkerhetspolitiske, markedsmessige og teknologiske utviklingstrekk de siste ti årene, som raskt har skapt utfordringer for beredskapsarbeidet som er vesensforskjellige fra de man hadde tidligere. Med bakgrunn i disse utviklingstrekkene har vi også en oppfatning av at man innen deler av forvaltningen ikke helt tar inn over seg de utfordringene som ligger i å utvikle et balansert og konsistent sikkerhetsregime innen IKT-baserte samfunnsinfrastrukturer på nasjonalt nivå. Å utvikle tiltak innenfor dette området krever ikke minst en metodisk og helhetlig tilnærming. Erfaringene fra forskningsprosjektet ”Beskyttelse av samfunnet (BAS) 5 – Sårbarhet i kritiske IKT-systemer” forsterker bare denne oppfatningen [1].

Målsettingen med denne rapporten er, med bakgrunn i arbeidet med BAS5-prosjektet og tidligere analysearbeider innen infrastruktursikkerhet, å gi en vurdering av hvilke konsekvenser utviklingen kan få for gjennomføring av sikkerhets- og beredskapstiltak innen IKT-området, spesielt på et nasjonalt nivå. Dette er et uhyre komplekst tema, som ikke kan behandles fullt ut i løpet av et fåtall sider. Det understrekes derfor at denne rapporten er ment som et *innspill til debatt*, for å bidra til nødvendige avklaringer. Rapporten gir en argumentasjon som i hovedsak er basert på *teknologiske perspektiver* på problemene som reises.

[1] Informasjons- og kommunikasjonsteknologi

2 Bakgrunn: Om IKT, EKOM, sikkerhet, robusthet og regulering

Det er to begreper som benyttes til dels om hverandre i denne rapporten: *IKT og EKOM*. EKOM står for elektronisk kommunikasjon, mens IKT står for informasjons- og kommunikasjonsteknologi. I rapporten brukes IKT som en generell term, mens EKOM brukes om tjenesten som utgjør K-en i IKT. Med andre ord inngår EKOM i de fleste systemer basert på IKT. Det er imidlertid verdt å merke seg at interne IKT-baserte tjenester er svært viktige for utviklingen og produksjonen av EKOM-tjenester. Komplekse IKT-tjenestestrukturer ligger til grunn for selv en enkel EKOM-tjeneste som telefoni. Disse to begrepene henger dermed svært tett sammen. Flere av eksemplene som omtales i denne rapporten vil være hentet fra EKOM-verdenen, men de vil etter vårt syn ha allmenn gyldighet for IKT.

Det er flere tilnærmingsmåter for å oppnå *sikkerhet og robusthet* i IKT- og EKOM-systemer. Det første man vil oppdage er at ulike kompetansemiljøer ser ganske ulikt på problemstillingen. Teknologen vil ofte søke å legge inn sikkerhetsfunksjoner i systemet, for å øke sikkerheten og robustheten i tjenesteleveransen fra systemet. Problemstillinger vil ofte være knyttet til hvilke tiltak som må gjøres i infrastrukturen til tjenesteleverandøren, og hva som sluttbrukerne selv må gjøre. Juristen og økonomen vil nok kunne ha andre tilnærmingsmåter for hvordan de ulike tjenestene kan sikres, med utgangspunkt i andre modeller.

Et problem som raskt vil komme i fokus er *hvem* som skal betale for økt sikkerhet, siden nødvendige tiltak i mange tilfeller ikke gir noen åpenbar funksjonell merverdi for brukeren i hverdagen. Så lenge man er innenfor en tjenesteleverandørs ansvarsområde, vil avveiningen mellom tilnærmingsmåter normalt være basert på en kostnyttetilnærming, som virksomheten selv foretar ut fra i hovedsak bedriftsøkonomiske hensyn. Sikkerhetsarbeidet gjennomføres da uten at det nødvendigvis tas spesielle hensyn til ulike oppfatninger av hva som er ”samfunnets beste”.

Det kan imidlertid hevdes at spørsmålet om et tilstrekkelig nivå av sikkerhet og beredskap i samfunnsviktige IKT-systemer er et viktig samfunnsanliggende, og noe som ikke bare kan være drevet av kommersielle kriterier. Dette krever imidlertid klarhet i hvilke krav samfunnet kan og bør stille, hvilke virkemidler samfunnet kan ta i bruk og hvilke aktører som har en rolle for å bidra til økt sikkerhet i IKT-infrastrukturer. I Norge har offentlige myndigheter lenge hatt sentrale roller i arbeidet med IKT- og EKOM-sikkerhet, gjennom blant annet lovmessig regulering og tilsynsvirksomhet. Et viktig spørsmål i resten av rapporten er hvordan denne rollen kan ivaretas i tiden fremover.

Rapporten har følgende struktur:

- Innledning og bakgrunn gis i kapittel 1 og 2.
- Kapittel 3 presenterer et historisk blikk på arbeidet med IKT- og EKOM-sikkerhet i Norge.

- I kapittel 4 drøftes noen av de prinsipielle utfordringene for arbeidet med IKT- og EKOM-sikkerhet i dag.
- I kapittel 5 skisseres et forslag til bruk ved utvikling av nasjonale regimer for IKT-og EKOM-sikkerhet. Som innledning drøftes sider ved prosessen etter BAS2-prosjektet [2], med hensikt å peke på noen forhold som er av relevans for problemstillingen.
- I kapittel 6 gis noen avsluttende merknader

3 Hvordan har regulering av EKOM-sikkerhet skjedd historisk?

I dette kapittelet skisseres sider ved hvordan sikkerhet innen EKOM har blitt regulert i Norge frem til i dag. Erfaringene her vil i stor grad også være gyldige for kritiske IKT-systemer som benyttes for produksjon av en mengde varer og tjenester i samfunnet, som kraftforsyning, prosessindustri eller samferdsel.

På bakgrunn av erfaringene fra 2. verdenskrig, utviklet norske myndigheter et eget Totalforsvarskonsept for beskyttelse av landet mot store påkjenninger, i sin ytterste konsekvens en invasjon fra Sovjetunionen. Sikring av landets teletjenester[2] var en viktig forutsetning for at dette konseptet kunne fungere.

Frem til på 90-tallet ble offentlige telekommunikasjonstjenester levert av en offentlig forvaltningsbedrift – Televerket. Til tross for at man hadde egne telenett med høyere krav til robusthet innen jernbanen, Forsvaret og kraftforsyningen, var offentlige teletjenester likevel en svært viktig del av datidens totalforsvar. Televerket hadde da også en sterk intern enhet som tok seg av behovene til Totalforsvaret. En rekke til dels svært tunge sikringstiltak ble løpende bygget inn i datidens telenett, for eksempel fjellanlegg og EMP-beskyttelse[3]. Enheten i Televerket hadde også god faglig kontakt med de viktigste aktørene innen Totalforsvaret, som var avhengig av teletjenester i en beredskapssituasjon. I tillegg til Forsvaret selv, inkluderte dette institusjoner som luftfartsmyndighetene, kraftforsyningen og NRK. Dette var organisert under Totalforsvarets sambandsnemnd (TSBN), under Televerkets ledelse.

På 90-tallet ble Televerket, med bakgrunn i en politisk beslutning, omorganisert fra å være statlig forvaltningsbedrift til å gå inn i en privat selskapsform med staten som eneeier, og til slutt et

[2] Begrepene elektronisk kommunikasjon (EKOM) og telekommunikasjon er ofte brukt om hverandre. EKOM er et nytt begrep som først ble tatt i omfattende bruk i forbindelse med utarbeidelse av EKOM-loven, som erstatter den tidligere Teleloven. EKOM brukes i denne rapporten fordi det er en mer presis beskrivelse av funksjoner og tjenester for elektronisk formidling av informasjon. Telekommunikasjon er fremdeles et mye brukt begrep, men oppfattes ofte som snevrere og mer opphengt i tidligere systemer og tjenester. I en historisk beskrivelse er det imidlertid mest korrekt å benytte begrepet tele/telekommunikasjon.

