UNIVERSITETET I OSLO
Institutt for informatikk

Filtrering og overvåkning av Internett - en casestudie i bruk av filtreringsmetoder og effektene de gir

Masteroppgave
(60 studiepoeng)

Gro Irene Sandvik

01.08. 2008

Abstrakt

Denne studien undersøker hva slags betydning filtrering har på en global infrastruktur som Internett, og hvordan filtreringsmetodene brukes i praksis for individer, private aktører og myndigheter i utvalgte land. Ved å se nærmere på dette blir det klarere hvordan filtrering fungerer, hvem som bruker det og til hvilke formål.

Sett i lys av at Internett er en infrastruktur som stadig utvikler seg, skjer det et stadig økende tilskudd av filtreringsapplikasjoner i nettverkskjernen. Studien prøver å finne ut om en slik utvikling skader generativiteten og fleksibiliteten, og dermed integriteten til Internett. Dette kan føre til at vi i framtiden står overfor et låst og usikkert nettverk hvor utviklingen har gått fra en distribuert til desentralisert topologi.

Ved å analysere innsamlet materiale fra Internett – inkludert tekst, nettsider, dokumenter, blogger, artikler og bøker – blir filtreringens rolle identifisert både på en praktisk og teoretisk måte. Det brukes blant annet teori og begreper hentet fra informasjonsinfrastrukturer, ende-til-ende designteori og teknologisk determinisme. Generativitet og fleksibilitet er sterkt koblet til ende-til-ende arkitekturen, og filtreringsapplikasjoner har en direkte påvirkning på denne arkitekturen.

Denne studien viser at dagens Internett har gått over til en ny struktur hvor ende-til-ende arkitekturen fortsatt eksisterer, men ikke etter de samme prinsippene som ble formulert flere tiår tilbake. Filtreringsapplikasjoner bidrar med en nyttig tjeneste ved å øke brukerkontrollen over Internett, og bør derfor ikke nedprioriteres i nettverket. Studien konkluderer med at i den videre utviklingen av filtreringsapplikasjoner er det viktig å innføre *mer åpenhet og gjennomskinnelighet til hvordan filtreringskriteriene blir satt*. Dette vil bidra til å styrke påliteligheten til applikasjoner i nettverket. Med dette er målet at den mer komplekse nettverksstrukturen vi ser allerede i dag skal bidra til en fleksibel, tilpasningsdyktig og pålitelig nettverksstruktur også i framtiden, slik de første Internett-arkitektene mente det skulle være.

Forord

Denne oppgaven avslutter min mastergrad i informatikk ved Universitetet i Oslo. Jeg vil takke Professor Ole Hanseth som er leder for forskningsgruppen Globale Infrastrukturer ved Institutt for Informatikk, Universitetet i Oslo. Han har gitt meg nyttig veiledning og mange gode tips i løpet av oppgaveskrivingen.

En spesiell hilsen til Kristian Spilhaug for å ha tatt seg bryet med å lese oppgaven og som har gitt meg verdifulle tilbakemeldinger, og til Mari Anne Killie som har stilt opp som undrende korrekturleser.

Takk til familie og venner, hvor jeg ønsker å nevne noen navn spesielt: Cecilie, Anne, Jorunn, Anita kakebaker og Mari Anne. Alle har hver på sin måte gitt meg støtte, motivasjon og velkomne pauser fra en, til tider, intens studiehverdag. En hilsen går også til Ingunn og Stine, som er gode venner jeg får sett altfor sjeldent, og til min hybelnabo Vibeke, som så dette forordet mens jeg skrev det, for hennes alltid gode humør.

Oppgaven har blitt skrevet på en datasal under ti meter fra der det nye informatikkbygget vil stå ferdig innen år 2010. Selv om det til tider har vært mye distraherende støy, er ”IFI 2” en velkommen utvidelse og nyttig videreutvikling for studiene ved Institutt for Informatikk, som denne studenten har hatt stor glede av.

Gro I. Sandvik

Oslo, juli 2008

Innholdsfortegnelse

Figurer

"What can be studied is always a relationship or an infinite regress of relationships. Never a 'thing'."
Bateson

1 Introduksjon

Internett[1] har blitt et levende og voksende miljø som bare blir tatt mer og mer i bruk. At en slik tjeneste er nyttig har allerede blitt bevist av hvor mange som bruker den. Dessverre så er det også negative aspekter ved denne globale infrastrukturen, for eksempel gjør den det lettere for kriminelle miljøer å finne likesinnede. Det finnes de som benytter seg av Internett for å utføre alt fra utpressing til pengesvindler i stor skala, ved å bruke filtreringsapplikasjoner for å kunne manipulere nettsteder.

Filtrering har gjort sitt innpass i alle de store applikasjonene for Internett, som elektronisk post (e-post) og World Wide Web (www). Det brukes blant annet søppel-filtre, søkemotorer og brannmurer for å filtrere informasjon eller eventuelle farlige angrep mot datamaskiner. Bruksområdene for Internett blir stadig flere, og med økningen kommer mange forventede, men også uforutsette problemstillinger. Prinsippene som er knyttet opp mot *ende-til-ende* arkitekturen ble definert da Internett ble designet. I dag har de blitt til en slik uforutsett problemstilling. Grunnen til dette er at prinsippene sier det ikke skal være noen implementeringer av applikasjoner i nettverkskjernen, slik det i dag likevel har blitt med filtreringsapplikasjonene. Tekniske filtreringsmetoder som DNS-manipulering, IP-blokkering og proxy-basert filtrering er derfor blant implementasjonene som kan bryte med ende-til-ende arkitekturen.

Casestudiene i denne oppgaven vil presentere tre vinklinger mot filtreringsfenomenet for å få en bredere innsikt i temaet. Den mest omfattende kritikken mot implementasjoner som bryter med ende-til-ende arkitekturen går på at fleksibiliteten til Internett blir skadet. Denne oppgaven vil bidra med rikere innsikt i om dette er tilfelle for filtreringsapplikasjoner i nettverkskjernen.

Videre har ende-til-ende arkitekturen en filosofi om at Internetts design støtter opp om frihet og demokrati. Dette begrunnes ved at den ivaretar nettverkets integritet fordi det er "umulig" for tredjeparter å sensurere mellom endepunktene uten å bli oppdaget (Sandvig 2006). Hvorvidt dette er en realitet i dag vil bli undersøkt i den delen av casearbeidet som går nærmere inn på kontrollen forskjellige myndigheter utøver over Internett.

[1] Ordet "Internett" blir skrevet med stor forbokstav i denne oppgaven siden det henviser til egennavnet for den globale infrastrukturen av mange sammensatte nett som følger samme standard.

Etter 11.september 2001 førte kampen mot terror til at det ble brukt mer ressurser enn før for å etablere en sterkere etterretningsvirksomhet. Hjelpemidler her er blant annet bruk av avanserte filtreringsapplikasjoner for å kunne samle opp og lagre informasjon for alle personer, som våre daglige gjøremål i form av handlevaner, reiser og andre aktiviteter. Det finnes databaser for alle former for informasjon om hva vi foretar oss elektronisk, som deretter kjøpes og selges blant kommersielle aktører for å øke kundemassene deres. De forskjellige fragmentene av informasjon kan slås sammen til en større helhet. I etterretningsvirksomhet brukes det for eksempel automatiserte analyse- og statistikk-programmer for innsamlet informasjon til å skille ut "faremomentene". Sett at det er en person som har lånt bøker som inneholder informajon om Al-Qaeda, og har stadige flyturer til Midt-Østen. Slike opplysninger kan til sammen avdekke forbindelser som ikke er synlige hver for seg. Samtidig åpner det for noen uklare grenser når det gjelder personvernet, i og med at alle vil være mistenkte til det motsatte er bevist. Casestudiene vil se nærmere på to kjente etterretningsprosjekter, Carnivore og ECHELON, for å få et innblikk i hvor langt filtreringsteknikkene har kommet.

Ofte er innhold på nettsteder i gråsonen av hva som kan sensureres uten å skade ytringsfriheten. Hvor grensene går for å vurdere nettsider som skadelige eller ulovlige vil variere fra land til land. Dette vil komme klarere fram i den delen av casestudiene som ser på hvordan filtrering kan brukes for å skape kontroll på Internett. Flere land blokkerer eller filtrerer politisk, kulturelt, seksuelt eller religiøst innhold for deres innbyggere. Det er funnet bevis for at minst førti land rundt i verden driver med denne formen for filtrering, blant annet i Asia, Midt-Østen og Nord-Afrika (ONI 2008).

Kina har lenge brukt de mest sofistikerte filtreringsteknikkene i verden på nasjonalt nivå. På denne måten har kinesiske myndigheter i stor grad klart å skaffe seg kontroll over hva innbyggerne deres har tilgang til på Internett. Egypt er et annet land som også ønsker å ha kontroll på hva brukerne foretar seg på Internett, uten at de vil hindre bruken av det. De fører ikke en like streng Internett-politikk som Kina, men i likhet med Kinas naboland, for eksempel Vietnam eller Singapore, viser også Egypt tendenser til å gå inn for en mer økt kontroll over sine brukere. En slik utvikling setter spørsmålstegn ved om folk i verden i dag har et "fritt Internett" til disposisjon, slik ende-til-ende arkitektene så det for seg i 1960-årene (Saltzer, Reed et al. 1984).

1.1 Retningen for forskningen og forskningsspørsmålet

Forskningsfokuset for oppgaven vil bygge på tre caser:

1. Eksempler fra allmenn bruk og misbruk av filtreringsapplikasjoner, det vil si kommersiell programvare som kan sjekke og filtrere "farlige" nettsider, analysere nettverkstrafikk, og lignende. Det tas med firmaers bruk rettet mot individer, og selskapers overvåkning over sine ansatte.
2. Gjennomgang av to spesielle etterretningsprosjekter, Carnivore og ECHELON, som bruker filtre i stor skala i et større miljø (som hele land og over flere land).
3. Studier av Kina og Egypts bruk av filtrering på Internett. De bruker forskjellige grader av kontroll, hvor Kina går for å være verdens beste på filtreringsteknikker. Denne casen tar opp hva slags kontroll som kan utøves på Internett på det mest "ekstreme" (Kina) og på en mer "vanlig" måte (Egypt).

Denne oppgaven støtter seg på tidligere forskning med ende-til-ende designteori, teknologisk determinisme, og teori hentet fra utvikling av informasjonsinfrastrukturer. Teorikapittelet vil utlede noen hypoteser fra disse teoriene som vil bli analysert i kapittel 7 etter at casestudiene har bidratt med mer innsikt. En innledende formulering av hypotesene er:

1. *Internetts ende-til-ende arkitektur trues av filtreringsapplikasjoner i nettverkskjernen, fordi de vil skade generativiteten (og dermed fleksibiliteten) til infrastrukturen*. Denne hypotesen blir undersøkt hovedsakelig i case 1 og case 2. Casene går nærmere inn på ende-til-ende prinsippene for slike applikasjoner ved å se på den allmenne bruken og hvor stor nytteverdi det er i dem.
2. *Internett støtter opp under frihet og demokrati ved at ende-til-ende arkitekturen ivaretar en sikker og pålitelig forbindelse uten at det skjer avskjæringer eller reguleringer av tredjeparter.* Dette blir undersøkt hovedsakelig av case 2 og case 3. Case 2 tar for seg avanserte avskjæringsteknikker, mens case 3 undersøker nærmere hvor fritt Internett er, samt ser på strenge former for kontroll på Internett.
3. *Drivkraften bak en økende implementering av applikasjoner i nettverkskjernen er ikke brukerstyrt, men teknologisk styrt.* Dette vil bli undersøkt på basis av hele casestudien for å se om teorien bak den teknologiske determinismen blir riktig for denne oppgaven.

Funnene fra casestudien vil bli sammenlignet med hypotesene i analyse- og diskusjonskapittelet for å gi rikere innsikt til å kunne besvare **forskningsspørsmålet** for oppgaven:

Har filtrering en konkret påvirkning på hvordan den globale infrastrukturen til Internett utvikles videre, og hvordan brukes filtreringsmetodene i praksis for individer, private aktører og myndigheter i forskjellige land?

Dette gir underspørsmålene:

- Hva er filtrering?
- Hvordan fungerer filtrering?
- Hvilke teknikker blir tatt i bruk?
- Hva er vanligst?
- Hvem bruker det?
- Hvilke problemer er knyttet til bruk av filtrering?
- Hvorfor brukes filtrering?

Fordi det ene gir det andre fører filtrering også gjerne til "undertemaet" *overvåkning* eller en form for *kontroll*. Dette temaet vil derfor også være en del av oppgaven.

Målene med denne studien er altså å undersøke hvordan filtrering påvirker nettverksstrukturen til Internett, samt å få dypere innsikt i gevinsten eller tapet i denne utviklingen av filtreringsapplikasjoner i nettverkskjernen. Studien vil se nærmere på bruken av filtreringsmetoder på forskjellige nivåer, fra enkeltindivider til myndigheter i utvalgte land, som representerer hver sine spesialiseringer innenfor feltet. Til slutt vil oppgaven ta for seg de sosiale effektene filtreringsmetoder som påføres Internett gir for brukerne.

1.2 Oppbygningen av oppgaven

Kapittel 2 Bakgrunn: gir en todelt introduksjon til Internett, filtrering og sensur. Første del tar for seg utviklingen av Internett i korte trekk og hva slags rolle Internett har idag. Andre del presenterer temaer knyttet til forskjellene mellom, og problemstillinger ved; filtrering og sensur.

Kapittel 3 Teoretisk bakgrunn: gir et teoretisk rammeverk som denne oppgaven bygger på, knyttet til sentrale temaer ved informasjonsinfrastrukturer, ende-til-ende arkitekturen og

teknologisk determinisme som; generativitet, fleksibilitet, om det går mot en ny design av Intetnett og hva som driver denne utviklingen.

Kapittel 4 Forskningsmetoder: forklarerer strategien bak forskningen, hvilke metoder som ble brukt og hvordan datainnsamlingen for oppgaven har foregått.

Kapittel 5 Filtreringsmetoder: viser de forskjellige variantene av filtreringsmetoder som finnes og gjennomgår hvordan de fungerer både som teknisk og sosial filtrering.