[3] Elektromagnetisk puls (EMP) har kortvarig varighet med svært høy energi, som dersom den er kraftig nok kan forårsake funksjonsforstyrrelse og ødeleggelse av elektronisk ustyr. EMP som er generert ved avsetning av kjernefysisk ladning over atmosfæren vil kunne få svært stort skadeomfang over store geografiske områder på bakken. Beskyttelsestiltak mot EMP er omfattende og kostbare. EMP avgir ikke trykk og er dermed ikke skadelig for mennesker og fysiske gjenstander.

regulært aksjeselskap med også private aksjonærer. Samtidig ble telemonopolet på de fleste områder avsluttet. Gjennom de såkalte Spesielle samfunnspålagte oppgaver (SSO) skulle imidlertid beredskapsansvaret fra Televerket videreføres i Telenor. Det ble også opprettet et Post- og teletilsyn[4] for å ta seg av forvaltningsoppgaver innen post- og telesektoren. Som følge av samme utvikling valgte man etter hvert å nedlegge det Telenor-ledede TSBN, og i stedet opprette Totalforsvarets råd for sikring av tele- og informasjonstjenester (TRSTI), under ledelse av Post- og teletilsynet.

Både TSBN og TRSTI besto av ledere og eksperter avgitt fra i hovedsak statlige aktører som var tunge brukere av teletjenester. Ved opprettelsen av TRSTI ønsket man å få til en videreføring av sikringstiltak i telenettet, og sørge for at nye tiltak ble iverksatt i tråd med løpende utvikling på området. Begge organene hadde viktige roller innen informasjonsutveksling og kompetanseutvikling.

Det ble imidlertid etter hvert åpenbart at verken TSBN eller TRSTI hadde mulighet til å få gjennomført saker etter at avmonopoliseringen i telesektoren var kommet godt i gang. Det oppsto en restanseliste over uavsluttede saker i TSBN som til slutt var ganske omfattende, og som dels ble en arv til det påfølgende TRSTI. Til tross for en ambisiøs start, gikk utviklingen på begynnelsen av 2000-tallet i retning av at sakslista i TRTSI ble ganske tynn. Muligens var dette en følge av at man innså at handlingsrommet var blitt svært begrenset.

På samme tid som TSBN var i ferd med å bli avløst av TRSTI, avsluttet FFI prosjektet ”BAS2 – Sårbarhet i offentlig telekommunikasjon”, et større arbeid som så på nasjonal telesikkerhet i en Totalforsvarskontekst [2]. Prosjektet presenterte fire alternative analyserte sikkerhetsstrategier med tilhørende tiltak. Etter at prosjektet ble avsluttet, igangsatte Samferdselsdepartementet prosjekt TIFKOM, med hensikt å forberede et nytt regulatorisk regime basert på innspillene fra BAS2-prosjektet [3]. Deretter ble det laget en Stortingsmelding – Stortingsmelding 47 (2000-2001), som ble behandlet av Stortinget i 2001 [4].

Ett viktig element i stortingsmeldingen var etableringen av en telesikkerhets- og beredskapsfunksjon i Post- og teletilsynet (PT). Til å begynne med ble TRSTI et organ med tett knytning til den nye funksjonen i PT. Etter en lengre tid preget av personellgjennomtrekk i PT på grunn av et politisk vedtak som innebar en flytting til Lillesand, har tilsynet funnet sin rolle. Underveis ble det funnet naturlig å avslutte TRSTI.

Denne raske historiegjennomgangen kan sikkert fortone seg både forenklet og noe subjektiv, men ett poeng er uomtvistelig. *Man har gått fra en situasjon der telekommunikasjonstjenester har vært levert av en statlig operatør som et samfunnsgode, til at disse tjenestene i dag leveres som kommersiell tjeneste i et åpent marked.* Samtidig har rammebetingelsene for myndighetsregulering av sikkerhetsarbeidet gjennomgått dramatiske endringer. Dette skal vi se nærmere på i kapittel 4.

[4] Først Statens teleforvaltning.

4 Utfordringer innen sikkerhet og beredskap i en nasjonal kontekst

De senere år har det vært gjennomført en rekke forsknings- og utredningsarbeider rundt temaet IKT- og EKOM-sikkerhet. Noen har dreid seg om samfunnssikkerhet i bredt perspektiv, mens andre har behandlet konkrete infrastrukturer, som for eksempel kraftforsyning, telekommunikasjon og vannforsyning. Fra offentlig forvaltning, forskningsinstitusjoner og konsulentselskaper har det med tiden blitt utformet relativt store mengder med publikasjoner om emnet og forslag til tiltak, blant annet i forbindelse med:

- Prosjektene i serien ”Beskyttelse av samfunnet” (FFI):
  - BAS2-prosjektet ”Sårbarhet i offentlig telekommunikasjon” [2]
  - BAS3 og 4 innen kraft- og transportsektoren, som også inneholdt IKT-perspektiver [5;6]
  - BAS5 om ”Sårbarhet i kritiske IKT-systemer” [1]
- Sårbarhetsutvalget (Willoch-utvalget) [7]
- ”Samfunnets sårbarhet som følge av avhengighet til IKT” (prosjekt i Nærings- og handelsdepartementet) [8]
- Vurderinger av behovet for autonomi innen EKOM-området (Post- og teletilsynet og FFI) [9]
- Infrastrukturutvalget (Justis- og politidepartementet) [10]
- Nasjonal strategi for informasjonssikkerhet (flere departementer) [11]
- Ulike stortingsmeldinger (flere departementer)

Man må imidlertid på et tidspunkt stille seg spørsmålet om hvilken nytte arbeidene i nyere tid har hatt for sikkerhet og robusthet i nasjonale IKT-baserte infrastrukturer. Arbeidet har åpenbart bidratt til å sette problemstillingen på den politiske agendaen. Fra en teknologs ståsted kan det imidlertid lett hevdes at sikkerhetsgevinsten ikke har vært like stor som volumet av arbeid skulle tilsi. Neste spørsmål blir da – hvorfor det? Det gis ikke noe klart svar på dette, men vi vil hevde at dette henger tett sammen med forhold knyttet til teknologisk, markedsmessig og sikkerhetspolitisk utvikling.

4.1 Endrede rammebetingelsene for sikkerhetsarbeidet

Allerede på 80-tallet gjennomførte FFI analyser innen sikkerhet i offentlig leverte telekommunikasjonstjenester. Utgangspunktet for disse arbeidene var:

- Et stabilt og omforent trusselbilde, hvor den dimensjonerende utfordringen var et militært angrep fra Sovjetunionen.
- Et enkelt ”marked”, i den form av at tjenesteleveransene skjedde fra kun én offentlig forvaltningsbedrift – Televerket.
- Enkel og oversiktelig tjenesterealisering i infrastrukturen. Selv om teknologiene som ble anvendt kunne være avanserte nok, var disse satt inn i innbyrdes strukturer som var relativt enkle og oversiktelige.

- Få tverrsektorielle avhengigheter - telesystemet hadde for eksempel i stor grad egen reservekraft som kunne tåle selv lange avbrudd i strømforsyningen, mens kraftbransjen på sin side hadde egne radiosystemer for å ivareta sambandsbehovet i sine operasjoner.

I denne situasjonen kunne FFI bruke analysemodeller som beskriver lineære struktursammenhenger for å få oversikt over svake elementer eller funksjoner i selv større systemer, og på den måten identifisere behov for forbedringer og tiltak[5].

I løpet av 90-tallet oppstod imidlertid flere samtidige utfordringer for IKT-sikkerhetsarbeidet, i form av raske endringer og økt kompleksitet:

Teknologiutviklingen førte til at det vi tidligere omtalte som telekommunikasjon har blitt utvidet til å innbefatte et større mangfold av tjenester for elektronisk kommunikasjon – EKOM. Internett utgjør en sentral infrastruktur i denne utviklingen. I tillegg kan det hevdes at samfunnets avhengighet av offentlige tjenester som elektrisk kraft og EKOM ble dramatisk mye større enn tidligere, ikke minst pga. en sterk gjensidig innbyrdes avhengighet av systemer og tjenester mellom ulike sektorer. Kompleksitet som følge av tett kobling mellom sektorer og systemer ble dermed en stadig viktigere faktor i sikkerhets- og beredskapsarbeidet. En annen faktor som forsterket dette ytterligere var at endringer i systemene og tjenestenes oppbygging skjedde stadig raskere. Oppdaterte oversikter over systemene ble stadig vanskeligere å utarbeide. Dette er forhold som omtales nærmere senere i dette kapittelet.

Tjenester innenfor EKOM-området ble utsatt for økt *konkurranseutsetting*. Tidligere offentlige forvaltninger som Televerket ble i løpet av få år forvandlet til private leverandører, og nye aktører dukket opp i tillegg. Kompleksiteten økte ytterligere som følge av dette, ikke minst når det gjelder hvilke roller ulike aktører kunne ha innenfor beredskapsarbeidet og hvem som skulle betale for økt sikkerhet. Det faktum at mange IKT-baserte tjenester og infrastrukturer ikke lenger er under direkte statlig forvaltning, er viktig for hvordan man skal sikre samfunnsinteresser mot større utfordringer.

Den *sikkerhetspolitiske utviklingen* gav også nye utfordringer. Det tidligere dimensjonerende scenariet for sikkerhetsarbeidet ble gradvis redusert i betydning utover 90-tallet. I dag er det mange aktuelle utfordringer for sikkerhets- og beredskapsarbeidet, uten at det er noen omforent oppfatning av hvilken som er viktigst. Dette gjør det vanskelig å sette klare mål for sikkerhetsarbeidet.

Disse utviklingstrekkene var sentrale for at flere av analysearbeidene som er omtalt over ble startet opp. På den andre siden er de også viktige forklaringer på hvorfor arbeidet med sikkerhet og robusthet er vanskelig og kanskje ikke har ført til de resultater man kunne ha forventet. Kompleksiteten i problemstillingene øker, og utviklingen går i noen tilfeller så raskt at analyser

[5] Disse analysene var svært eksplisitte i å påpeke svakheter i systemene, og dermed også høyt graderte.

og utredninger knapt har rukket å bli ferdig før deler av resultatene har vært foreldet. Resten av dette kapittelet vil diskutere noen av disse utviklingstrekkene i detalj.

4.2 Teknologiutvikling

Siden dette er en teknologisentrisk beskrivelse, er det naturlig med en kortfattet beskrivelse av noen sentrale trekk i den teknologiske utviklingen innen nettverksteknologi, sett i et sikkerhets- og sårbarhetsperspektiv.

4.2.1 Organisatoriske og teknologiske strukturer innen EKOM og distribuerte IKT-systemer

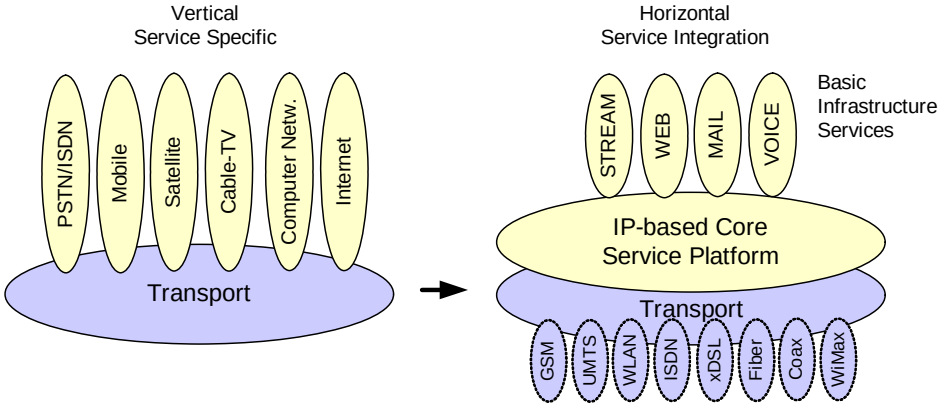
Det var tidligere svært nære relasjoner mellom der infrastrukturer faktisk var lagt ut i form av fysiske forbindelser, som kabler og radiolinjer, og der informasjonen virkelig fløt. I dag er nettverksstrukturene langt mer sammensatte. Selv om informasjonen fremdeles til slutt flyter i de fysiske forbindelsene, har behovet for blant annet fleksibilitet ført til at formidlingen av informasjon i et nettverk er inndelt i ”logiske” lag over den fysiske kanalen, med ulik funksjon i nettstrukturen.

I et moderne kommunikasjonsnett kan det være svært vanskelig å følge hvor brukertrafikken faktisk går gjennom disse lagene. Funksjonene på hvert lag realiseres som tjenester, der tjenestene som benyttes på de ulike lagene også kan leveres av flere tjenesteleverandører. Mens man før med høy sannsynlig kunne fastslå hvor en informasjonsstrøm gikk mellom f eks Oslo og Moss, for eksempel i form av en telefonsamtale, er dette i dag nær umulig å fastslå uten grundige undersøkelser. Mens den før i hovedsak ville gå den rette veien mellom Oslo og Moss, kan den i dag like gjerne fysisk gå via Stockholm eller Gøteborg. Hvor den virkelig går geografisk vil også være svært dynamisk. Det som er virkelighet i dag kan være noe helt annet i morgen. Det gjøres hyppige endringer i systemstrukturene, som blant annet har sammenheng med en sammensetting av tekniske, økonomiske og markedsmessige faktorer.

Distribuerte IKT-systemer utvikles dermed til å inneha en svært kompleks og dynamisk struktur. Forståelsen av disse strukturene er svært viktig for utviklingen av effektive sikkerhets- og beredskapsregimer.

4.2.2 Konvergens

Mens man tradisjonelt produserte tjenester på vertikalt atskilte plattformer, der hver tjeneste levde sitt liv tilsynelatende stort sett uavhengige av hverandre, går utviklingen nå raskt i retning av at tjenester legges inn på én horisontalt integrert tjenesteplattform. Dette gir kunden mer og bedre tjenestefunksjonalitet, samtidig som at tjenesteleverandørens tjenesteproduksjon blir mer effektiv. Dette er søkt illustrert i Figur 4.1, der tidligere vertikale tjenesteplattformer som Internett, kabel-tv og telefoni, overføres til samme horisontalt integrerte tjenesteplattform. Tjenestenoder på kanten av den integrerte plattformen står for tjenesteproduksjon overfor brukerne. Det som leveres til kunden er basert på grunnleggende tjenesteklasser. Som det også fremgår av figuren er begge modellene avhengige av det samme underliggende transportnettet.



Figur 4.1 Overgang til horisontalt integrert tjenesteplattform innen EKOM

Det kan hevdes at en slik integrert tjenesteplattform vil gi negativ virkning med hensyn til sikkerhet og robusthet, ved at ”alle eggene havner i samme en kurv” – ett stort system. Tidligere kunne man sikre robusthet ved å iverksette separate tiltak i enkelte av tjenestene. Dette kunne i det minste gi en illusjon av at tjenesten som ble levert var robust. Videre hadde man også en form for plattformredundans, ved at hvis f.eks. mobiltelefonitjenesten ikke virket, så ville jo likevel fasttelefonitjenesten fungere. Imidlertid var uansett det underliggende fysiske transportnettet felles for alle tjenester og dermed også en viktig felles faktor med hensyn til sårbarhet.

En fordel med en utvikling mot konvergens er likevel at operatøren må legge seg ekstra i selen for å få denne felles plattformen mer robust enn det som var tilfelle for hver av enkelttjenestene. Han kan da også bruke sine samlede ressurser på denne strukturelt enklere plattformen, som det på mange måter vil være enklere å legge inn god redundans i. Dette vurderes samlet sett å være en styrke for alle de medier og tjenestenett som benytter infrastrukturen. Det må legges til at arkitekturen til dette ”nye” integrerte nettdesignet også har svært sterke kvaliteter innebygd, som også anses sterke nok til å bli benyttet i militære nett. Nettogevinsten vurderes derfor å være klart positiv fremfor negativ.