Kapittel 6 Casestudier

Case 1: Allmenn filtrering til skade og nytte for Internett: tar for seg eksempler på bruk og misbruk av vanlige tekniske filtreringsmetoder. Det vises privatpersoners og selskapers bruk av kommersiell programvare for å utføre filtrering og overvåkning.

Case 2: Etterretningstjenesters overvåkning og filtrering: tar for seg hvordan regjeringer i vestlige land har valgt å gjennomføre kontroll av Internett ved overvåkning for å hindre blant annet organisert kriminalitet og terrorisme. Det tas opp bestemte prosjekter som utfører slik overvåkning, og hvordan prosjektene kan bli brukt til andre formål enn hva de var tiltenkt opprinnelig.

Case 3: Land som fører streng Internett-politikk: blir illustrert gjennom eksempler hentet fra Kina og Egypt. Disse to landenes bruk av filtrering og sensur på Internett vises, samt forskjellene i praktisering av filtreringsmetoder mellom disse to landene.

Kapittel 7 Analyse og diskusjon: av oppgavens tema relatert til den teoretiske bakgrunnen nevnt i kapittel 3 i tillegg til forskningsspørsmålet.

Kapittel 8 Konklusjon: oppsummering av hovedproblemene og funnene som er blitt gjort i oppgaven.

"The Net interprets censorship as damage and routes around it."
John Gilmore

2 Bakgrunn

Dette kapittelet er en todelt introduksjon til Internett, filtrering og sensur. Første del tar for seg utviklingen av Internett i korte trekk, med ende-til-ende arkitekturen og standardene nettverket er basert på, Internett som massemedia og Internett som en informasjonsinfrastruktur. Andre del presenterer temaer knyttet opp mot problemstillinger relatert til, og forskjellene mellom, filtrering og sensur. Denne bakgrunnen er med for å klargjøre senere temaer i oppgaven.

2.1 Internett

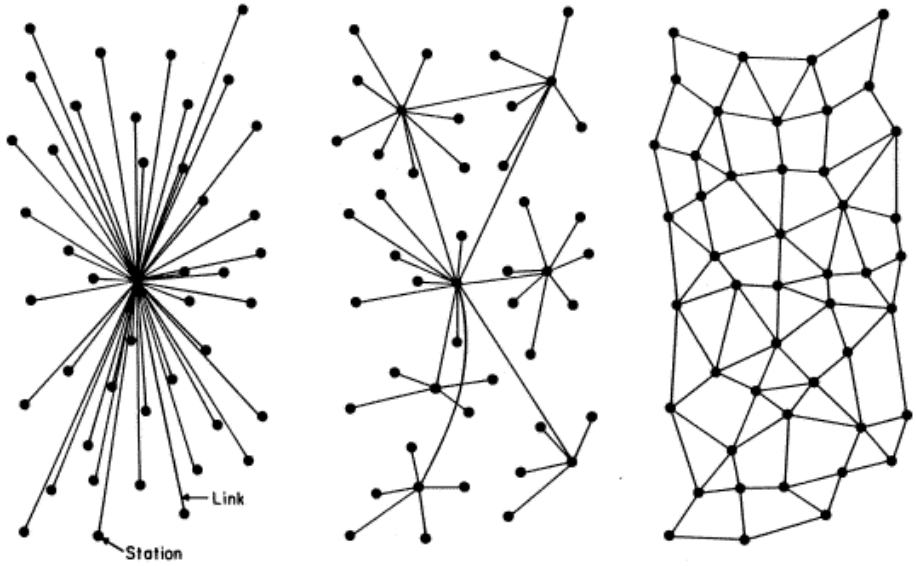
Internetts historie går fra å være et eksperiment rundt pakkesvitsjing-teknologi på universiteter, til dagens globale kommunikasjonsnett. Valget av en distribuert topologi la grunnlaget både for arkitekturen og for applikasjonene, noe som gjorde at brukerne fant infrastrukturen så nyttig at den har blitt et nytt massemedia.

2.1.1 Historien til Internett

Begynnelsen på Internett-historien kan ifølge Gisle Hannemyr spores så langt tilbake som til 1930-tallet (Hannemyr 2005). Det var da Vannevar Bush kom med de første tankene for alternativ informasjonshåndtering, hvilket resulterte i artikkelen As We May Think (Bush 1945). Her tar han opp hvordan tilgang til informasjon og effektiv organisering av informasjon vil være for samfunnets beste. Dette var før dataalderen, slik at Bush så for seg elektromagnetiske løsninger for å kunne lage en innretning han kalte Memory Expander (Memex). Den skulle fungere som et skrivebord med innebygde skuffer. Skuffene skulle bli styrt via et tastatur, som automatisk kunne hente fram ønsket informasjon slik at de kom til syne under en gjennomsiktig bordplate. Teknologien for å lage Memex var ikke tilstede på den tiden, men artikkelen viste seg å være en sterk motivasjon for Douglas Engelbart og J.C.R. Licklider. Dette var forskere som skulle vise seg å bli sentrale i Internetts historie. Engelbart ble leder for Augmentation Research Center, et laboratorium ved Stanford Research Institute (SRI) i Palo Alto, California. Licklider ble utnevnt av det amerikanske forsvarets forskningsråd, Advanced Research Projects Agency (ARPA), til å lede et prosjekt for å blant

annet utvikle og bedre forstå samarbeid mellom menneske og maskin. Dette ble startet opp i 1962, og Licklider hadde fra starten av en visjon om et ”galaktisk nett”, og at dette nettet skulle være like tilgjengelig hjemmefra som på kontoret.

Ideen om ARPAnet ble presentert offentlig første gang i 1967 på en liten konferanse i Gatlinburg, Tennessee. Her ble også pakkesvitsjing-teknologi presentert av engelskmannen Roger Scantlebury. Dette var et vendepunkt for nettverksprosjektet, for gjennom denne konferansen ble de som jobbet med dette overbevist om at pakkesvitsjing var den beste løsningen for ARPAnet. Likevel var det flere som (uavhengig av hverandre) var inne på tanken om samme teknologi, blant annet Paul Baran ved RAND Corporation. De som jobbet med ARPAnet-prosjektet ønsket at det skulle bli mulig å bruke delte ressurser i form av vertsmaskiner, uten at alle måtte ha hver sin som da bare var i bruk en liten prosentdel av tiden den sto på. Fordelene med et slikt nett var økonomisk gevinst og at samarbeid over avstander ville bli lettere. Baran sitt arbeid var verdt å ta med i den videre utviklingen av ARPAnet, spesielt hans utledning om fordelene ved et distribuert nettverk (Baran 1964).



Figur 1: Forskjellige nettverkstopologier. Fra venstre: sentralisert, desentralisert og distribuert

Figuren viser tre forskjellige nettverkstopologier, med hver sine kvaliteter. I et *sentralisert nettverk* vil all kommunikasjon rutes gjennom et sentralt punkt. Telekommunikasjon er eksempel på et slikt nettverk. En ulempe her er at hvis det skulle skje ”et brudd på linja” så er kommunikasjonen brutt. Den vil ikke kunne rutes gjennom en alternativ node for å holde kommunikasjonen i gang.

Ved bruk av et *desentralisert nettverk* vil det være noen flere knutepunkter å rute kommunikasjonen i mellom. Det vil oppstå flere kontrollpunkter, for eksempel ved at det implementeres funksjoner i selve nettverket. En slik design av desentralisert nettverk åpner

for andre problemstillinger. Dersom det skulle skje en svikt ved bare noen få noder, så kan i verste fall hele kommunikasjonen bryte sammen også her.

Ved å velge et *distribuert nettverk* vil en eventuell feil i en del av nettet ikke hindre pakkene i å komme frem. De vil bare finne en annen vei i nettet, siden det vil være flere veier mellom to noder. Dette medfører også at en pakke som sendes først kan komme fram sist, siden dette avhenger av hvilken vei den har tatt i nettet. Dermed vil mottaker få ansvaret med å sette sammen pakkene i riktig rekkefølge.

Det virket mest hensiktsmessig å gå for en distribuert topologi og pakkesvitsjing i den videre nettverksutviklingen, til tross for at det var et brudd med datidens almenne kunnskap om nettverksarkitekturer og bruken av telekommunikasjonsnett med sentralisert topologi. Valget førte til en ende-til-ende arkitektur i og med at alle funksjonene ville bli implementert på endepunktene, mens nettverkskjernen ville forbli enklest mulig.

Den første vellykkede forbindelsen mellom to vertsmaskiner, fra University of California, Los Angeles (UCLA) til SRI var oppe 29.oktober, 1969. Protokollen som ble brukt for å lage vert-til-vert forbindelsen het Network Control Protocol (NCP). Etter denne suksessen gikk utviklingen raskt. I desember 1969 var fire pakkesvitsjer (noder) utplassert hos SRI, UCLA, University of California, Santa Barbara (UCSB) og hos University of Utah i Salt Lake City (UTAH) for en første eksperimentell utprøving, og et år etter bestod nettet av 13 noder utplassert stort sett på øst- og vestkysten i USA (Hannemyr 2005). Med dette hadde nettverksprosjektet gått fra å være et prosjekt om eksperimentering med pakkesvitsjing som teknologi til å bli begynnelsen på et større kommunikasjonsnettverk.

Teknologien begynte å spre seg fort, og i 1973 var Norge det første landet utenfor USA som ble knyttet til ARPAnet. En måned etter fulgte England opp og ble knyttet til ARPAnet via Norge. I 1975 hadde nettet vokst til omtrent 50 noder, med ytterpunkter på Hawaii, Kjeller og i London, og disse var koblet til 150-200 vertsmaskiner (Spilling 1995).

Hittil hadde nettet blitt brukt både for militære og akademiske tjenester, men i 1984 ble ARPAnet splittet i to. Den ene delen ble kalt MILnet og ble en lukket tjeneste tiltenkt militære formål. Den andre delen fortsatte å hete ARPAnet og var åpen for sivilt bruk. Da ARPAnet i 1983 gikk fra NCP til de nye protokoll-teknologiene Transmission Control Protocol / Internet Protocol (TCP/IP), så ble hva vi kjenner som dagens Internett tatt i bruk (Hannemyr 2005). Unix la inn støtte for TCP/IP bruk for sine implementeringer og bidro dermed med en ytterligere økning av Internettbruken.

Antallet brukere har bare fortsatt å øke siden Internett ble tilgjengelig for privatpersoner, slik det skjedde i Norge ved etableringen av Oslonett i 1991. Målinger i Norge ved inngangen til 2008 viser at to av tre husholdninger har bredbåndstilgang (Statistisk_Sentralbyrå 2007). Når det gjelder Internett-tilgang for andre land er dette

varierende. I mange land er det de samme tallene som går igjen som vi har sett her til lands med en økende tilgang og bruk, men noen land skiller seg ut med sine strenge tilgangspraksiser. Jeg vil komme tilbake til disse senere i oppgaven, med spesielt fokus på bruk av Internett i Kina og Egypt, og hvordan filtrering kan brukes til å skape kontroll. Dette er mulig på grunn av at det har skjedd et brudd med den opprinnelige arkitekturen til Internett, som i utgangspunktet hadde et veldig enkelt design. Etter hvert som Internett har fortsatt å vokse har den blitt mer sammensatt og kompleks, fordi blant annet filtrering har blitt applikert på forskjellige lokasjoner i nettverket.

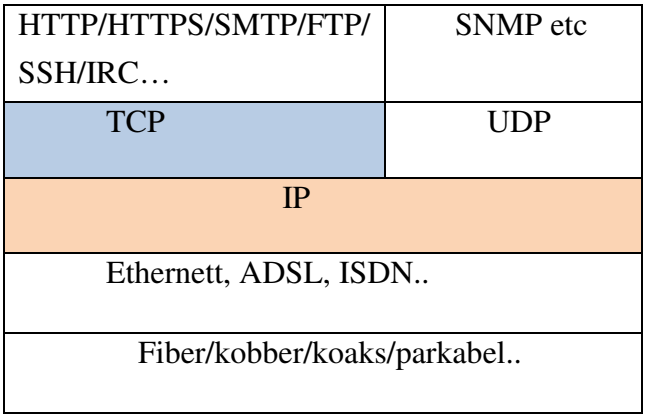
2.1.2 Ende-til-ende arkitekturen

Nettverkssystemet til Internett er lagt opp slik at det er et datagram-overføringssystem og ikke et pålitelig kretsnettverk. Dette gir som nevnt noen fordeler ved en distribuert topologi, i tillegg til at et datagramnettverk trenger mindre svitsjing. Det er ikke nødvendig å ta lokale sikkerhetskopier mellom nodene eller vente på bekreftelse om at neste node har fått dataene. Denne fremgangsmåten gir et raskere nettverk fordi det ikke blir utført pakkebehandling underveis. Det blir en enklere intern køstruktur og lettere håndtering av nettverksprotokollene (Huston 2008).

Et pålitelig kretsnettverk opererer veldig ueffektivt hvis et element innenfor nettverket når full kapasitet. Dette kan føre til en ”buffer overflow” som i et kretsnettverk skaper en stopp-og-reparer betingelse. En slik pause i trafikken kan gi bølgeeffekter gjennom hele nettverket på mye av den samme måten som trafikkork i vanlig veitrafikk. Til sammenligning vil et datagramnettverk med overskuddstrafikk ganske enkelt droppe all trafikk ved punktet for overmetting, slik at det ikke skaper effekter for resten av nettverket. Dette er basert på prinsippet bak ende-til-ende arkitekturen om å holde kjernen enkel. Det blir overlatt til endepunktene å finne feilen, reparere datatapet og be om ny sending av dataene om nødvendig (Huston 2008). En slik arkitektur skaper et mer fleksibelt nettverk, som er en av de store problemstillingene å klare å oppnå ved design av informasjonsinfrastrukturer.

Mange teknologiske utviklinger har vist tendenser til å gå mot modulariseringer. Nå kan ikke lenger en informasjonsteknologi sees på som en selvstendig enhet, men må sees som en del av et større integrert nettverk. Selv om Internetts nyuviklinger baserer seg på programvare har modularisering gått framover også her. Det klareste uttrykket for modularisering i datanettverk er utviklingen av standardmodellen for å representere kommunikasjonen mellom datamaskiner (Sandvig 2006). Dette standardiserte settet av protokoller gjør det enklere for utviklere å jobbe på hver sin del av applikasjonene. De trenger ikke å måtte tenke på hvordan en bit overføres fra en maskin til en annen fordi dette overlates til undernivåene.