Hever man imidlertid blikket fra tjenesteleverandøren og ser det hele utenfra i et samfunnssyn, kan det hevdes at konvergens som beskrevet over vil gi enda større kompleksitet og dynamikk totalt sett. Mens man tidligere kunne velge å se kun på de tjenestestrukturer man oppfattet som viktige, for eksempel fasttelefonitjeneste, er man nå i prinsippet stilt overfor et komplett tjenestetilbud. For en utenforstående, som kunde eller regulatorisk myndighet, vil det nå fortone seg som enda vanskeligere (om ikke umulig) å tilegne seg en detaljert oversikt over for eksempel sammenhengen mellom nett- og tjenestestruktur, som er viktig for å forstå en tjenestes robusthet.

Vi vil derfor hevde at selv om hver enkelt operatør isolert sett vil kunne oppnå en mer homogen og oversiktlig infrastruktur, vil det bli vanskeligere for aktører utenfra løpende å forstå konsekvensen av utviklingen med hensyn til sikkerhet og sårbarhet. Med så vidt omfattende problemstillinger, blir også kundenes og myndighetenes tilgang på kompetanse og ikke minst relasjon til operatørene av tjenestene svært kritisk.

4.3 IKT som forutsetning for basisgoder i samfunnet

Dette kapittelet beskriver utviklingen mot IKT-baserte infrastrukturer i samfunnet, hvor ulike IKT-systemer blir svært viktige for levering av ulike samfunnskritiske tjenester. Beskrivelsen er i hovedsak basert på to eksempler fra en artikkel av BAS-miljøet i tidsskriftet Telektronikk [12].

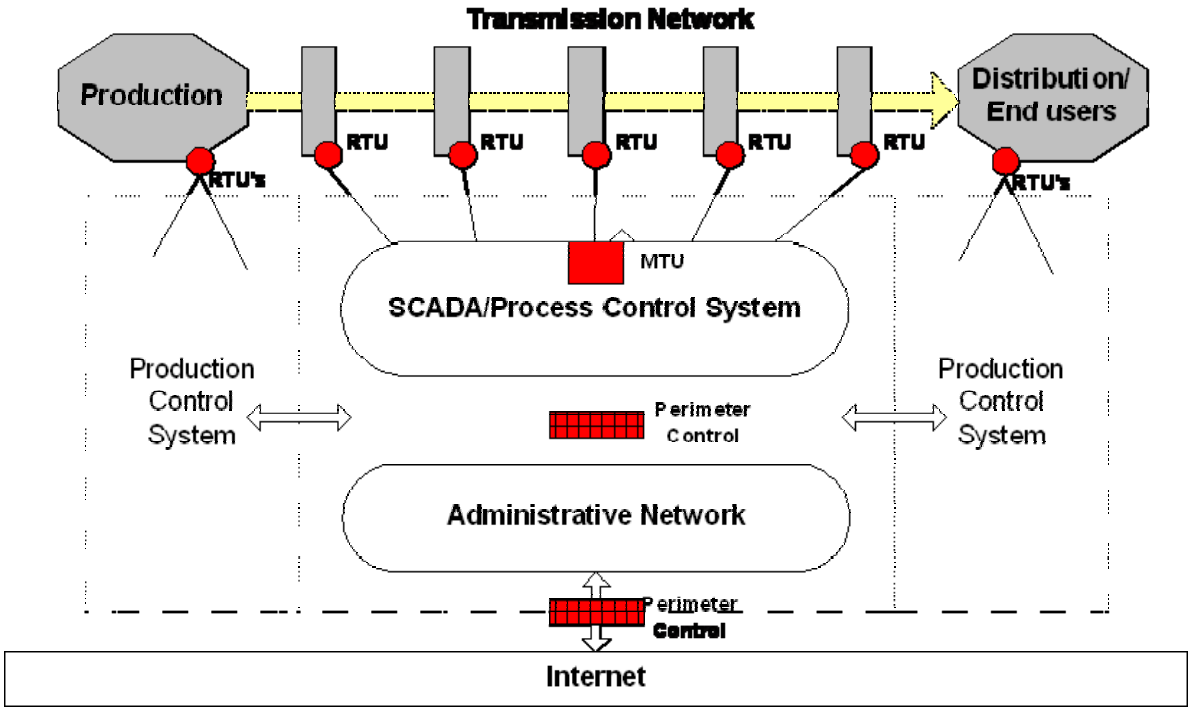
4.3.1 Kraftforsyningen som IKT-infrastruktur

Kraftforsyningen i Norge er et godt eksempel på en IKT-basert infrastruktur som har gjennomgått en rivende utvikling de siste tiårene. I denne sektoren har IKT-systemer gradvis gått veien fra å være støttesystemer for den daglige driften, til å være grunnforutsetninger for at det i det hele tatt kan leveres strøm til norske forbrukere.

Tidligere ble kraftinfrastruktur bygget for å forsyne lokalsamfunn nær vannkildene med strøm. Disse lokale forsyningene var isolert fra hverandre, uten behov for gjensidig kontakt. Gradvis ble disse lokale forsyningene koblet sammen, og nettverk for levering av strøm ble bygget inn til områder uten egen lokal kraftproduksjon. I dag har vi et landsdekkende sammenkoblet strømnett, som også har koblinger til utlandet.

Til å begynne med ble denne infrastrukturen driftet og overvåket manuelt. De fleste installasjonene i kraftnettet var bemannet, og personene kommuniserte med sentrale driftsressurser via talesamband og telefaks for å levere data, slå effektbrytere på og av og planlegge vedlikehold. Dette talesambandet var basert på et svært robust telefonisystem.

Gradvis så man imidlertid muligheten for at IKT-baserte driftsløsninger kunne understøtte en mer effektiv gjennomføring av disse arbeidsoppgavene, enten automatisk eller via fjernstyring. Dels fjernet dette behovet for en stor mengde ansatte i kraftforsyningen, dels la dette til rette for mer effektiv utnytting av infrastrukturen slik at denne kunne belastes mer. I løpet av få år ble strømnettet i hovedsak ”tømt for folk”, og i stedet fylt opp av datamaskiner for styring og kontroll av nettet. Drift og overvåking skjedde via et IKT-system tett integrert med kraftinfrastrukturen, hvor en håndfull mennesker fra sentrale driftssentraler i praksis kunne styre hele infrastrukturen. Figur 4.2 gir en skissemessig fremstilling av dette.



Figur 4.2 Kraftforsyningen som IKT-infrastruktur

Informasjonsflyten i dette systemet gikk tidligere i hovedsak via en egen sambandsinfrastruktur, men det kan hevdes at anvendelsen av ulike offentlige IKT- og EKOM-tjenester nå er på full fart inn også i kraftforsyningen. Samtidig vokser de gjensidige avhengigheter mellom kraftforsyningen og EKOM-området. Kraftforsyningen blir med denne utviklingen mer og mer avhengig av fungerende EKOM-tjenester, mens EKOM-operatørene i mindre grad enn før legger inn reservekraft i sine nett og tjenester.

Som det også fremgår av Figur 4.2 knyttes også nå de fleste infrastrukturer til Internett. Både anvendelsen av Internett og den plattform for trusler som Internett betyr, øker kompleksiteten for sikkerhets- og beredskapsarbeidet ytterligere.

En utfordring som følge av dette er at sikkerhetsarbeidet innenfor kraftforsyningen i økende grad blir et spørsmål om hvilken sikkerhet og robusthet man klarer å bygge inn i IKT-systemene. Selv om det fremdeles er mulig å vurdere sårbarheter for produksjonsanlegg og kraftlinjer separat, med tradisjonelle analysemodeller, vil sammenkoblingen av en allerede kompleks fysisk infrastruktur med IKT gjøre det vanskelig å se logiske årsakssammenhenger mellom feil som oppstår og hvilke konsekvenser de kan medføre.

4.3.2 RFID-samfunnet

Eksempelet i foregående kapittel viste hvordan utviklingen av en IKT-basert infrastruktur gir betydelige utfordringer for arbeidet med sikkerhet og robusthet. Innenfor kraftforsyningen er det likevel mulig å peke på en konkret ansvarlig myndighetsaktør som kan følge opp dette arbeidet. Imidlertid finnes det områder i samfunnet hvor dette vil være mye vanskeligere, om ikke umulig.

”Radio Frequency Identification” (RFID) er en teknologi som har fått økende anvendelse. Dette er i praksis små brikker, de minste mindre enn 1 kvadratmillimeter, som kan plasseres på nær sagt ethvert fysisk objekt. Disse brikkene kan kommunisere med utplasserte lesere som ved et elektromagnetisk signal ber om informasjon fra brikkene. Mulig informasjon kan blant annet være faste egenskaper ved objektet brikken er plassert på, som identifikasjonskoder, produksjonssted, og fysiske egenskaper til objektet. Brikkene kan også utstyres med små mikroprosessorer.

Anvendelsesområder så langt har vært som en form for erstatning for strekkoder i dagligvarehandelen, registrering av passering for automatisk avkreving av bompenger, og for styring og kartlegging av hvor ressurser befinner seg i logistikksystemer (blant annet militære). Det forventes imidlertid at denne teknologien vil bli tatt i bruk i langt større grad enn det vi har sett i dag. Telenor R&I arbeider nå med løsninger hvor mobiltelefoner utstyres med RFID-brikker [13]. Kombinert med SIM-kortet i telefonen og et kredittkort gir dette brukeren en komplett løsning for mobil kommunikasjon, identifikasjon og elektronisk betaling. Telefonen kan da benyttes til alle dagligdagse gjøremål, for eksempel for betaling av matvarer og transportbilletter, lagring av informasjon knyttet til åpningstider og reiseruter, identifisering for tilgang til arbeidsplassen osv.

Dette vil naturlig nok være en svært effektiv løsning for brukerne, i alle fall så lenge de ikke fysisk mister telefonen. Imidlertid må et slikt omfattende sensornettverk understøttes av en rekke sammenkoblede databaser, hvor informasjon samlet inn fra utallige lesere lagres og prosesseres, understøttet av effektive EKOM-tjenester. En rekke ulike aktører, fra infrastrukturleverandører til innholdsleverandører og sluttbrukere av alle nyanser, vil være avhengige av den enkelte tjenesten som leveres. Tjenester og informasjon fra så godt som alle samfunnsfunksjoner vil logisk samles på ett sted.

Denne teknologien må i løpet av få år forventes å gi grunnlag for et bredt spekter av tjenester, alt fra enkeltindividers dagligdagse handlelister for å fylle kjøleskapet til store effektive internasjonale logistikksystemer. Feil som oppstår i dette systemet kan, når avhengigheten har blitt stor nok, gi dramatiske konsekvenser for samfunnet. Men hvem vil være ansvarlig for å ivareta sikkerheten i dette nettverket? *Dette systemet vil ikke ha noen enkelt sektormyndighet som ansvarlig for sikkerhet og beredskap, slik som i kraftforsyningseksemplet over. Samfunnets avhengighet av infrastrukturen vil likevel kunne bli dramatisk.*

4.4 Hva er egentlig trusselen?

I en diskusjon rundt sikkerhet og beredskap er det viktig å avklare hva som faktisk er utfordringen. En slik klarhet finnes ikke i dag, men det finnes svært mange meninger om dette. Noen vil på den ene siden krisemaksimere og hevde at de venter på den store IKT-smellen, i form av et digitalt 9-11 eller digitalt Pearl Harbour. På den annen side vil andre ikke uttrykke noen særlig bekymring. Ingen ting av større betydning har skjedd. Det meldes riktig nok stadig om hendelser der for eksempel EKOM-tjenester ikke fungerer noen timer, eller om banker som har problemer med sikkerheten i sine interne datasystemer og nettbanker. Man har endog for noen år

siden hatt en konkurs hos en større EKOM-operatør (EniTel), med potensielt negative konsekvenser for større kunder som for eksempel Oslo Børs. Likevel har det så langt vist seg at dette har vært håndterbart.

Uklarheten om hva trusselen faktisk er melder seg på flere nivåer. Sikkerhetspolitisk vil man i dag ofte se uttalelser som ”det er sannsynlig at noe usannsynlig vil skje”, ”trusselbildet er bredt og sammensatt, preget av usikkerhet og uforutsigbarhet” og lignende. Det er ikke umiddelbart lett å sette klare ambisjonsnivåer for det nasjonale arbeidet med IKT-sikkerhet med et slikt utgangspunkt. På teknologisk nivå er det alltid mulig å peke på mange enkeltsårbarheter og mulige angrepsveier inn i IKT-systemer, og supplere dette med generelle beskrivelser av aktører som kan ha ulike motiver for og kapabiliteter til angrep mot systemene. Imidlertid viser det seg vanskelig å koble slike teoretiske vurderinger til realistiske og omforente beskrivelser av hva trusselen faktisk vil være i tiden fremover.

Alle verdens samlede IKT-systemer og nettverk utgjør et så vidt samlet og komplekst system at selv enkle feil kan få uante konsekvenser, avhengig av hvilken avhengighet ulike brukergrupper har opparbeidet av ulike tjenester. Den samme kompleksiteten gjør imidlertid også at IKT-systemer vil være vanskelig å angripe, fordi virkningen av angrep vil være usikkert. Det kan vise seg vanskelig å avgrense konsekvensen av angrepet, og man kan stå i fare for sette ut av funksjon tjenester man selv trenger til eget kommunikasjonsbehov. Angriperen kan selv være avhengig av tjenestene for økonomiske transaksjoner, kommunikasjon med samarbeidspartnere eller til propagandaformål.

I et sikkerhetspolitisk landskap der vi har vansker med å se verken en konkret eller overhengende trussel, vil det være vanskelig å oppnå en omforent oppfatning av hva våre systemer og infrastrukturer skal beskyttes mot. Spørsmålet om sikkerhet og robusthet dreier seg dermed om noe mer enn kun en teknologisk fundert beskyttelse av et teknologisk system. En stor utfordring i forhold til trusler og trusselbildet som helhet blir å sette teknologi og anvendelse inn i en større sammenheng.

4.5 Om myndighetenes rolle innen IKT- og EKOM-sikkerhet

I et marked kan følgende hevdes: I stedet for at en statlig aktør sikrer at tjenestene inneholder tilstrekkelig sikkerhet og beredskap, er det *kunden* som må etterspørre det han trenger. I utgangspunktet er det to naturlige roller i markedet; *leverandøren av tjenester og den kompetente kunden som stiller krav til tjenesteleveransene*. Disse må så bli enige om egenskapene i leveransen dem i mellom, også med hensyn til sikkerhets- og beredskapsfunksjoner

Likevel kan det hevdes at avtaler mellom kunder og tjenesteleverandører av ulik størrelse ikke nødvendigvis bidrar til at det utvikles tjenester som også er robuste overfor større utfordringer mot samfunnet. Skal samfunnet ha et slikt tjenestetilbud, må sannsynligvis myndighetene på en eller annen måte på banen. Myndighetene kan i utgangspunktet ha rolle som innkjøper på vegne av fellesskapet eller kravstiller gjennom lover og forskrifter. I dagens regime søker man å

tilnærme seg dette på begge måter. Med bakgrunn i teknologisk og strukturell utvikling, krever begge roller imidlertid svært høy kompetanse. Dette kompetansebehovet vil øke ytterligere med utviklingen i årene som kommer.

I dette ligger et svært viktig poeng i at myndighetene ikke lenger har tilgang til kompetansen om den tekniske infrastrukturen eller om operasjonen av denne som de hadde før. De kan heller ikke uten videre forvente å tilegne seg denne i en situasjon hvor teknologiutviklingen skjer svært raskt. Dette har svært mye å si for hvilke tiltak det er realistisk å iversette av myndighetene, og hvilke reguleringsmodeller som kan fungere. Mot slutten av rapporten vil vi derfor drøfte ulike tilnærminger til et myndighetsengasjement ut fra denne problemforståelsen.