Alt som finnes av tjenester i Internett er basert på slike protokoller. Vi har for eksempel nettlesere som Internet Explorer og Mozilla Firefox som begge er programmert på toppen av HTTP protokollen, og filoverføringstjenester som er programmert over FTP protokollen. HTTP og FTP protokollene er igjen programmert over TCP protokollen og slik fortsetter det. Internett deler opp sin kommunikasjon i fem lag som vist i modellen under[2]. Hvert protokollag hos sender snakker med samme lag hos mottaker.



Figur 2: Internetts protokollstakk

IP snakker mellom alle nodene i nettet som IP-pakken er innom, og er forbindelsesfri. Det vil si at hver datapakke finner en vei gjennom nettet uavhengig av de andre pakkene som tilhører samme meldingssekvens. Pakkesvitsjingen gjør at meldingen deles opp i datapakker slik at hver pakke kan bli behandlet som en selvstendig enhet under transporteringen til mottaker. IP er en ”best effort” tjenestekvalitet og dermed en *usikker tjeneste*, noe som fører til datagramoverføringens egenskaper. På samme måte er User Datagram Protocol (UDP) også en forbindelsesfri og usikker tjeneste. Denne protokollen brukes til enkle signaliseringstjenester som ”streaming media” av lyd eller bilde, hvor det er akseptabelt med tap av noen datapakker innimellom i sekvensen.

Til forskjell fra IP så snakker TCP mellom avsendermaskin og mottakermaskin og er en forbindelsesorientert og sikker protokoll. Det er på TCP-nivået at den upålitelige IP-datagram tjenesten blir behandlet ved at pakkene sorteres i riktig rekkefølge. Eventuelle pakker som mangler blir så sendt på nytt. Alle pakker som blir sendt vil være de samme pakkene som kommer frem. I konteksten med arkitekturen til Internett kan ende-til-ende applikasjonen sees som en del av TCP, en ende-til-ende protokoll som gir applikasjonen på nivået over en pålitelig levering av ende-til-ende datastrøm (Sandvig 2006).

[2] Den tradisjonelle OSI-modellen bruker 7 lag, men Internetts protokollstakk slår sammen noen av lagene

2.1.2.1 Internettapplikasjoner

Internett var i starten bare ment for enkel kommunikasjon, men har i ettertid bare fortsatt å vokse, mens stadig flere bruksområder har åpenbart seg. Baksiden er at vi i dag står overfor en mengde uforutsette problemer som har kommet i kjølvannet av Internetts spredning. For hver nye applikasjon som blir tatt i bruk har det dukket opp noen sideeffekter man ikke forutså da de ble utviklet. Mange tenker automatisk på www når Internett nevnes, siden det er den letteste og mest brukte tjenesten, men Internett har mange andre applikasjoner. I tillegg til www (HTTP protokollen) har vi også e-post (SMTP protokollen), nyhetsgrupper (NNTP protokollen), filoverføringstjenester (FTP protokollen) og lignende. De to applikasjonene www og e-post er så viktige for Internetts suksess at de nevnes spesifikt her. Filtrering utgjør en viktig rolle i påvirkningen av begge disse applikasjonene, og denne oppgaven bygger mesteparten av casestudiene på dette.

E-post er den elektroniske varianten av brevpost. Bakdelen ved denne tjenesten har vist seg ganske tydelig i form av utsending av store mengder *spam*, også kjent som søppelpost. Problemene øker ved at de som sender ut reklame kan benytte seg av forskjellige ”triks”, for eksempel zombiemaskiner[3]. Dette er maskiner som andre kan få kontroll over hvis eieren har vært uoppmerksom og lastet ned for eksempel en dataorm[4] eller trojaner[5]. Maskinen kan dermed brukes til masseutsending av spam. Andre utnyttelser av e-post kan være e-postvedlegg som inneholder virus. Virus blir skrevet for forskjellige oppgaver. En oppgave kan være å distribuere seg selv automatisk til alle adressene som står på e-post lista, før den pakker opp selve viruset på maskinen. Disse ondsinnede programmene kan slette filer, gjemme trojanere eller ormer, ødelegge, spre seg, gjøre maskinen til zombie og mye mer. Foruten de opplagte skadene kan formålet bak dette være et ønske om å innhente personlig informasjon som kan brukes til blant annet pengesvindel eller utpressing.

Filtrering er et sentralt begrep sammen med e-post. Nesten samtlige e-postsystemer kommer med et innebygd filtreringsprogram for å fange opp spam så det ikke kommer i innboksen. Spamanalytiker Chenxi Wang hos analysegruppen Forrester antok at den gjennomsnittelige innboksen mottok 4.351 spam-poster i 2007 (VG 2007). En annen bruk av filtrering er avskjæring av e-poster ved hjelp av programvare med avanserte filtreringsmekanismer. Casestudiene i kapittel 6 vil gi eksempler på dette.

---

[3] Zombiemaskiner er infiserte datamaskiner brukt til å utføre automatiske oppgaver uten at eierne av maskinene er klar over hva som skjer.

[4] Ormer kan i motsetning til virus ikke spre seg for ’egen maskin’, men trenger hjelp for eksempel i form av at de kommer i et e-postvedlegg som brukeren åpner. Dermed kan ormen hoppe videre fra maskin til maskin.

[5] Trojanske hester er programmer som gir seg ut for å være nyttige, ufarlige programmer, mens de har en skjult effekt som bare inntrengeren vet om, for eksempel å gjøre maskinen til en zombie.

Det er mye som kunne vært sagt i forbindelse med e-post. Likevel vil oppgaven hovedsakelig basere seg på bruken av filtrering på hovedapplikasjonen www, med dens enorme brukergruppe. Det startet i 1990 da CERN begynte med prosjektet www under ledelse av Berner-Lee. Han la ut resultatene sine som fri programvare på nettet, slik at andre kunne bidra. Programmerere ved University of Illinois var de første til å utvikle en nettleser i 1993, som ble kalt Mosaic. Takket være dette grafiske grensesnittet, som også for første gang gjorde det mulig å vise bilder på nettet, ble antallet brukere av www raskt økende. 1993 var også året hvor www tok over en større andel av trafikken enn noen annen Internettapplikasjon. Fra 1972 og fram til da hadde e-post hatt denne plassen (Hannemyr 2005).

2.1.3 Ulike tilnærminger til Internett

Før filtrering og sensur tas opp nærmere vil det være nyttig å se på de ulike tilnærmingene Internett presenterer. Internett kan beskrives på flere måter og tre av disse er verdt å nevne:

1. Internett er en **standard** for hvordan ulike datanett skal sammenkobles.
2. Internett er en **global infrastruktur** av sammenkoblede datanett som bruker den nevnte standarden i punkt 1.
3. Internett er et **massemedium** ved at punkt 1 og 2 er oppfylt slik at nettet er tilgjengelig for mange mennesker.

2.1.3.1 Internettstandarder

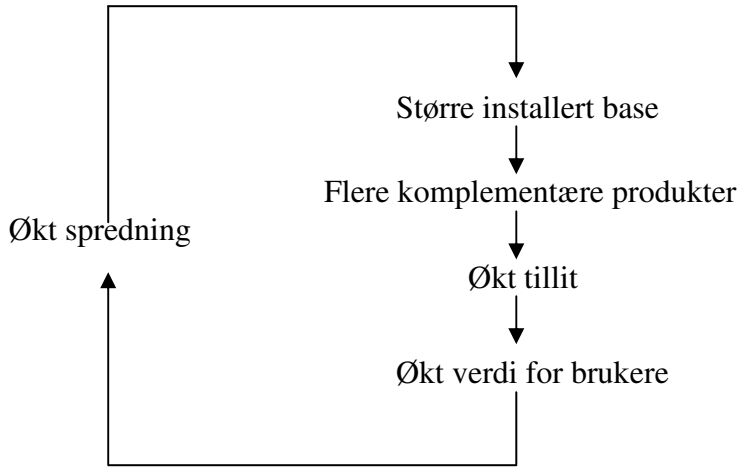
Standarder kan deles i tre kategorier, vi har *de facto*, *de jure* og *formell standard*. De facto er standardiseringer som oppstår fordi det har blitt et flertall av brukere av løsningen. En voksende brukerskare er noe som ofte skjer i en automatisk prosess over tid, helt til det blir naturlig å definere elementet som en de facto. De jure betyr basert på loven, altså lovgivende standarder. Den siste standarden, formelle standarder, gjelder for Internett og alle standarder som har blitt formet av institusjoner. Internett er bygd på komponenter som implementerer standardiserte kommunikasjonsprotokoller som for eksempel: TCP, IP, SMTP, HTTP, FTP eller SSH. Former for filtrering kan brukes i forbindelse med SMTP trafikk som for eksempel spamfiltre eller avskjæring av e-post, eller TCP/IP blokkering og DNS-manipulering på HTTP-forespørsler.

Hvor avgjørende det er å ha en riktig standard kan illustreres med revideringen av IP, som blir sett på som den mest alvorlige utfordringen Internetts vekst har ført til i dets nesten 40-årige eksistens (Monteiro 1998). Når det ikke er flere IP-adresser å dele ut vil Internett stagnere, og ikke lenger kunne være en global II. Dette medførte en ny IP versjon som skulle gi rom for 2^{32} mulige adresser. En innføring av en ny løsning for IP-adressering og en ny

standard må være kompatibel med den gamle (Hanseth and Monteiro 1998, k.5). IPv6 ville imidlertid kreve en omlegging av mange nett. For at infrastrukturen som helhet ikke skal ta skade av utviklingen, er det nødvendig å sørge for en bakoverkompatibilitet ved design av nye standarder. Problemet med IPv6 ble midlertidig løst ved å ta i bruk brannmurer som skiller lokale nett fra globale, slik at de samme IP-adressene fra IPv4 kunne gjenbrukes[6].

2.1.3.2 Internett som en global infrastruktur

Internett består av mange mindre nettverk som følger de samme standardene slik at de i fellesskap utgjør en global infrastruktur. Internetts ende-til-ende arkitektur sier mye om hvordan infrastrukturen ser ut. Når det gjelder globaliteten så kan det være lettere å forstå denne veksten ved å se på Internett som en selvforsterkende prosess, som Grindleys modell (Grindley 1995, s.27) illustrerer i figuren under.



Figur 3: Grindleys modell

Internett har klart å bygge videre på sin egen suksess. Når den installerte basen til Internett vokser, slipper flere tjenester og produkter til. Dette gjør at brukerskaren øker siden flere finner det de søker. Dermed får de et større tillitsforhold til II'en fordi det fører til at verdien av infrastrukturen øker. Slik går det i en sirkel med økt spredning som igjen fører til større installert base.

Et "problem" med Internetts design er at den er veldig låst som følge av at alle må bruke den samme TCP/IP protokollen for å kunne være i stand til å kommunisere med hverandre. Stiavhengighet, eller *"path dependency"*, inntreffer når det oppstår en avhengighet av tidligere beslutninger i designprosessen, som ofte kan bestemme den videre veien for hvordan en II utvikler seg. Hvis det er stor stivavhengighet kan det gå utover fleksibiliteten til en II, fordi den ikke får utvikle seg fritt (Hanseth and Lyytinen 2004). Den teknologiske plattformen i form av TCP/IP protokollen har blitt låst for Internett i dens videre utvikling.

[6] IP versjonene hoppet fra IPv4 til IPv6, versjon 5 var bare et prøvestadium som ikke kom i bruk.

Det er ingen andre protokoller enn TCP/IP som vil fungere i kommunikasjonen på Internett. Hvis ikke nettverket er fritt for hindringer, for eksempel filtreringsapplikasjoner, vil det ikke være garantert at det er riktige endepunkter som kommuniserer med hverandre eller om det er kommet noen uønskede tredjeparter inn i forbindelsen. Siden det er mange mennesker som bruker Internett blir det fort vanskelig å vurdere hvor innholdet kommer fra og hvem det er ment for.

2.1.3.3 Internett som et massemedium

Definisjonen på et massemedium er at det skal være en form for massekommunikasjon, det vil si kommunikasjonskanaler eller meddelsesmidler som gjør det mulig å spre et budskap til mange mennesker over et stort område på kort tid (Wikipedia 2008). Massemediene blir kalt ”den fjerde statsmakt” fordi de gjennom overvåkning og rapportering indirekte kontrollerer de andre statsmaktene regjering, parlament og domstoler. Tradisjonelle massemedier er aviser, radio og fjernsyn som formidler nyheter og informasjon, underholdning, reklame og propaganda. Mens aviser og tidsskrifter tilhører de tidligste massemediene vi har, tilhører Internett et av de nyeste innslagene, og antagelig også det største. TV kan riktignok sende over landegrenser, men Internett gir, gjennom sin www applikasjon, mulighet for å sende ut og hente opp informasjon når som helst en måtte ønske, forutsatt at ingen blokkerer trafikken.

Internett har en økonomisk fordel ved at nesten alle har mulighet til å bruke det, fattig som rik. Dermed kan i praksis hvem som helst gi uttrykk for sine meninger i innlegg som alle kan aksessere, gitt at det er mulig å finne siden. Til sammenligning vil en avis eller TV innebære kostnader før en privatperson kan ta dem i bruk.

Mye av det som har gjort at Internett har vokst til dagens proporsjoner er at det er basert på folks samarbeid gjennom åpen programvare. Ved å la alle brukere av nettet være med på å forbedre programvaren har Internett oppnådd en popularitet som har overgått all forventning, blant annet fordi det er en struktur som fungerer. Lickliders visjon om at alle skulle ha det ”galaktiske nettet” tilgjengelig, på jobben som i hjemmet, har i dag blitt en realitet. I tillegg er vi ikke lenger begrenset til spesifikke kontaktpunkter. Med trådløs aksess og mobilteknologi kan vi like gjerne koble oss opp mot Internett mens vi er ute og reiser, eller bare går en tur til butikken.