4.6 Nivåer av reguleringsregimer innen IKT- og EKOM-sikkerhet

Man kan i utgangspunktet tenke seg at sikkerhets- og beredskapsfunksjoner, i tillegg til på virksomhetsnivå, etableres på enten nasjonalt eller globalt nivå. Siden IKT- og EKOM-systemer som nevnt kan være vanskelig å definere helt klart, kan det for enkelthets skyld være hensiktsmessig å bruke Internett og EKOM som modell for en drøfting av sikkerhet og beredskap i de to sistnevnte nivåene. Informasjon er i stor grad hentet fra [14].

Internett utgjør i sin vide definisjon den globalt sammenvevde kombinasjonen av EKOM-tjenester og IKT-systemer for sluttbrukere. Internett består av et svært sammensatt nettverk av nettverk, der sluttbrukerne bruker dette nettverket til stadig flere anvendelser. Tradisjonelt har dette dreid seg om tjenester som web og epost, men man finner stadig nye måter for integrerte distribuerte anvendelser i for eksempel forretningsprosesser. IKT-systemer med sentrale funksjoner innen prosessindustri, samferdsel og kraftforsyning er i dag integrert med Internett, og bruker Internett som del av sin IKT-arkitektur. Globale og nasjonale EKOM-tjenester er i tillegg fundamentale for kommunikasjonsfunksjonene i Internett.

Internett kan sannsynligvis i liten grad la seg regulere på et globalt nivå. Grunnen til dette er at Internett eies og kontrolleres av mange aktører i et svært mangfoldig fellesskap. Det er i dag mer enn 20 000 registrerte autonome systemer (AS)[6]. Mange av disse aktørene driver ikke sin virksomhet etter kommersielle prinsipper. Internett kjennetegnes da også i dag nettopp med en svært liten grad av overordnet global styring. Det er vanskelig å se for seg noe annet enn at global styring hovedsaklig må være konsensuspreget, og dermed dreie seg om svært "enkle" og langsiktige forhold.

Man kan hevde det samme for andre former tjenester fra IKT-systemer, som for eksempel tradisjonell EKOM eller prosesstyringssystemer. Selv med økende grad av globalisering, både når det gjelder eierskap og operasjon av infrastrukturer, vil det samtidig være forskjeller i for eksempel kultur og sikkerhetspolitisk ståsted avhengig av hvor virksomheten er geografisk forankret.

[6] Et AS er et nettverk med en klart definert rutingpolicy som registreres hos IANA. Kravet om en rutingpolicy er helt nødvendig for å få registrert et AS, som beskrevet i retningslinjer for opprettelse, valg og registrering av et AS i RFC 1930. Her beskrives et AS som "the unit of routing policy in the modern world of exterior routing".

På nasjonalt nivå er det ulike muligheter for regulering. Det kan for eksempel dreie seg om krav til grunnleggende redundans i ulike deler av nettinfrastrukturen til "viktige" tjenesteleverandører. Andre muligheter er ulike former for fysisk beskyttelse av viktige infrastrukturelementer i for eksempel et IKT-nettverk. I et nasjonalt regime er det også mulig å tenke seg mer generelle tiltak som utdanning og beredskapsøvelser på tvers av organisasjoner og samfunnssektorer.

Det er imidlertid viktig å se hvilke begrensninger og muligheter som foreligger i et mulig nasjonalt regime. Hvilke tiltak vil kunne ha effekt i forhold til de ressurser som legges ned i dem? Tiltak knyttet til sikkerhet og beredskap må passe inn i en større helhet, og enkelttiltak vil ofte ha begrenset effekt dersom de ikke hører med i en helhetlig strategi. I en nasjonal kontekst kan det være en fare for at tiltak med stor symbolsk virkning utad og lav kostnad får stor oppmerksomhet, fremfor en helhetlig tilnærming og vekt på de tiltakene som er effektive sammen. Ikke minst vil det være en stor utfordring å gjennomføre tiltak rettet mot virksomheter som kan være del av store internasjonale operasjoner og eierstrukturer.

Det vil være forbundet med store utfordringer å etablere et regime for sikkerhet og beredskap innen dette brede og mangfoldige IKT-området, på tvers av virksomheter og samfunnssektorer. Særlig blir dette åpenbart ved anvendelse på RFID-eksemplet ovenfor. Dersom det er et politisk ønske om sikkerhetsregimer som går ut over hver enkelt virksomhets kommersielt baserte egeninteresse, vil det være en rekke valg man må foreta uansett ambisjonsnivå. Dette vil bli nærmere drøftet i kapittel 5.2.

5 Et nasjonalt regime innen sikkerhet og beredskap

I dette kapitlet forsøker vi å skissere innretningen for et mulig nasjonalt regime innen sikkerhet og beredskap knyttet til samfunnsviktige IKT-systemer og tjenester. I første del av dette kapitlet gis en kort drøfting av erfaringer fra EKOM-sektoren med utgangspunkt i prosessen etter BAS2-prosjektet, med hensikt å peke på noen forhold som er relevante for utviklingen av denne skissen.

5.1 Sikkerhet og beredskap innen EKOM-sektoren

5.1.1 Kort om prosessen etter BAS2

Forslagene fra BAS2 om sikkerhet og beredskap innen EKOM ble fremlagt i 1999, det vil si for ca åtte år siden. Disse ble fremlagt i form av fire alternative strategier som hver inneholdt et sett med tiltak [2]. Tiltakene og strategiene var som del av analysen i BAS2 kosteffektivitetsberegnet. Siden da har av mange årsaker svært få av de konkrete forslagene om tiltak blitt gjennomført. Riksrevisjonens gjennomgang av arbeidet med IKT-sikkerhet peker på at dette delvis er et resultat av en forvaltningsskikk [15]. Det kan imidlertid diskuteres om hvorvidt denne typen tiltak er gjennomførbare med det forvaltningsregimet vi i dag har, der ting må ta tid i forhold til tradisjonelle krav til forsvarlig behandling.

Som beskrevet i kapittel 4 har forhold knyttet til teknologiske forutsetninger, markedsutvikling og sikkerhetspolitisk situasjon endret seg betydelig i løpet av disse åtte årene. Forutsetningene for et nasjonalt sikkerhetsregime innen EKOM har dermed endret seg ganske dramatisk parallelt med denne utviklingen. Mange av tiltakene som ble foreslått av BAS2-prosjektet er det antagelig heller ikke lenger hensiktsmessig å innføre. Globaliseringen på både operatør- og nettnivå gjør at flere av tiltakene trolig ikke vil være mulig å gjennomføre i dag. Det nasjonale handlingsrommet til å innføre en rekke typer tiltak med formål å redusere sårbarhet anses i løpet av disse årene å være er stekt redusert. Utviklingen innen Internett har gitt betydelige bidrag til denne utviklingen.

Det neste spørsmålet vil da være hva som bør være Statens og samfunnets rolle innenfor IKT- og EKOM-sikkerhet. Dette kommer vi tilbake til, men har likevel noen umiddelbare synspunkter.

Med rammebetingelsene som i dag foreligger er det lite realistisk å søke å gjøre kommersielle EKOM-tjenester så robuste at de med en høy grad av sikkerhet skal kunne benyttes av viktige samfunnsfunksjoner også under større påkjenninger. Ut fra den generelle avhengigheten det moderne samfunnet har av slike tjenester vurderes det likevel som hensiktsmessig å gjøre disse så sikre som mulig, men forankret i en realistisk tilnærming til de foreliggende rammebetingelsene. Gitt dette må sikkerhet i slike tjenester i all vesentlighet baseres på relasjonen mellom kunde og tjenesteleverandør. Ikke fordi dette nødvendigvis er ideelt for samfunnet, men fordi det i praksis ikke er gode alternativer til denne tilnærmingen. En konsekvens av dette er at det bør utvises stor forsiktighet med å etablere tekniske og organisatoriske sårbarhetsreduserende tiltak basert på en myndighetsregulering med målsetting nasjonal sikkerhet. Likevel vurderes det å være enkelte typer tiltak som relativt kosteffektivt kan være med på å bedre robustheten når IKT- og EKOM-tjenester utsettes for negativ påvirkning.