Forskjellen mellom Internett som massemedium og som en global infrastruktur bør presiseres. Massemediumet er Internett som en helhet, og er ukontrollerbart i sin omfattende størrelse og de utallige oppkoblingsmulighetene. Internett som en global infrastruktur kan derimot kontrolleres via de som kontrollerer ”sin” del av infrastrukturen (Larsen, Wik et al. 2000). Denne dualiteten mellom infrastrukturen og massemediet har gitt rom for utallige

diskusjoner om Internett som et ukontrollerbart miljø, spesielt når det kommer til om det er mulig å applikere effektiv filtrering og sensur i slike omgivelser.

2.2 Filtrering og sensur

Filtrering og sensur er to begreper som har lett for å flyte over i hverandre når de skal brukes i Internettsammenheng. For eksempel har en nettside blitt sensurert hvis den har blitt fjernet for at brukere ikke skal kunne lese innholdet på den, men den kan også ha blitt utilgjengelig ved bruk av filtreringsteknikker som har lokalisert den. Nettsiden har først gjennomgått en filtrering, for deretter å bli sensurert. En vesentlig forskjell mellom filtrering og sensur er at filtreringsprogrammer i utgangspunktet er frivillige å bruke, i den forstand at den som eier maskinen selv kan bestemme om programmene skal tas i bruk. Sensur på den andre siden brukes gjerne i forbindelse med når offentlige myndigheter forhåndssensurer trykte medier som bøker, aviser, tidsskrifter eller teater og film.

En nettside som har blitt blokkert i etterkant følger ikke egentlig definisjonen av ordet sensur. Et tema som først har blitt publisert vil mest sannsynlig allerede ha nådd noen, slik at det vil være mulig å nå informasjonen via andre kanaler enn den sensurerte kanalen. I Norge sier den norske grunnloven paragraf 100 at ”*Trykkefrihed bør finde Sted*”, og vi er vant med at det er fri ytringsrett. Dette er ikke tilfelle for alle land i verden, og hvis en bruker bor et sted hvor myndighetene for eksempel jevnlig sperrer alle kommunikasjonsforsøk fra ISP’ene[7] ut av landet vil blokkeringen være så effektiv at det likevel kan være snakk om en ”suksessfylt” sensur.

Denne oppgaven vil fokusere mer på filtrering enn sensur, men fordi de påvirker hverandre så vil det være naturlig å komme inn på sensur i casestudiene. Dette vil blant annet komme opp i case 3 der Internettbruken i Kina og Egypt blir presentert. Spesielt Kina har valgt å følge strenge regler for å holde dette nye massemediet under kontroll. Her vil all filtrering foregå ut fra bestemte kontrollpunkter, selv om disse punktene i noen tilfeller kan holdes mer skjult enn andre steder.

2.2.1 Kontrollpunkter for filtrering

Generelt kan det sies at Internettfiltrering kan oppstå ved fire kontrollpunkter i nettverket: Internett backbone, ISP’er, institusjoner og på individuelle datamaskiner (ONI 2008). Det første punktet blir som regel utført ved internasjonale gateways ved at det implementeres nasjonale filtreringsteknikker som kan påvirke hele land. ISP’er implementerer som regel

[7] ISP står for Internet Service Provider og vil bli brukt som forkortelse for nettleverandør gjennom oppgaven.

filtreringsteknikker som regjeringen har foreslått. Filtrering på institusjonsnivåer kan være på Internett-kafeer, universiteter, statlige arbeidsplasser og lignende. Filtreringer her skjer gjerne for å håndheve de reglene som er viktige for institusjonen det gjelder. Det siste punktet kan for eksempel gjelde datamaskinen i hjemmet hvor brukere velger å installere filtreringsprogrammer. Disse kontrollpunktene vil bli nøyere presentert i casestudiene.

Grunnene for filtrering avhenger av situasjonen. Filtrering som foregår på landsbasis skjer helst i land som utøver streng Internett-politikk, mens filtrering i private hjem kan være for å skjerme definerte brukere som barn i forskjellige aldre. Arbeidsplasser på sin side kan finne det økonomisk lønnsomt å ta i bruk tidsbestemte filtreringer for å blokkere nettsider som tar fokuset vekk fra arbeidet i kontortiden (Øien 1998).

2.2.2 Filtreringsanalyser

Når vi hører ordet filtrering i forbindelse med Internett tenker vi gjerne på at enkelte sider blokkeres. Dette er riktignok en form for filtrering, men bare en av mange. Filtrering kan i praksis også brukes for eksempel innen virusbeskyttelse til å finne dataormer, og til å filtrere bort bestemte deler av nettsider. For å få til dette brukes det forskjellige typer filtreringsanalyser og algoritmer. Programvareutviklere kommer med stadig mer avanserte filtreringsmekanismer. Generelt kan det sies at filtreringsprogrammer jobber med et sett datafiler som deretter sammenlignes mot et forhåndsdefinert sett med regler. Datafilene kan være alt fra en nettside til en nyhetsgruppe eller e-post.

Filtrering av Internett åpner for flere problemstillinger, som hvordan vi skal få et program til å takle menneskelige perspektiver som meninger bak ord og uttrykk. Siden verdier og meninger ikke kan bli analysert etter samme kriterier som ”vanlige” ord så vil dette i noen tilfeller føre til misoppfatninger og filtreringer på feil grunnlag. Det er som regel to løsninger på slike dilemmaer som også viser seg å være de to største utfordringene og problemene ved filtrering. Den ene måten er å sette kriteriene for hva som skal filtreres så lavt at det ikke er fare for at unødvendig mye filtrering skjer. Dette vil føre til hva som kalles underblokkering, hvor også uønskede data vil slippe gjennom. Den andre måten vil på tilsvarende måte føre til at for lite informasjon slipper gjennom fordi kriteriene er så høye at det oppstår overblokkering. Dermed vil informasjon som i utgangspunktet ikke er uønsket eller utgjør noen fare, likevel bli filtrert bort slik at det fører til tap av data.

Ulemper som over- og underblokkering åpner for at flere organisasjoner ansetter personer til å overvåke, vurdere og filtrere informasjon. Ofte vil en innholdsanalyse utført av mennesker avdekke hva som vil være nyttig filtrering. Denne fremgangsmåten er imidlertid ikke realistisk å håndheve for alt innhold på Internett, på grunn av dets eksponentielle vekst. Med slike mengder av data å se gjennom har det blitt nødvendig å utvikle automatiske

søkeverktøy med forhåndssatte søkekriterier. Det er vanlig å dele slike filtreringsprogrammer i to kategorier; filtre basert på *automatisk analyse* og filtre basert på *innholdsanalyse* (Øien 1998).

2.2.2.1 Automatisk filteranalyse

Dette er filtermetoder som søker gjennom nettsteder og blokkerer de sidene som har forbudte nøkkelord, bilder eller en annen form for kriteria som har blitt satt. Ofte brukes det ferdige filtreringsordlister i disse programmene, men en vanskelighet med dette er at listene krever stadig oppdatering. Siden det er disse listene som setter filtreringsnivået er det noen leverandører som leverer ut programmene gratis, men tar betalt for ordlistene.

Automatiske filtreringsmetoder kan fort føre til overblokkeringsfiltrering siden det er tilfeller hvor meninger og verdier av nøkkelord kan bli borte i analysen. For eksempel kan et pornografisk rettet filter blokkere sider som inneholder ord som ”Moby Dick” eller ”breast cancer”.

En metode som er relatert til nøkkelordsøk har vi når analysen blir brukt til å dynamisk endre innholdet på en nettside ved å fjerne noen av ordene og legge igjen andre isteden, slik at informasjonen får et annet budskap. Nettsiden er ikke blokkert, så det er en mulighet for at brukere ikke engang får med seg at siden har blitt filtrert. Dermed blir heller ikke nysgjerrigheten vekt for hva som har blitt sensurert.

2.2.2.2 Innholdsanalyse

For å kunne utføre en innholdsanalyse trengs det en vurdering av innholdet på www. Noen må utføre denne vurderingen, og som regel er det innholds- eller programleverandøren som gjør dette. For å få med semantikken i innholdet utføres vurderingene i utgangspunktet av mennesker.

På grunn av den store informasjonsmengden på Internett har det, også for denne metoden, blitt tatt i bruk automatisk innholdsanalyse som jobber hovedsakelig på http-protokollen. Forskjellen på automatisk filteranalyse og automatisk innholdsanalyse ligger i merkingen av innholdet. Mens den første metoden bruker ferdige ordlister til å gjennomføre søk, bruker den andre en merking av innholdet og vurderer det etter hvilken klasse og tema den hører inn i. En slik merking gjøres etter vurderingskriterier. Aktørene bak filtreringsprogrammer kan enten utvikle sitt eget vurderingssystem, eller de kan ta i bruk ”ferdigklasser” som for eksempel Platform for Internet Content Selection (PICS) [8]. Brukere som velger å bruke et filtreringsprogram kan dermed stille inn hvilke nivåer og graderinger av innhold en ønsker i følge vurderingssystemet. Filtreringen kan skje gjennom programvare

[8] PICS er ikke en standard, men en mal som assosierer innhold på Internett med kategorier ved bruk av metadata. Metatagen forteller hvilken kategori nettsiden har blitt merket med slik at søkemotorene kan lese tagen.

installert på brukerens datamaskin, eller gjennom tjeneren brukeren er knyttet opp til (Staksrud 2002).

Vanskelighetene ved å lage en fast, internasjonal standard for filtreringsanalyser er at det ikke tas hensyn til lokale eller nasjonale behov. Løsningen har vært å utvikle kategorier som tar hensyn til nettopp dette. Ved å merke innholdet med metatager kan det klassifiseres etter de kriterier det gjeldende landet vektlegger. Dette kan skje ved å bruke internasjonale standarder som Internet Content and Rating Association (ICRA). For ICRA er de valgte kategoriene sex, nakenhet, vold og fornærmende språk. Fordi ICRA bygger på PICS kan disse kategoriene leses av alle nettlesere som har lagt inn støtte for dette. Blant annet har Microsoft valgt å bruke ICRA i sin Internet Explorer (Staksrud 2002).

Aktører som lager sine egne innholdfiltre kan velge å gjøre dem svært enkle ned til bare to klasser: godkjent og ikke-godkjent innhold. Det er opp til aktørene å velge hva slags nivå filtreringsanalysene skal kjøre på applikasjonene deres. I tillegg finnes det bestemte kategorier som inkluderingsfiltre hvor brukere er tillatt å aksessere en *hviteliste*. Dette er en liste som inneholder godkjente nettsteder, mens alt annet blir blokkert. Denne metoden er antagelig mest brukt i enkelte organisasjoner hvor begrenset tilgang til forskjellige nettsteder ikke er noen hindring for at arbeidsoppgavene kan utføres. Vi har også eksluderingsfilter-metoder som hindrer brukere å aksessere nettsteder som står på en *svarteliste.* Det betyr at alle nettsteder som ikke står på listen er lovlig å aksessere.

2.2.2.3 Nettikette

En annen form for filtrering er en viss form for selvsensurering, men uten at det skjer en krenkelse av ytringsfriheten, slik innholdsfiltrering i noen tilfeller kan. Det foregår reguleringer på tre plan, ingen regulering, offentlig regulering eller bransjen regulerer som de selv syns passer. I Norge er Internettetisk råd et forsøk på det tredje (Øien 1998). Den Norske Dataforening (DND) har anbefalt at man heller utarbeider en ”Vær varsom plakat” med retningslinjer for etisk adferd på Internett, enn å opprette et juridisk Internettetisk råd. De begrunner dette med at politi og domstoler allerede er satt til å håndheve brudd på norsk lovgivning, og at dette er tilstrekkelig myndighetsutøvelse (DND 2008).

Det har over tid vokst frem en del uskrevne regler for kommunikasjon via e-post, USENET og andre nettbaserte tjenester tilsvarende de vi er vant til fra hverdagslivet i samfunnet ellers. Disse reglene blir gjerne kalt nettikette eller nettvett, og fungerer som retningslinjer for ønsket oppførsel på Internett skapt av flertallets seriøse brukere (Nettikette 2006). Det er et mindretall av brukere som lager problemer for andre, og disse er ikke på langt nær mange nok til at alle bør kuttes vekk fra nettverksaksess. Mange av problemene som oppstår kan løses ved å reagere når en ser at det er grunn til å gjøre det, for eksempel i et universitetsmiljø, eller på en arbeidsplass. Det er mange utfordringer ved sensur og privatliv

på datamaskiner som er tilkoblet nettverk, og fornuftige brukere som viser etikk og skjønn kan løse mange av dem (Costello 1991).

2.2.3 Grensene mellom filtrering og sensur

Beskyttelse er motivet de fleste aktører gir når de blir spurt om hvorfor eventuelle reguleringer blir gjort. Men hvem skal egentlig beskyttes, og mot hva? Når det gjelder sensur av Internett er det noen typiske holdninger som går igjen. For det første vil de fleste forbinde sensur med noe negativt. For det andre vil en bruker (uansett hvem det er snakk om) antagelig innen få minutter finne informasjon som vil føles støtende. Mange ganger vil slikt støtende innhold være inspirert av brukerens egen kultur eller religion. Problemstillingen her blir hvilke begrunnelser for valg av sensurering av innhold man skal følge. Land med tverrkulturelle aspekter krever sine egne lokale tilpasninger. Konflikter oppstår for eksempel mellom Sørøst-Asias vekt på kontroll og Vestens liberale individualisme.

Det er imidlertid fem hovedstrategier som har gått igjen for land som har formulert en politikk for å kontrollere innholdet på Internett. Disse går på bruk av lovverk, selvregulering med Internettbransjen blant annet ved bruk av felles etiske regler, bruk av tipslinjer (spesielt i bekjempelsen av barnepornografi), informasjonsopplysning og holdningsskapende arbeid, og teknisk regulering for eksempel ved den nevnte filtreringen og klassifiseringen av innhold (Staksrud 2002).

På arbeidsplasser kan det argumenteres for at sensur av Internett er nødvendig, siden arbeidstakere er betalt for å utføre bestemte oppgaver som ikke inkluderer surfing på alle mulige nettsteder. Disse grensene vil ikke være like tydelige på en akademisk arbeidsplass.

”Tvilsom” informasjon kan enten sees som lovlig eller ulovlig, eller som etisk eller uetisk (Peace 2003). Lovlig og etisk innhold må selvfølgelig være usensurert. Ulovlig og uetisk innhold kan sensureres. Det er gråområdene som er problemet, for eksempel lovlig men uetisk (prostitusjon kan høre til denne gruppen) eller ulovlig men etisk (pengespill kan høre til denne gruppen), og det er slike forskjeller som blir klarere når forskjellige kulturer tar i bruk sensur. Sensurering krever i mange tilfeller en vurderingssak siden forskjellig verdenssyn påvirker hva folk finner støtende.

2.2.3.1 Farlig informasjon

Internett kan tilby alle former for informasjon for de som leter etter den. En vanlig kritikk fokuserer på voldsbruken i dataspill, bilder og på nettsider. En episode noen mener har tilknytning til farlig påvirkning fra dataspill skjedde 20.april, 1999. Da var det en skytetragedie ved en high school i Littleton, Colorado. To skolekamerater møttes en morgen, gikk og bowlet, for deretter å dra på skolen bevæpnet med halvautomatiske våpen, pistoler og

hjemmelagde bomber. De drepte tolv medelever og en lærer og ga flere varige mén før de skøt seg selv. I ettertid kom det fram at guttene var ivrige dataspillere av voldsspillet *Doom*. Dette førte til at opinionsmålingene for Internett-sensur gikk opp, og hele trettifire prosent av amerikanerne mente Internett hadde mye av skylden for drapene[9]. Halvparten av alle spurte mente at regulering av Internett var en effektiv måte å stoppe vold i skolene (Staksrud 2002).

Farlig informasjon på Internett kan være ”umoralsk” eller ”korrupt” informasjon. Bruksområdene på Internett kan deles i flere kategorier: En kategori er ”speech acts”, det vil si handlinger som gjøres via informasjonsteknologi som å overføre penger, stemme, kjøpe noe, signere en kontrakt og lignende. En annen kategori er selve spredningen av informasjon, og med *farlig informasjon* så er det denne delen det tenkes på. Spredning av informasjon kan igjen skilles i ervervelse og tilgang til informasjon. Tilgang betyr at en person kan få tak i informasjon hvis ønskelig, mens ervervelse er den aktive forståelsen av denne informasjonen (Müller 2006).

I sammenheng med filtrering og sensur kan det nevnes fem kategorier for farlig informasjon som ikke burde spres (Müller 2006):

- *hemmeligheter,* eller privatliv som er beskyttet under personvern.
- *Informasjon som er støtende eller ærekrenkende*.
- *Løgner,* for eksempel hvis noen sprer informasjon om at Holocaust aldri skjedde (i Tyskland er dette ulovlig å påstå).
- *Korrupt informasjon* som er informasjon som forventes å ha en skadelig effekt på personer som for eksempel mindreårige.
- *Informasjon med spesielle rettigheter* som patenter og copyrights.

En slik klassifisering av farlig informasjon er ikke en fasit for temaer det bør applikeres filtreringsapplikasjoner på, men gir en god pekepinn på temaer som er i gråsonene for hva som er lov til å filtrere bort og hva som bør filtreres bort.

2.2.3.2 Ytringsfrihet

Selv om det er flere negative og uventede sideeffekter av en global infrastruktur som Internett, er det også en sterk ressurs som gjør at bruken bare fortsetter å øke. I et forsøk på å kontrollere de negative aspektene ved Internett opprettet Norge i 2002 Datakrimutvalget. I

[9]Journalisten Michael Moore lagde en dokumentarfilm om denne hendelsen med tittelen *Bowling for Columbine*. Teorier som lett tilgang på våpen og store sosiale forskjeller som fyrer opp under voldelige løsninger sto også sentralt. Et av hovedpoengene til Moore var at massemediene bidrar til å skape frykten i det amerikanske samfunnet.

2007 overleverte utvalget "Lovtiltak mot datakriminalitet" til Justis- og Politidepartementet for å kontrollere eventuell kriminell aktivitet på nettet, spesielt med tanke på barneporno (Datakrimutvalget 2007). En som surfer på nettet og kommer inn på et nettsted med ulovlig innhold vil få opp en side som Kripos[10] har laget som sier at nettstedet er blokkert og at bruk av nettstedet vil være straffbart. Denne formen for blokkering er mulig i Norge bare ved frivillig samarbeid mellom norske myndigheter og Internettleverandører[11]. Det betyr at ikke alle Internettleverandørene velger å være med på dette samarbeidet, og dermed blir filtreringen bare delvis effektiv.

Et annet problem er hvordan utenlandske sider skal håndteres, siden reglene for hva som er ulovlig innhold varierer mellom Norge og andre land. For eksempel er pengespill som poker forbudt i Norge, mens det er legalt andre steder. Hvis Norge skulle begynne å blokkere innhold som blir distribuert via lovlige kanaler i andre land som Norge ikke nødvendigvis har noe samarbeid med, såkalte "data havens", blir spørsmålet om vi skal iverksette nasjonale tiltak for filtrering istedenfor bare på tilbydernivå. Det finnes flere sorter for innholdsfiltrering som ikke tar ned hele siden, men bare deler av den. Spesielt Kina har blitt verdens fremste ekspert på dette feltet. Med de teknikkene som brukes i Norge vil en filtrering gi samme effekt som når en server eller et nettsted blir tatt ned. Datakrimutvalget har delt seg ved at flertallet ikke vil ha en slik form for filtrering. Dette forklares med at hensynet til EMK[12] artikkel 10, ytringsfriheten, må settes foran sensurering av utenlandske nettsider. Bestemmelsen oversatt til norsk lyder:

"Enhver har rett til ytringsfrihet. Denne rett skal omfatte frihet til å ha meninger og til å motta og meddele opplysninger og ideer uten inngrep av offentlig myndighet og uten hensyn til grenser. Denne artikkel skal ikke hindre stater fra å kreve lisensiering av kringkasting, fjernsyn eller kinoforetak."

Ofte må det gjøres en vurdering av dilemmaet mellom ytringsfrihet og sensur, og hvem som skal ha lov til å sette disse grensene. I Norge har vi valgt å unngå nasjonal kontroll av filtreringer. Dette er blant annet basert på kritikken med at når barneporno kan sperres, så kan også andre nettsteder som inneholder litteratur, ytringer og meninger sperres. En annen løsning er å sørge for å ha full kontroll på hva slags innhold som er tilgjengelig på Internett for brukere og heller la ytringsfriheten bli nedprioritert. For å få til dette brukes det enten en eller flere sorter for tekniske filtermetoder, eller kombinasjoner av disse. Det finnes også

[10] Den nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet

[11] Kripos' barnepornofilter er utviklet i samarbeid med Telenor

[12] Den Europeiske Menneskerettskonvensjon

ikke-tekniske filtermetoder, som pålagt selvsensur eller 'take-downs', som for eksempel blir praktisert i Kina hvor de fører en strengere Internettpolitikk enn typiske vestlige land gjør.

2.3 Oppsummering

Den historiske opprinnelsen til Internetts elementer besto av et pakkesvitsjet datanettverk basert på ende-til-ende arkitektur og standardiserte protokoller. En distribuert topologi gir fleksibilitet til Internetts arkitektur ved at datapakkene kan bruke flere veier gjennom et åpent nettverk, fritt for applikasjoner som kan påvirke pakkene. Nettverkskjernen holdes enklest mulig ved å legge funksjonalitet (i form av applikasjoner) på endepunktene i henhold til ende-til-ende arkitekturen. En slik arkitektur skaper et mer fleksibelt nettverk og støttes av et sett med standardiserte protokoller som gjør det enklere for utviklere å jobbe på hver sin del av applikasjonene uten å måtte tenke på hvordan nettverket fungerer. Alt som finnes av tjenester i Internett er basert på slike protokoller, som http, ftp og smtp. Etter hvert har det imidlertid kommet til nye egenskaper og funksjoner ved mye brukte nettverkstjenester som www. Dette har ført til en utvikling som ingen forutså den gangen nettverksprosjektet startet. Internetts stadig økende informasjonsmengde har gitt grunnlag for å lage applikasjoner som til en viss grad kan kontrollere ukontrollerbare omgivelser ved bruk av filtreringsapplikasjoner som for eksempel gir sensurering. Det er flere problemstillinger rundt filtrering og sensurering, som hvem som skal bestemme hva som er akseptabelt innhold og hva som ikke er det. Dette har ført til forsøk på tilnærminger av standardiseringer for å klassifisere støtende og ulovlig innhold som PICS og ICRA.

De største dilemmaene ved filtreringsapplikasjoner omhandler over- og underblokkering. Automatisering av slike applikasjoner er ofte en nødvendighet på grunn av de store informasjonsmengdene som er tilgjengelig på Internett. Internettfiltrering kan oppstå ved fire kontrollpunkter i nettverket; Internett backbone, ISP'er, institusjoner og på individuelle datamaskiner. For å utføre filtrering på for eksempel en større del av et nettverk, kan det være ønskelig å implementere filtrering hos en ISP for å få best mulig effekt. Imidlertid tilhører en ISP den indre delen av et nettverk, og dermed fører det til brudd på ende-til-ende arkitekturen som sier at kjernen skal være enklest mulig for å ivareta fleksibiliteten i nettverket. Samtidig bidrar filtrering med en større tjeneste hvis den blir implementert der den gjør mest nytte for seg, og på den måten bidrar også den med fleksibilitet. Denne spenningen mellom filtrering og ende-til-ende arkitekturen vil bli nøyere omtalt i det neste kapittelet.

"If this stone won't budge at present and is wedged in,
move some of the other stones round it first."
- Ludwig Wittgenstein

3 Teoretisk bakgrunn

Dette kapittelet gir et teoretisk rammeverk av oppgaven basert på tidligere forskning for å forstå fenomenet filtrering og dets påvirkning på Internett. Samtidig etableres det tre relevante hypoteser for oppgaven ut i fra relevant teori for informasjonsinfrastrukturer (heretter kalt II), ende-til-ende designteori og teknologisk determinisme[13]. Internett kan kalles for den ultimate II, og ved å bruke II-teori som verktøy ønsker jeg å klargjøre rollen filtrering har innenfor Internett. For å gjøre dette vil designutfordringer bli tatt opp i form av ende-til-ende prinsippene som Internett bygger på. Det blir presentert sentrale begreper som *ende-til-ende arkitekturens kobling til generativitet og fleksibilitet*. Videre gjennomgås det noen problemstillinger som oppstår ved økende integrasjon av filtreringsapplikasjoner i nettverket, som *kan* bidra til mer kompleksitet for Internett. Et naturlig spørsmål er hvilken utvikling ende-til-ende arkitekturen går mot og hvordan dette påvirker samfunnet. Dette temaet behandles i delkapitlet om den teknologiske determinismen.

3.1 Informasjonsinfrastrukturer

En II kan vise seg i mange former, fra veinett og telefonnett til Internett, som består av sammenkoblede datanett som bruker den samme standarden. Mye av utfordringene ved en II ligger i hvordan man skal takle designutfordringene som kompleksiteten bringer når II'en vokser. I tillegg er det gjerne snakk om store skalaer og funksjonelle vanskeligheter ved at ikke alle muligheter kan kartlegges i designfasen. (Hanseth and Lyytinen 2004).

[13] Selv om II-teori og ende-til-ende designteori ikke er gjeldende teorier på lik linje med teknologisk determinisme velger jeg å bruke dem som en del av det teoretiske grunnlaget. Dette er fordi de er meget relevante for denne oppgaven og vil bidra til å klargjøre definisjons- og begrepsbruken i analyse- og diskusjonsdelen.

3.1.1 Definisjoner og begreper

Definisjonen for en II er i følge Hanseth og Lyytinen (2004):

en delt og heterogen installert base under stadig utvikling, og som har informasjonsteknologiske muligheter i brukersamfunn som er basert på åpne eller standardiserte grensesnitt.

For at definisjonen skal gi mer mening går jeg først gjennom hva de forskjellige begrepene betyr og hvordan Internett oppfyller dette.

En delt II betyr at samme enhet brukes av flere brukere eller brukergrupper. Et eksempel på en slik delt enhet er e-post systemer. Disse kan se forskjellige ut avhengig av programleverandøren, men de representerer den samme bruken. Det finnes også flere andre tjenester som er delt mellom brukere, for eksempel samtaler mellom grupper og fildelingstjenester.

En heterogen installert base består av ulike tekniske og ikke-tekniske elementer med relasjoner som endres over tid, men som alltid er knyttet sammen i et sosio-teknisk nettverk som blir mer komplekst etter hvert som en II vokser. Den installerte basen har alltid elementer som har eksistert fra før den ble definert, med varierende betingelser og krav for videre utvikling. For Internett består den installerte basen av komponenter som brukererfaringer og praksis, programvare, basestasjoner, satellitter, kabler, rutere, maskinvare, ”back bones” i form av standarder og spesifikasjoner, alle integrerte tjenester, brukere av tjenestene og utviklere inkludert deres kunnskaper som blir knyttet til basen. Denne installerte basen er sosio-teknisk siden den har en blanding av elementer fra teknologisk til sosial art, hvor flere av elementene alltid har vært der. I dag strekker den installerte basen til Internett seg over hele verden. En typisk egenskap ved installerte baser er at de er i stor grad uomstøtelige (Hanseth and Monteiro 1998, k.9).

Åpenhet i sammenhengen II betyr at det er ingen begrensninger på antall brukere, antall noder i nettverket, teknologiske komponenter eller andre elementer i den installerte basen. I tillegg er en II åpen i tid, fordi den ikke har noen bestemt start eller sluttdato. Internett oppfyller kravet om åpenhet ved at den ikke har noen avklarte grenser for sin II, og kan fortsette å vokse.

Standardiserte grensesnitt er en nødvendighet for å unngå at det skal bli mange uavhengige forbindelser hvor alle har hvert sitt sett med regler. Isteden er det ønskelig å kunne knytte sammen og integrere elementene i en ekte II som er basert på de samme standardene. Internett har bygd hele sin (protokoll-)struktur på standarder.

Internett kan i aller høyeste grad defineres som en II, og dens stadige vekst gjør at den blir et godt eksempel på alle utfordringene en II står ovenfor, med uante sideeffekter og spørsmål om hvorvidt den er i stand til å takle disse.