Et sentralt spørsmål for å avklare nødvendige tiltak er imidlertid hvilket sikkerhetsnivå man bør kunne oppnå og hvilken hensikt dette skal ha for samfunnet. For å bestemme hvilke tiltak man må gjennomføre for å oppnå dette sikkerhetsnivået, kreves en *metodisk og ikke minst sporbar prosess*. I analysene i BAS2 ble det i stor grad søkt gjennomført en slik tilnærming. I ettertid ble det imidlertid som følge av flere forhold ikke sett som hensiktsmessig å gjennomføre tiltakene. Ambisjonene som ble lagt til grunn for arbeidet var langt større enn det som i praksis viste seg mulig å få til. [7]

For å etablere et nytt regime er det likevel helt sentralt å gjøre dette ved hjelp av en prosess med tilsvarende egenskaper som BAS2. Da FFI kom med sine anbefalinger, var dette basert på analysearbeidet til flere forskere i mer enn ett år, og i tilegg med utgangspunkt i tidligere forskning innenfor samfunnets sårbarhet. Vi mener med den erfaringen at det krever betydelig kunnskap om EKOM og ikke minst metodekunnskap hos myndighetene for å etablere et nytt

[7] Dette kan jo kanskje hevdes å være et argument mot strukturerte prosesser. Disse er heller ikke bedre enn forutsetningene tilsier. Dette understreker imidlertid bare behovet for å ha omforente og klare forutsetninger for å gjennomføre et hensiktsmessig sikkerhetsarbeid.

regime for informasjonssikkerhet basert på nåtidens forutsetninger. Til en hver tid oppdatert kunnskap om teknologi og marked vil være en avgjørende forutsetning for å lykkes, selv for et enkelt reguleringsregime. Derfor er det svært viktig at det opprettes gode relasjoner mellom myndigheter og operatører. Det er naturlig at et myndighetsorgan har dette ansvaret. Det er imidlertid viktig å merke seg de naturlige begrensninger som vil måtte ligge i en slik kontakt gitt virksomhetenes klare kommersielle føringer. En EKOM-operatør er en kommersiell virksomhet som har naturlige kommersielle føringer. Informasjon som for eksempel berører f.eks. forretningsmodeller vil denne svært nødig gi fra seg.

5.1.2 Typer av tiltak basert på erfaringer fra prosessen etter BAS2

Med erfaring fra prosessen etter BAS2 vurderes det som sannsynlig at man i fremtidige regimer må gå inn for et ambisjonsnivå som ligger langt under det som er foreslått i Stortingsmelding 47. Det synes videre hensiktsmessig å prioritere to hovedtyper av tiltak. Det første dreier seg om *rammebetingelser og tilrettelegging* knyttet til anvendelsen av IKT- og EKOM-tjenester, mens det andre dreier seg om *samfunnsmessig beredskap* i forhold til svikt i tjenestene i tid og omfang.

Anbefalingene fra BAS2 var i stor grad rettet mot *sårbarhetsreduserende tiltak*. Ressursbruken ble i stor grad rettet mot relativt kostnadstunge tiltak for beskyttelse av vitale deler av infrastrukturen. Prosessen etter BAS2 tyder imidlertid på at det realistisk sett bør vises avholdenhet knyttet til myndighetsstyrt etablering av denne typen tiltak. Det systemet man skal beskytte er for det første så komplekst at en i analysen av slike tiltak ofte ikke vil ha tilstrekkelig sikker kunnskap om den virkning de vil ha. Et annet forhold er at slike tiltak ofte vil påvirke operatørens måte å operere på, noe som gjør at denne sannsynligvis vil være motvillig til å innføre tiltaket. Sist og ikke minst vil slike tiltak ofte være svært ressurskrevende.

Et myndighetsengasjement på området *rammebetingelser og tilrettelegging* kan være å bidra til at relevant informasjon om sikkerhet flyter mellom operatørene og deres kunder, og at det etableres hensiktsmessige kundeavtaler dem i mellom. Herunder kommer også å utvikle bredt anlagt informasjon om sikkerhet til ulike typer kundegrupper, f eks i form av “best practices”. Hensikten med dette er at en kunde i størst mulig grad skal vite om hvilken grad av sikkerhet en tjeneste innehar. Dette for å kunne forstå den risikoøkning egen virksomhet utsettes for som følge av anvendelsen av tjenesten. Det er svært viktig at det offentlige som kunde blir foregangsvirksomheter på dette området. Inntrykk samlet inn gjennom BAS-prosjektene over tid har vist at offentlige kunder ofte har vært svake i denne sammenheng. Mange av disse har en holdning om at dette er sektoransvaret til “et annet offentlig organ”. EKOM-tjenester og ulike IKT-baserte infrastrukturer skal som følge av dette sektoransvaret i utgangspunktet være robuste, og “er dermed ikke vår sak”. Da bestiller man de tjenestene som er rimeligst, uten hensyn til sikkerhet.

Et myndighetsengasjement på området *beredskap* vil dreie seg om å bistå aktørene i markedet med å redusere konsekvensen av svikt i tjenesteproduksjon. Dette kan dreie seg om tilsyn med at beredskapsplaner utvikles og følges ut fra en minimumsstandard. Dette kan også

bestå av å arrangere faglig samarbeid mellom konkurrerende aktører på området, og arrangere ulike typer samøvelser for å øve på beredskapsutfordringer.

Som allerede indikert viser erfaringene etter BAS2 at det er på de to sistnevnte områdene at et myndighetsengasjement vil være både realistisk og effektivt, sett fra et samfunnsperspektiv. Det vil være også realistisk ut fra den betalingsvilje offentlig sektor synes å ha på dette området, og ut fra den teknologiske kompetansegap som eksisterer mellom den enkelte operatør og aktuelle myndighetsorgan.

5.2 Innspill til innretning for nasjonalt regime

Til tross for at sikkerhet og beredskap innen IKT-systemer og EKOM er et svært komplekst tema, er det etter vår vurdering fremdeles viktig at myndighetene har et ansvar for utviklingen. Dette ansvaret bør imidlertid reflekteres i en utforming og et nivå som gjør det hensiktsmessig i forhold til formålet, og som samtidig er gjennomførbart både med hensyn til økonomiske ressurser og de kompetanserelasjoner man kan forvente å ha mellom myndighetsorgan og systemoperatører/-eiere.

Som forsøkt skissert tidligere i rapporten ligger det svært komplekse systemer og systemstrukturer til grunn for problemstillingen, der også rammebetingelsene må kunne karakteriseres som komplekse. Fordi det er mange mulige tilnærmingsmåter til å nå et mål om tilstrekkelig nivå av sikkerhet og beredskap i en samfunnskontekst, er det svært viktig å ha en metodisk tilnærming til det å velge tiltak.

Når myndighetene skal utvikle regimer innen sikkerhet og beredskap innen IKT-systemer og EKOM, er det av fundamental betydning at det som utvikles baseres på en *kontinuerlig og løpende prosess* i sikkerhetsarbeidet. *Arbeidet må ikke baseres på "skippertaksbaserte" tiltakslister, men på en prosess som fortløpende bidrar til vurderinger av sikkerhet og robusthet.* Denne prosessen må være metodisk og sporbar, og det er viktig at man i denne løpende tar sterkt hensyn til den teknologisk faglige utviklingen.

Det foreslås derfor at man utvikler en prosess som på tvers av sektorer og ansvarsområder kan gi nødvendig helhet og konsistens ved utvikling av strategier og tiltaksforslag. Den overordnede prosessen har følgende hovedpunkt:

1. Det avklares hvilke utfordringer og trusselbilde sikkerhetsarbeidet skal rettes mot – hva er egentlig utfordringene for arbeidet med nasjonal IKT-sikkerhet?
2. Det bestemmes klare ambisjonsnivåer og målsettinger – hvor vil vi konkret med sikkerhetsarbeidet?
3. Det identifiseres hvilke virkemidler som basert på relevans og realisme kan bidra til å oppfylle målsettingen, og det måles hvilken effekt og kostnad disse har.