3.1.2 Fleksibilitet og generativitet

Fleksibilitet er viktig ved design av en ny II med tanke på ikke å låse fast mulighetene den installerte basen gir. Fleksibilitet kan oppnås ved modularisering, slik at man kan lage flere mindre enheter og bruke enkle grensesnitt mellom de forskjellige modulene. Dermed blir det lettere å beholde oversikten, sammenliknet med et stort system som inkluderer alle funksjonene for alle brukere, noe som sjelden vil være nødvendig. Det klareste uttrykket for modularisering i datanettverk er utviklingen av standardmodellen, det vil si Internettprotokollen som ble vist i kapittel 2 (Sandvig 2006).

En løsning for å bevare fleksibilitet kan være å fokusere på den installerte basen og hvordan denne kan vokse. Ved å bruke den installerte basen som et anker fins det et trygt utgangspunkt for å kunne konsentrere seg om den videre veksten og unngå teknologiske feller (Hanseth and Lyytinen 2004). Internett og bruken av www er et eksempel på hvordan det er mulig å fortsette å bygge på den installerte basen istedenfor å etablere en ny, og det har vært en løsning som hittil har fungert veldig bra.

Generativitet er en generalisering av ende-til-ende prinsippene og en strategi for å kunne øke fleksibiliteten til en II ved å tenke gjennom noen prinsipper og krav som kan testes på den. Zittrain (2006) snakker om hvordan meningen bak generativitet har en essensiell kvalitet; det å *tillatte uvarslede endringer gjennom store, varierte og ukoordinerte publikum*. Dette er i stor grad avhengig av hvor nærme de uvarslede endringene er ende-til-ende arkitekturen. Med dette har Zittrain presentert fire generelle punkter for å oppnå generativitet, som også kan applikeres på Internetts design:

Det første punktet omhandler *hvordan teknologiens innflytelseskapasitet er for forskjellige oppgaver*. Protokollbruken til Internett har løst mange problemer ved datafordeling, og det er en billig nettverkstjeneste. Det teknologiske grunnlaget glir over i formålet med neste punkt som går på *tilpasningsdyktigheten over et område av forskjellige oppgaver.* Tilpasningsdyktigheten til Internett har ført til at det har en sterk innflytelse på en rekke tjenester innenfor områder som vitenskapelig ressursdeling, teknologi, e-handel, sosiale nettsteder og mye mer. Det er en II som kan applikeres på stadig nye tjenester. Tredje punkt dreier seg om *hvor lett det er å lære seg å håndtere teknologien*. Selv om Internett tilbyr mange vanskelighetsgrader hvor flere trenger erfarne brukere, er det lav terskel for å ta i bruk nettverkets tjenester for førstegangsbrukere. Dette kravet er også influert av aspekter som for

eksempel tilgjengeligheten på kunnskapsrike folk, dokumentasjon og standardiseringsnivåer (Hanseth and Nielsen). Sett fra en teknisk side er det et strukturert nettverk som tillater brukere å designe nye applikasjoner uten å måtte tenke på de forskjellige nivåene med protokoller og behandling av datapakker. Siste punktet omhandler *tilgjengelighet*. Internett har ingen sentrale portvoktere som blander seg inn i programutvikleres arbeid med å lage nye applikasjoner, slik at tilgjengeligheten er stor. Disse punktene bidrar i felleskap til Internetts globalitet, som kan nås overalt både av utviklere og brukere.

Benkler bruker ikke ordet generativitet, men det er disse punktene som omhandles når han sier at ende-til-ende arkitekturen og programmerbare terminaler har et felles samspill som begge avhenger av hverandre. Dette er fordi en innretning er en enhet med et begrenset og definert sett av funksjoner (Benkler 2006), for eksempel vaskemaskin, mikrobølgeovn, radio og lignende. Slike enheter har datamaskiner i seg, men programvaren kan sjelden modifiseres av brukerne. De er hva Star kaller *fikserte-valg kategorisett* som presenterer barrierer for brukerne (Star 1999). Benkler er bekymret over flere forslag om å øke sikkerheten og stoppe "skadelig" bruk av Internett (ved nye lovvedtekter og lignende) vil hindre brukere av Internett i å programmere sine egne datamaskiner. En parallell til dette er et eksempel Hanseth trekker fram om *trusted computing* teknologi[14] og hvordan det kan bli implementert på måter som begrenser mulighetene for brukerne *og* er rotfestet i loven (Hanseth and Nielsen) En slik utvikling vil låse muligheten brukere har over datamaskinen og Internett, og vil bryte med fordelene ved en ende-til-ende arkitektur.

Selv om generativitet er et universelt begrep uavhengig av teknologi, er den koblet til ende-til-ende arkitekturen, som er et kommunikasjonsnettverk. En av grunnene til at Internett anses som et godt eksempel på en vellykket II er at det oppfyller alle kravene om generativitet. Det ble innledningsvis for oppgaven nevnt at filtreringsapplikasjoner brukes på Internett blant annet for å oppnå mer kontroll. Hvis dette sees i sammenheng med dette avsnittet, hvor det er blitt understreket hvor viktig generativiteten er for å ivareta fleksibiliten til Internett, kan følgende hypotese utledes:

Selv om formålet med filtrering er å få mer kontroll bidrar det til en mer komplisert nettverksstruktur, og er med på å skade generativiten for Internett.

Fra Internett først ble designet og til i dag har det vært flere utvidelser av bruksområdet som har vært med på å skape uro i arkitekturen Internett er basert på. Alle II'er har uforutsette hindringer i form av designutfordringer som gjerne viser seg på et senere tidspunkt enn da

[14] For mer opplysninger om trusted computing kan denne linken følges. Den viser en kort animasjon sett fra et kritisk synspunkt http://www.lafkon.net/tc/, aksess 10.06.2008.

strukturen ble formet. Dette er risikoer som alltid vil være tilstede, men ved å ta høyde for dem ved å satse på å ivareta fleksibiliteten vil det bli lettere å håndtere nye, kompliserende faktorer.

3.1.3 Risk og kompleksitet ved en II

Ulrich Beck (2003) har presentert en teori om hvordan ønsket om for mye kontroll kan føre til det motsatte i praksis. Mye kunnskap og forsøk på å integrere mest mulig med målet om å skape full kontroll øker også kompleksiteten i II'en slik at det kan bli mange uoversiktelige elementer i infrastrukturen. Spørsmålet blir om dette vil skje med Internett når filtreringsmetoder implementeres i et ønske om å skape mer kontroll over nettverket.

Under utviklingen av informasjonsteknologi har det kommet flere vinklinger og problemstillinger til denne teknologien, som har tatt IT videre til ICT. Det er alt nevnt stadig økende, komplekse oppbygninger for å kunne gi mer fleksibilitet til brukeren. Egenskapene til en II representerer også styrkene ved en II. Siden teknologi i dag har blitt en integrert del av samfunnet har det i større grad blitt nødvendig å se på brukeraspektene. Ved å bli bedre kjent med hvilke sosiologiske prosesser som kan finne sted i et teknisk samfunn kan det gi større innsikt i hvilke problemer som kan opptre i form av sideeffekter. Siden en II er et sosio-teknisk nettverk finnes det mange ukjente faktorer, for eksempel hvordan brukere vil oppfatte og ha nytte av systemet. Internett er et eksempel på dette siden ingen visste at det ville bli en en så stor brukermengde den gangen ARPAnet startet opp sine første eksperimenter.

II-teori kan hjelpe til med å strukturere forståelsen av helheten i sosio-tekniske systemer. Når vi får navn på enkeltdelene i systemet og kan konkretisere hindringer er vi i stand til å kunne legge opp en videre strategi til å forbigå disse. Noen av de komplekse problemstillingene som II-teori derimot ikke klarer å belyse kan stamme fra mangelen av teorier som kan beskrive problemet. I følge en kontroversiell teori av Whorf (1956, s.66) kan vi bare konstruere tanker som reflekterer ord vi kan. Utfordringene er altså de samme; kompleksiteten som er ett av kjennetegnene til en infrastruktur er fortsatt til stede og gjør det vanskelig for utviklerne å kunne forutse alle sideeffektene. Målet blir vel heller å kunne sette navn på flest mulig av dem.

"Increased integration leads to increased complexity, ... increased complexity leads to increased risks. … the result of the integration efforts is increased risks, that is less control." (Hanseth and Ciborra 2007)

Med andre ord: når en II vokser blir den mer kompleks, sammensatt og sammenflettet. Noen områder av strukturen kan gi uforutsette effekter, som igjen kan skape domino- eller

boomerangeffekter i systemet. Når vi ikke kan kartlegge alle slike effekter, noe vi sjelden kan, har vi plutselig ukjente risikofaktorer. Disse risikoene øker med veksten av integrasjonen (Hanseth and Lyytinen 2004).

Denne oppgaven vil blant annet teste en bestemt boomerangeffekt; hvorvidt filtrering slår tilbake på designen av Internett. Internett som et sosio-teknisk system har en iboende kompleksitet i seg, som *kan* bli større ved økt integrasjon. Hvis denne kompleksiteten øker vil generativiteten i ende-til-ende arkitekturen bli mindre, og dette vil føre til mindre fleksibilitet for Internett. For å gjøre denne problemstillingen klarere vil det neste avsnittet ta for seg ende-til-ende arkitekturen.

3.2 Ende-til-ende designteori

Argumentasjonen rundt ende-til-ende (heretter kalt e2e) arkitekturen ble lagt fram av nettverksarkitektene Jerome Saltzer, David Reed og David Clark i 1981. Den teknologiske beskrivelsen er blitt tatt opp i kapittel 2. Her ble det blant annet omtalt hvordan intelligensen i nettverket er fordelt ute på endepunktene for at minst mulig kompleksitet tilføres nettverkskjernen, slik at nettverket kan støtte flest mulig applikasjoner. Dette avsnittet vil ta for seg noen synspunkter og teorier om hvordan Internett følger denne designen i dag, dens videre utvikling og hva slags påvirkning filtrering har.

3.2.1 Ende-til-ende prinsippene

Selve e2e-konseptet kommer av Internett før den ”siste” utviklingen av applikasjoner, altså den gang alle funksjoner virkelig ble implementert ved endepunktene. Hovedprinsippene ved e2e er at hvis en funksjon trenger deltagelse av endepunktene for nettverket skal den ikke implementeres på noe annet sted innenfor nettverket. Hvis dette skjer vil det oppstå en redundans. Dette vil da gjelde en hvilken som helst funksjon som blir implementert i kjernenettverket fordi funksjonen allerede er implementert ved et endepunkt. Videre kan det argumenteres for at en funksjon som likevel blir implementert i kjernenettverket uansett vil være redundant fordi det vil være applikasjoner som har tilgang på den, men som aldri vil trenge den. Et konsept ved designen til e2e er som nevnt at den skal være enkel i kjernen og at all kompleksitet skal ligge ute på endepunktene. Ved å tilføre applikasjoner i nettverket vil dette føre til større kompleksitet som kan medføre sideeffektene nevnt over, samt mer kostnader for alle nettverksbrukerne. Dette vil være uavhengig av om applikasjonene blir brukt eller ikke siden de fortsatt vil være der (Saltzer, Reed et al. 1981).

En komplisert kjerne vil utgjøre en større trussel for et nettverk. Hvis en applikasjon nå skulle feile kan den ta ned store deler av nettverket. Hadde det vært en applikasjon ved et endepunkt ville ikke denne kunne gjøre like stor påvirkning for andre deler. Nettverksdesignere gjør stor forskjell på elementer som er inne i nettverket og de som er utenfor. En feil ved en enhet inne i nettverket gir en mer *universal* slagkraft (Clark and Blumenthal 2000). Dette vil også gå utover den distribuerte strukturen vi så på i kapittel to, og Internett vil isteden kunne nærme seg en *desentralisert* struktur. Denne meningen deles av David (2001) som sier at en slik ny struktur blir drevet fram av alle aktørene som har spesielle interesser av å skape profitt på Internett, og som dermed bidrar med sine egne applikasjoner i kjernen.

Internettprotokollen er som byggesteiner som fungerer bra for alle applikasjoner som bruker den samme designen. Det som ikke ble tatt hensyn til da de første utviklerne av Internett la dette teknologiske grunnlaget, var bruksområder de ikke hadde forutsetninger for å vite om. Et eksempel er overføringer av video og lyd som brukes i stor skala i dag. Skulle disse applikasjonene fulgt e2e-prinsippet, hadde det betydd at Internett måtte sende den samme strømmen av video og lyd like mange ganger til alle som ville se dette. Det ville mest sannsynlig endt med overlasting av data og kommunikasjonsbrudd. Isteden har applikasjonen blitt bygd ut til å mestre multimedia-strømmer som sender den samme strømmen bare en gang slik at denne går ut til alle som vil bruke den. Brukeres krav til slike nye tjenester er med på å dytte applikasjonene inn i nettverket, og filtrering har en stor rolle i så måte.

3.2.2 Filtreringens innflytelse på ende-til-ende

I dag er det flere applikasjoner som blir påført inne i nettverket, som brannmurer, filtrering og IP-maskeringsbokser[15]. Brannmurer kan utføre oppgaver utover det å gi beskyttelse fra skumle angrep utenifra. De kan også påvirke trafikk i begge retninger slik at de fungerer som trafikkfiltre. Måter å gjøre dette på er blant annet å stille inn hvilke programmer som skal ha tilgang på Internett og hvilke nettsider som skal blokkeres. Trafikkfiltre kan dermed bli *et generelt verktøy for å påføre kontroll på nettverket* (Clark and Blumenthal 2000). Et eksempel er overgangen fra en gammel IP-protokoll til en ny som viser hvor vanskelig det kan være å innføre endringer i en II som Internett som allerede har rukket å få mange brukere. Sommeren 1994 var det blitt laget en IPv6 som skulle bygge videre fra IPv4, men denne har ennå ikke blitt tatt i bruk selv om den er inkludert i alle nye operativsystemer. Isteden har det oppstått

[15] Også kalt Network Address Translators (NAT) som redigerer IP-adressene underveis i overføringen.

subnettverk ved å skjerme nettverkene fra hverandre i form av brannmurer som filtrerer nettverkstrafikken. Dermed kan flere maskiner ha samme IP-adresse uten å påvirke hverandre.

ISP'er står i en særstilling når det gjelder hva de kan og ikke kan, fordi de som regel ikke har mange lovvedtekter å følge (dette kan variere fra land til land). ISP'er har ikke kontroll over endepunkter men er en del av det interne nettverket. Det vil si at alle oppgaver en ISP gjør utover det å videresende pakker vil være en form for brudd på e2e-prinsippene. ISP'er pleier likevel å utføre en mengde forskjellige filtreringsoppgaver for å være i stand til å skille mellom kundene sine og hvilke tjenester de har betalt for. Dette kan sees på som markedsføring og hvordan gjøre profitt. En kunde som betaler mer vil for eksempel ha rett til tilgang på forskjellige spilltjenere, mens en minimumskunde vil bli blokkert fra dette. I prinsippet fungerer dette på samme måte som at førsteklasses flypassasjerer betaler mer og får tilgang på bedre mat og seter. Forskjellen er at i "Internett-land" er dette brudd på e2e-filosofien, og noen Internett-entusiaster vil si at slike restriksjoner som blir overført til Internett-tjenester er moralsk feil (Clark and Blumenthal 2000).

Utvidelsen av bruksområder på Internett er i samsvar med II-teorien og den installerte basen som vokser og utvikler seg videre også innenifra kjernen – og det er her konflikten ligger, fordi e2e-designprinsippene handler om at slik utvikling skal skje fra endepunktene. Med denne oppbygningen har e2e-nettverk blitt hyllet som demokratisk og at dens form produserer brukerfrihet for alle som tar den i bruk (Sandvig 2006). En slik påstand kommer av at e2e-designen gjør det mer vanskelig for uønskede tredjeparter å kontrollere kommunikasjonen på nettverket. Med dette kan følgende hypotese utledes:

Internett er fritt for alle, e2e-arkitekturen gjør at tredjeparter ikke kan avskjære kommunikasjonen mellom endepunktene, og verner om integriteten i nettverket.

En slik hypotese trenger et bredere innsyn i utviklingen vi går mot i dag og videre framover. Internett har forandret seg fra den første kommunikasjonen som ble foretatt i 1969 til vår moderne bruk som inkluderer en mengde mer funksjonalitet.

3.2.3 Framtidens ende-til-ende

To forskjellige tilnærminger vil bli presentert videre. Først vil godene ved en e2e-arkitektur bli nevnt og hva som risikeres å gå tapt ved ikke å ta hensyn til denne. Deretter presenteres en annen synsvinkel som ikke ser det samme behovet for å følge e2e-prinsippene, men som heller ønsker å forbedre eller utvikle e2e for å etterkomme dagens nye krav til applikasjoner.

3.2.3.1 Beholde ende-til-ende

Et synspunkt er at de forventede godene ved å gjøre forbedringer i kjernen av nettverket bør bli vektet mot tapet av å gå vekk fra e2e-arkitekturen. Det å introdusere løsninger som implementeres i kjernen av nettverket vil føre til at noe annet må ofres, som de *framtidige fordelene* ved å ha en e2e-arkitektur. Positive sider ved e2e-designen til Internett inkluderer skalering, utvidelse av forbindelser til lave kostnader og at det er lett å utvikle og anvende nye applikasjoner, noe som igjen stimulerer nyskapninger. Der det ikke er mulig å plassere teknologiske løsninger ved endepunktene går det an å bruke mer ressurser på å utvikle effektive politiske og lovlige institusjoner for å regulere oppførselen til Internett-brukere. Å anta at den mest effektive veien til å forbedre Internett-ytelse er ved å støtte seg på hva som kan vise seg å være midlertidige ”fixer” kan ødelegge for alle de andre sosiale og økonomiske fordelene som e2e-arkitekturen bringer med seg (David 2001).

Det kan bli gjort uomstøtelige skader på Internetts e2e-arkitektur ved at det blir en liberal aksept av alle teknologiske løsninger så lenge de ser ut til å virke fint der og da. Det er (minst) to generiske tekniske spørsmål som bør stilles i denne sammenhengen. Den første er om behovet for en teknisk ”fix” reflekterer en betingelse som ellers ville fortsatt å eksistere på Internett, eller om den trolig ville blitt forbigående. Den andre er om den foreslåtte tekniske løsningen vil fortsette å holde seg over tid istedenfor å gi en midlertidig hjelp (David 2001). Det er fortsatt et valg å lete etter andre alternativer og institusjonsmekanismer for å styre oppførsel på Internett, istedenfor å la det gå utover en teknologi som har mange fordeler.

Kombinasjonen av kommersielle aktører som ønsker å skape profitt, og brukere som stiller økende krav til Internettapplikasjoner, fortsetter å utfordre e2e-prinsippene. Det er blitt en økende etterspørsel etter bedre overføringer av lyd og video. Konkurranse mellom forskjellige ISP’er utfolder seg i nye tjenester de tilbyr kundene sine. Sist men ikke minst har filtrering blitt tatt i bruk for å blokkere uønsket eller ulovlig trafikk, eller å foreta trafikkanalyser for å tyvlytte på mistenkelig trafikk. Dette er fordi det har blitt en økning av tredjeparters involvering i kommunikasjon (Clark and Blumenthal 2000). Casestudiene i kapittel seks vil gi flere eksempler på slik bruk av filtrering.

3.2.3.2 Videre utvikling av ende-til-ende

Det er motstridende synspunkter om en utvikling som nevnt ovenfor vil eller ikke vil ødelegge e2e-arkitekturen. Det ”tekniske argumentet” sier at e2e dytter intelligensen til grensene av nettverket og skaper *applikasjonsinsensitive* nettverk. Slike nettverk gir byggeblokker som mange andre typer av bruk kan benytte seg av og på samme tid et miljø hvor det trengs få mellompunkter. Dette lavnivået er mer som en form for tjeneste blant mange andre muligheter. En påstand er at Internett er applikasjonsinsensitiv bare så lenge applikasjonen det er snakk om ligner hva det ble sett for seg av de første designerne av

TCP/IP. E2e-argumentet er en måte å stoppe de nye mellompunktene ved å argumentere for at de er *tekniske ukorrekte*. Dette gjøres ved at den som er flinkest til å følge defineringen av e2e historisk sett og stiller spørsmålet ”er dette e2e anno 1969 eller ikke?” vil være den som får kontrollen til å definere framtiden. En slik fremstilling kan undergrave nyvinnende teknologier, fordi de ikke har den samme filosofiske oppbygningen som fra 1960-årene (Sandvig 2006).

I den retningen Internetts utvikling går mener noen at e2e-arkitekturen er historie, og at vi er i ferd med å finne tilbake til et komplekst og dyrere nettverk. Det vil si at e2e vil fortsette å eksistere, men ikke lenger som en modell som bare bruker TCP som universell adapter mellom applikasjonene og nettverkene. Isteden utvikler dagens applikasjoner seg til å håndtere mer kompleks nettverksoppførsel (Huston 2008).

Den pågående debatten om tekniske og politiske vinklinger til e2e er ifølge Sandvig (2006) misvisende fordi de skjuler argumentene som er viktig. Det er ikke e2e designen som innehar fordeler, men alle egenskapene som blir assosiert med modellen som innehar disse kvalitetene. Det vil si *fleksibilitet, gjennomsiktighet* og *åpenhet* som legger til rette for at flere får deltatt i designen. Debatten om e2e tar fokuset vekk fra slike perspektiver og vinkler det isteden inn på tradisjonelle tankemåter som ikke lenger stemmer med hvordan Internett har utviklet seg. Disse egenskapene burde isteden være mål hver for seg og ikke sett under én felles teknisk korrekthet fra e2e-argumentasjonen.

Applikasjonene som alt befinner seg i nettverket i dag er en form for ”mellomvare” og har blitt en integrert del av nettverksdesignen. Plutselig er det ikke sikkert at en IP-sesjon åpnes med det endepunktet det spør etter. Det kan like gjerne være en avskjærende proxy-agent i nettverket som later som er det motstående punktet. Det later til at Internett har utviklet seg til å bli et mellomvaresystem heller enn et sammenhengende og enkelt e2e-system. Denne utviklingen er med på å utvide e2e fra å være en enkel, toveis forbindelse til en komplisert, multidel prosess (Huston 2008).

Mens denne ”e2e-kampen” foregår har noen av applikasjonene i nettverkskjernen tatt på seg ansvaret for å vedlikeholde en sikker overføring og kommunikasjon mellom partene. For eksempel sies https-protokollen å være den eneste gjenværende protokollen som klarer å gå rundt brannmurer, filtre og NAT’s. Det fins mange måter å sikre nettverket på, og flere av disse vil bli gjennomgått i kapittel fem.

En kan spørre hva som er drivkraften bak denne fortsatte økningen av applikasjoner i nettverkskjernen. Er det et ordentlig behov for en slik utvikling som nå skjer med ende-til-ende arkitekturen, eller er det en teknologistyrt determinant tilstede?

3.3 Teknologisk determinisme

Teknologisk determinisme er teorien om at teknologi er en autonom kraft som endrer samfunnet, til forskjell fra sosial determinisme hvor samfunnet er kraften som endrer teknologien. Det er en teknologisk ledet teori om sosiale endringer som ser på teknologi som hovedgrunnen til endringene som har skjedd opp gjennom historien. Denne teorien kalles en teknologi-dytt (*technology-push)* teori framfor en *demand-pull* teori, og innebærer at det er teknologien som kommer først og ikke etterspørselen som krever teknologien (Chandler 2002). Teknologisk determinisme er en form for reduksjonisme framfor holisme. Med dette menes det at teorien reduserer et stort fenomen til et enklere fenomen av en annen klasse. Målet er å få en enkel årsak-effekt form etter et mono-kausalt prinsipp som enklest kan forklares som en biljardkule-modell av endringer.

Ved å se på Internett i et holistisk perspektiv blir det overveldende og vanskelig å bearbeide informasjonsmengden, og langt verre å se de mindre variasjone som eksisterer i praksis, kultur og norm. For å skjønne dynamikken bak variasjonene må de heller beskrives på det dypeste nivå i II design (Star 1999). Både teknologisk determinisme og II-teori betyr at den komplekse helheten må reduseres til flere mindre biter som kan jobbe mot hverandre.

Teknologiske determinister tolker teknologi generelt, og kommunikasjonsteknologi spesielt, som basisen for samfunnet vårt. Ifølge en slik filosofi vil Internett være en innflytelsesrik faktor ved endringer i samfunnet. Teknologisk determinisme på dets mest ekstreme form betrakter hele samfunnet som bestemt av teknologi. Sagt med andre ord: at teknologien former alle sosiale og kulturelle fenomener. Dette er imidlertid bare en av to varianter av teknologisk determinisme. Den andre varianten sier at den teknologiske drivkraften er bare en av mange drivkrefter og dermed ikke en absolutt bestemmende faktor.

Opphavet til Moores lov er et argument for at det er teknologisk determinisme på gang. Moores lov sier at antallet transistorer som kan plasseres på integrerte kretser dobles for hvert andre år. Selv om denne loven er basert på en empirisk observasjon, har den vist seg å stemme fra det ble registert tall for dette i 1965 og fram til i dag. En slutning som kan trekkes er at: datakraft fortsetter å øke fordi den ganske enkelt er i stand til det. Vi som forbrukere kan protestere mot det å benytte oss av bestemte produkter, men vi kan ikke protestere mot at det uten noen god grunn skjer en fordobling av chip-kapasitet hver 24. måned (Ceruzzi 2005).

Sett fra et teknologisk deterministisk synspunkt er alle mennesker styrt av teknologien. Det kan tenkes flere argumenter for å støtte påstander om hvor viktig teknologi har blitt for mennesker i verden i dag, ta for eksempel hvor avhengige mange av oss har blitt av mobiltelefonen. Dette er bare en i rekken av nyvinninger vi har adoptert uten å stille mange spørsmål. De svarene vi eventuelt får vil være påvirket av hva produsenter og selgere velger å

fortelle kundene sine. Hvordan kan vi opprettholde teorier om sosial forming av teknologien når vår daglige interaksjon med teknologi er drevet til en slik grad av *technology-push* fra ingeniører (Ceruzzi 2005)? Dette kan utledes i følgende hypotese:

Filtreringsapplikasjonene fortsetter å utvikle seg fordi de kan, ikke fordi de må på grunn av etterspørsel. Teknologien/ingeniørene styrer brukerne og ikke motsatt.

Hvis filtreringsapplikasjonene som implementeres i nettverkskjernen egentlig er en unødvendighet, fører det til den allerede nevnte overflødigheten i form av redundans. Dette kan videre gi en "falsk etterspørsel" som tilsynelatende rettferdigjør applikasjonenes bruksområder. I et slikt scenario vil ingeniørene videreutvikle filtreringsteknikkene bare fordi det er mulig å gjøre forbedringer, ikke fordi brukerne har bedt om det, og dermed oppnå en kontroll over brukerne.

3.4 Oppsummering

Siden infrastrukturer utvikler seg over lang tid vil mange av behovene være ukjente i selve designprosessen. Et resultat av de teknologiske fremskrittene som gir stadig bedre båndbredde, rekkevidde og oppkoblingsmuligheter til Internett bidrar til å gjøre nettverket mer komplekst og sammensatt. I denne oppgaven er spesielt egenskapene og utfordringene ved II'er som fleksibilitet og generativitet, kompleksitet og e2e-prinsippene i sentrum. Disse fører til sammen til et mer generelt spørsmål om hvem som styrer denne utviklingen, teknologien selv eller brukerne.

Det ble understreket hvor viktig generativiteten er for å ivareta fleksibiliteten til Internett og at ende-til-ende arkitekturen er sterkt koblet til disse to midlene. Alle applikasjonene som implementeres i nettverkskjernen bryter med semantikken til Internettprotokollen og er en direkte motsigelse av e2e-arkitekturen til Internett. Likevel er det de som hevder dette er en nødvendig utvikling av applikasjoner og at e2e-arkitekturen må tilpasse seg en ny tid. Dette kapittelet har introduserte flere nyttige begreper som generativitet, fleksibilitet, ende-til-ende prinsipper og teknologisk determinisme som vil bli brukt i analyse- og diskusjonskapittelet.