Utfordringer og trusselbilde

Det er svært viktig at man på tvers av sektorer og ansvarsområder identifiser og definerer klart hva som er trusselen mot de systemene og tjenestene man ønsker å beskytte. Det er samtidig

viktig å identifisere hvilke samfunnsaktører som er relevant del av problemstillingen, i forhold til leverandører, sluttbrukere og myndighetsorgan. Det samme gjelder tjenester – hvilke tjenester er relevante i forhold til aktørene. Man må sørge for at dette får forankring i mest mulig objektive vurderinger av virkeligheten, samtidig som at vurderingene også i stor grad må ta inn over seg den videre utviklingen. Eventuelle enkeltindividers synsing og svakt forankrede oppfatninger vil påvirke prosessen svært negativt.

Ambisjonsnivå og målsetting

Med bakgrunn i en mest mulig konkret oppfatning av utfordringene man står overfor, må det defineres et ambisjonsnivå for sikkerhetsarbeidet som man på nasjonalt nivå mener er hensiktsmessig innen de ulike sektorene. Dette ambisjonsnivået gjenspeiles videre i en konkret målsetting. Denne skal gjenspeile en klar mening om hva man ønsker å oppnå. Denne vil derfor ofte være en mangedimensjonal størrelse som må bygges opp med delmålsettinger i ett eller flere nivåer.[8] Opp mot denne målsettingen, som skal kunne måles, knyttes effekten av ulike enkelttiltak og kategorier av enkelttiltak. Med hensiktsmessig menes at ambisjonsnivået er konsistent, for eksempel at det er politisk vilje til å få det gjennomført.

Virkemidler

Til slutt kommer identifisering av tiltak som i en eller annen form kan gjennomføres for å oppnå den målsettingen som foreligger. Tiltakene kan av type være teknologiske, organisatoriske eller juridiske (lover og forskrifter). Tidligere i dette kapitlet er det kort beskrevet tre tiltakskategorier som blant annet er relevant i strukturering av et målhierarki som knytter sammen egenskaper ved tiltak til en målsetting:

- Sørge for at rammebetingelser og tilrettelegging for sikkerhet og beredskap innen produksjon og anvendelse av IKT og EKOM-tjenester
- Beredskapstiltak knyttet til en tjenesteproduksjon og tjenesteanvendelse
- Sårbarhetsreduserende tiltak i tjenesteproduksjonssystemer

En slik prosess må være en del av en kontinuerlig pågående prosess eiet og drevet frem av den offentlige forvaltningen. Dette vil være ressurskrevende. Det vil være behov for metodeverktøy og fagkompetanse for å gjennomføre en slik prosess. Gjennom BAS-prosjektene fra BAS2 til BAS5 har slike metoder gjennomgående vært i fokus. Her nevnes kort noen av områdene der det finnes vesentlige metodemessige bidrag fra BAS-prosjektene:

- BAS 2-3: Scenarioanalyse og beslutningsstøtte knyttet til valg av strategier og tiltak. Benyttet på konkrete infrastrukturtiltak målt opp mot scenarier og andre utfordringer.
- BAS 5: IKT-sikkerhet – tiltak dreier seg om å redusere risiko for tjenestetilbyder og sluttbruker. Utvikling av metoder for å adressere/håndtere risiko i IKT-avhengige infrastrukturer
- BAS 5: Metoder for rangering av tiltak (dr.grad Janne Hagen)

[8] Å sette sammen og bestemme en målsetting vil ofte være en stor del av oppgaven. Å gi et konkret eksempel på målsetting i formatet til denne rapporten vil kunne gi et galt inntrykk av hva som menes. Det vises derfor til [16] der oppbyggingen av et målhierarki i forbindelse med tiltaksanalysen i BAS2-prosjektet er beskrevet (telekommunikasjon).

6 Avsluttende kommentar

Det er vår klare anbefaling at man i det videre arbeidet med sikkerhets- og beredskapsregimer innen offentlig forvaltning sørger for å utvikle en prosess som skissert i denne rapporten, og som går på tvers av sektorer og ansvarsområder. På denne måten vil man kunne oppnå en helhetlig og ikke minst realistisk og kosteffektiv tilnærming til å møte et vanskelig problemkompleks. Selv om det vil være ressurskrevende for forvaltningen, anbefales det på det sterkeste at realiseringen av en slik arbeidsprosess velges fremfor at man med jevne mellomrom børster støv av tidligere tiltakslister og legger disse til grunn for sikkerhetsarbeidet. Én fare med sistnevnte tilnærming er at disse raskt kan bli basert på ”gamle” sannheter.

Det er videre svært viktig at man i denne prosessen sørger for at de tiltakene som fremkommer gjennom tilnærmingen faktisk kan gjennomføres, og ikke blir værende som symboler i offentlige handlingsplaner og meldinger. Å gi samfunnsviktige brukere en falsk forventning om nivået av sikkerhet i EKOM-tjenester og IKT-avhengige samfunnsinfrastrukturer er svært lite heldig. Da kan det være bedre å ikke ha noen tilnærming i det hele tatt, og la markedet styre den videre utviklingen alene.

Referanseliste

[1] H. Fridheim and J. Hagen, "Beskyttelse av samfunnet 5 - Sluttrapport," FFI/RAPPORT 2007/01204, 2007.

[2] J. Hagen and K. O. Nystuen, "Beskyttelse av samfunnet med vekt på offentlig telekommunikasjon," FFI/RAPPORT 99/00240, 1999.

[3] Prosjektgruppe TIFKOM, "Teleberedskap i fritt konkurransemarked," Samferdselsdepartementet,2000.

[4] Samferdselsdepartementet, "Stortingsmelding 47 (2000-2001): Telesikkerhet og -beredskap i et marked med fri konkurranse,"2001.

[5] H. Fridheim, J. Hagen, and S. Henriksen, "En sårbar kraftforsyning - sluttrapport etter BAS3," FFI/RAPPORT 2001/02381, 2001.

[6] J. Hagen, G. H. Rodal, E. Hoff, B. Lia, J. E. Torp, and S. Gulichsen, "Beskyttelse av samfunnet med fokus på transportsektoren," FFI/RAPPORT 2003/00929, 2003.

[7] Justis- og politidepartementet, "Et sårbart samfunn,"NOU 2000:24, 2000.

[8] Nærings- og handelsdepartementet, "Samfunnets sårbarhet som følge av avhengighet til IT,"2000.

[9] H. Fridheim, J. Hagen, K. O. Nystuen, and I. Johansen, "Nasjonal autonomi for elektroniske kommunikasjonsnett og -tjenester," FFI/RAPPORT 2005/00175, 2005.

[10] Justis- og politidepartementet, "Når sikkerhet er viktigst,"NOU 2006:6, 2006.

[11] eNorge, "Nasjonal strategi for informasjonssikkerhet - Utfordringer, prioriteringer og tiltak.," Forsvarsdepartementet, Nærings- og handelsdepartementet, Justis- og politidepartementet, 2003.

[12] J. Hagen, H. Fridheim, and K. O. Nystuen, "New challenges for emergency preparedness in the information society," *Telektronikk*, vol. 1/2005, pp. 48-54, 2005.

[13] J. C. Calvet, "NFC Mobile Payment and Ticketing (Powerpoint slides)," Telenor R & I, 2007.

[14] A. Thuv, R. Windwik, K. O. Nystuen, and T. Sivertsen, "Sårbarheter i Internett," FFI/RAPPORT 2007/00903, 2007.

[15] Riksrevisjonen, "Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur,"Dokument nr 3:4 (2005-2006), 2005.

[16] J. Hagen, K. O. Nystuen, H. Fridheim, and E. Østby, "Analyse av sårbarhetsreduserende tiltak innen telekommunikasjon," FFI/RAPPORT 99/00241 (Konfidensielt), 1999.