"Scientific progress consists largely in the elimination of contradictions wherever we find them."
Karl Popper

4 Forskningsmetoder

Da jeg først ble introdusert for temaet som skulle studeres, filtrering på Internett, var det ikke gjort noen klare avgrensninger. Første fase ble veldig omfattende med innsamling av relevant teori og dokumentasjon for feltet. Siden oppgaven bygger på Internett ble det naturlig å bruke det som hovedkilde for innsamling av informasjon. Den ivrige starten på datainnsamlingsprosessen gjorde at jeg måtte ta et skritt tilbake og tenke på hvilket fokus, tilnærming og metoder jeg ville bruke for å unngå en mengde overflødig data. I dette kapittelet viser jeg hvilke fremgangsmåter jeg valgte for å få struktur på studiene i form av metoder, utvelgelse og analyse av datasettet.

4.1 Valg av metode

Det er to hovedformer for forskningsmetoder, *kvalitativ* og *kvantitativ* metode. Kvalitativ forskning er utviklet med tanke på samfunnsvitenskapen til forskjell fra kvantitativ forskning som var ment for å studere naturfenomener i naturvitenskapen. Kvalitativ forskning er designet for å hjelpe oss å forstå hva slags samfunns- og kulturkontekst vi lever i. Hva som skiller kvalitative metoder fra kvantitative er blant annet hvordan data blir samlet inn. Det er ikke alltid lett å skille mellom datainnsamling og dataanalyse når det blir mer subjektive tolkninger under kvalitativ forskning, mens kvantitativ klarer å skille mye klarere mellom disse to prosessene. Kvalitativ forskning gir ofte bedre rom for forskerens egen vinkling, og dette påvirker hvordan dataene samles inn (Silverman 2005).

Det brukes ofte kvalitative metoder for å finne ut av menneskers livshistorier eller hverdagshendelser. I dette tilfellet vil kvalitative metoder brukes for å finne ut mer om interaksjonene først og fremst mellom Internett og filtrering, men en underliggende årsak inkluderer brukerne av denne tjenesten som har blitt en hverdagslig del av manges liv. Noen mener at kvalitative metoder kan gi en dypere forståelse av sosiale fenomener enn hva som er mulig med kvantitative metoder. Kvalitativ forskning prioriterer studier som oppfatninger, meninger og følelser, en følelsesmessig modell. Det er også andre modeller for kvalitativ forskning, motstykket til den følelsesmessige er samspill framfor meninger og hva folk gjør uten noen spesiell referanse til hva de måtte føle eller tenke. Dette gir den konstruktive

modellen som vil være sentral for denne oppgaven, men ikke helt uten noen følelsesmessige innspill fra den førstnevnte modellen.

Kvalitative studier kan være deduktive eller induktive, det vil si teste eller bygge teorier og hypoteser. Denne oppgaven vil deduktivt teste noen eksisterende teorier og hypoteser nevnt i kapittel tre. Men mens oppgaven prøver å forstå filtrerings-fenomenet vil den også induktivt prøve å komme frem til og gi nye forklaringer og forståelse for oppgavens forskningsspørsmål.

Eksempler på kvalitative metoder er blant annet etnografi, action research, grounded theory og casestudier. Før jeg bestemte meg for valg av metode ville jeg først finne ut mer om det jeg forsket på, for deretter å velge en passende metode. Temaet for mine studier ville være dybdestudier innenfor fenomenet filtrering på Internett ved å se nærmere på tre områder innenfor dette temaet. Det naturlige valget av metode ble derfor casestudier.

Forskning er basert på tre alternative filosofiske perspektiver: positivistisk, fortolkende og kritisk (Myers and Avison 2002). En positivistisk holdning antar at forskningen er objektivt gitt og kan beskrives ved målbare egenskaper – uavhengig av observatøren og instrumentene som blir brukt. Generelt vil positiviske studier gå inn for å støtte den allerede antatte teorien for det gjeldende fenomenet. En kritisk holdning antar en samfunnskritisk retning. Her antas det at samfunnsvirkeligheten er historisk skapt og produsert eller reprodusert av folket som lever i samfunnet. Fokuset er på motsetninger, konflikter og motsigelser i samfunnet. Ved å identifisere ”problemene” er målet at det skal bli lettere å eliminere dem. Jeg har valgt det siste perspektivet for denne oppgaven, altså en fortolkende holdning. Den sier at tilgang til virkeligheten gis gjennom samfunns-konstruksjoner som språk, bevissthet eller delte meninger. Med dette er målet å få en forståelse av samspillet mellom Internett og filtrering, og hvordan disse påvirker hverandre.

4.2 Casestudier

Den mest brukte kvalitative metoden i informasjonssystemforskning er casestudier, som har blitt definert av Yin (1994) som følgende:

En empirisk granskning som undersøker et moderne/samtidig fenomen innenfor dets virkelige kontekst spesielt når grensene mellom fenomenet og konteksten ikke er åpenlyst klare.

Noen av vanskelighetene med å studere infrastrukturer er hvordan en skal gå fra tradisjonelle etnografiske områder og over i et virtuelt miljø. En spesiell utfordring blir hvordan man håndterer store kvantum med data, for eksempel en mengde nettsider, og hvordan forstå samspillet mellom online og offline oppførsel fra brukernes side. Ved å følge noen

retningslinjer som kommer fra andres erfaringer kan disse utfordringene imøtekommes. Viktige punkter er å studere designen til infrastrukturen og forstå paradoksene til infrastrukturen som både transparent og ugjennomsiktelig. Dette inkluderer alle "mindre" deler ned til de minste komponentene som ledninger, kabler og innstillinger. Poenget er å ikke miste noen viktige aspekter ved å overse de "usynlige" delene av II'en, og fokusere på hva indikatorene for studien forteller oss (Star 1999).

Det har kommet flere gode studier om II'er i de siste årene, blant annet om forskjellige Internettsamfunn som Multiuser Dungeons (MUDs) eller virtuelle rollespill. Slike studier er viktig fordi de tøyer vår forståelse av identitet, status og samfunn (Star 1999). Her følger en definisjon av Internett feltarbeid slik Hannemyr forklarer det[16]:

Internett feltarbeid er forskning innenfor sosiale, kulturelle, politiske, økonomiske, etiske, tekniske og aestetiske aspekter ved Internett som inkluderer observasjon av hendelser på Internett eller akkumulerte kvalitative eller kvantitative data fra online miljøer (som e-post, nettsider, diskusjonsgrupper, virtuelle samfunn og/eller arkiver) på Internett for undersøkelse og analyse.

Det vil si at Internettforskning i sammenheng med casestudier blir feltarbeid hvor "felten" er Internett. Eksempler på Internett feltarbeid inkluderer analysering av konversasjoner på chattekanaler, etnografisk forskning i virtuelle samfunn, bruk av roboter til å samle inn og analysere online data på en kvantitativ måte, og de to som er mest sentrale for denne oppgaven: analysering av online arkiver og Internettsider som mediauttrykk (Hannemyr 2006).

Stake har identifisert tre former for casestudier (Silverman 2005, s.127). Vi har *den indre casestudien* som består av én case hvor det ikke gjøres forsøk på å bygge teorier eller gjøre generaliseringer utenfor casen. Den neste er *den instrumentale casestudien* hvor casen er et instrument for å finne ut av et annet hovedtema enn hva selve casen går i dybden av. Til slutt er det den jeg har valgt; *den samlede casestudien,* som er et studium av flere caser for å undersøke et felles fenomen. Ved å velge denne formen for casestudie ønsker jeg å oppnå en bred empirisk database som kan deles inn i tre hovedkategorier.

Den første kategorien består av data som vil kunne gi et allment perspektiv om praktisering av filtreringsteknikker gjort av privatpersoner, selskaper og kommersielle firmaer. Den andre kategorien vil gå mer i dybden av spesielle prosjekter som overvåker

[16] Hentet fra en gjesteforelesning i faget inf5220 på UiO som Gisle Hannemyr holdt høsten 2006. Han brukte kilde fra blant annet Steven G. Jones: Doing Internet Research. Critical Issues and Methods for Examining the Net (1999).

samfunnet på vegne av myndigheter. Den siste kategorien vil ta for seg land som presenterer hver sine perspektiver for hvordan håndtere sensur og filtreringspolitikk på Internett. Datasettene for disse hovedkategoriene vil gjennomgå en kvalitativ innholdsanalyse og bli testet mot forskningsspørsmålet. Ved å sammenligne resultatene av analysen fra de tre kategoriene håper jeg at denne studien vil være med på å heve kunnskapsnivået om hvordan filtrering og Internett innvirker på hverandre, og i hvilken retning de vil bevege seg fremover.

4.3 Datainnsamling

Jeg har brukt Internett som ressursportal til å søke etter skrevne dokumenter (via online databaser og biblioteker) som bøker, artikler eller manuskripter. Ved siden av dette har jeg funnet informasjon fra fysiske biblioteker, nettsider, blogger, chatteforum, e-poster og gode tips fra medstudenter og veileder.

I min innsamlingsprosess har jeg tenkt på utsagnet *tekst er aldri bare tekst, det er også kontekst*, og at det må tas hensyn til hele innholdet for ikke å mistolke meningen bak en enkelt ytring. Dette gjelder spesielt ved aksessering av "tilfeldige" nettsider, blogger og chatteforum.

De empiriske dataene har blitt samlet inn i tidsrommet februar 2007 til og med juni 2008. Hovedvekten av dataene som er blitt brukt ble samlet inn høsten 2007 og på nyåret 2008. Det er blitt brukt kilder fra forskjellige årstall, siden målet har vært å få samlet inn mest mulig om temaet i seg selv for å få et helhetlig syn på utviklingen av fenomenet, istedenfor å bare bruke kilder av nyere dato.

I datainnsamlingsprosessen bestemte jeg meg for å bruke formålsstyrt utvelgelse, framfor en statistisk tilnærmelse. Det vil si at datasettene i de tre casene er nøye plukket ut basert på at jeg ville finne ut hvordan filtreringsmetoder brukes i praksis fra privatpersoner, kommersielle aktører til myndigheter i forskjellige land. Dette dekket et stort felt hvor jeg var nødt til å avgrense temaet ved å være kritisk i min utvelgelse av representative data fra disse gruppene. Et problem ved slik utvelgelse av data er problemet med all den irrelevante informasjonen som fins på Internett og det å vite kilden bak informasjonen. Men basert på tre klare ideer om hva jeg ville ha som hovedtema for casene ble det enklere å gjøre konkrete søk.

4.3.1 Kildekritikk

Ved forskning må en ta hensyn til data som for eksempel kan være beskyttet under personvernloven. I denne oppgaven er det bare blitt brukt offentlige data som er tilgjengelig for alle å se. Dette gjorde det lettere med tanke på hensyn til etiske dilemmaer i forskningen. Slike dilemmaer gjelder for eksempel bruk av anonymiserte kilder og navn på personer som

er med i medisinsk forskning eller forskning i forbindelse med institusjoner. Den positive effekten av ikke å ha slike sensitive datasett er at alle kildene jeg har brukt for å kunne gjøre mine tolkninger dermed står fritt for andre å bedømme. Kildehenvisningene er blitt dokumentert i oppgaven og er vedlagt i referanselisten. Mesteparten kan lokaliseres på nett, bortsett fra noen av bøkene som ikke finnes som gratis nedlastingsversjoner. Disse kan skaffes via online nettbutikker eller i et bibliotek.

Hvorvidt det er bra å bruke Internett som hovedkilde er et aspekt som må vurderes. Viktige faktorer er autentikasjon, nøyaktighet, meninger, i hvilken sammenheng nettsider er satt opp, og det faktum at Internett i praksis gir alle individer mulighet for å publisere så godt som hva enn de måtte ønske. Dette er en problemstilling som ikke blir relevant for de kildene som er basert på publiserte artikler, som inneholder forfatternes fulle navn og institusjonstilhørighet. En god del av kildene er også hentet fra nyhetssider som offentliggjør journalistene, og flere av disse nyhetslenkene er blitt dobbelt- (og trippelt) sjekket ved å søke dem opp på andre nyhetsmedier på Internett for å se om perspektivene journalistene har valgt å vektlegge samsvarer med hverandre.

En av kildene som er blitt brukt er nettstedet til OpenNet Initiative (ONI), som har sin egen agenda å formidle, men som likevel går inn for å presentere funn på en mest mulig objektiv måte, og som også er tilknyttet forskningsmiljøet til fire universiteter[17]. Siden alle nettsider kan sies å forme innholdet etter hva som er deres budskap har jeg gått inn for å finne de sidene som har blitt anerkjent av tredjeparter.

Likevel har jeg flere kilder fra Internett-sider som ikke like lett kan spores tilbake til opphavspersonene. Disse kildene har jeg også brukt mer skeptisk enn de andre kildene ved å la det komme klart fram i oppgaven når det er snakk om folks meninger og ytringer. I sin kontekst var det passende å ta med også noen slike kilder, spesielt med tanke på at bloggevirksomhet på Internett har blitt et sterkt ytringsmiddel for folk som for eksempel lever i regimer hvor myndighetene utøver sterk sensur og filtrering av massemedia. I slike situasjoner kan blogging og personlige nettsider være en måte å formidle usensurerte nyheter på - uten at det vil føre til bøter eller fengselsstraffer.

4.4 Valide og konsistente målinger

Kvalitative studier kan i sammenligning med kvantitative studier sies å være en mer subjektiv form for forskning. Dette har ført til en del kritikk mot denne forskningsmetoden, og at det er

[17] Forskningen til ONI gjøres i samarbed med de fire akademiske institusjonene the University of Toronto, Berkman Center for Internet & Society at Harvard Law School, the University of Cambridge og the Oxford University.

vanskeligere å kunne måle validitet og presentere en overbevisende utledning av resultatene. For å oppnå validitet må forskeren ha en kritisk holdning til sine egne studier, og det er noen punkter som kan brukes for å nå fram til mest mulig valide funn (Silverman 2005):

Først kan en se om det er mulig å finne et motbevis. Om dette går er ikke konklusjonen riktig. Alternativt kan man unngå å hoppe til konklusjoner før det er blitt gjort en nøye gjennomgang av mulighetene som finnes. Neste punkt er å sammenligne med andre caser ved å undersøke alle detaljer og datafragmenter og se at det er konsistens her. Tredje punkt går på at all (relevant) data skal innarbeides i analysen. Det vil ikke være en gyldig konklusjon før generaliseringene holder for absolutt alle deler av dataene som er blitt samlet inn. Etter dette må de avvikende casene lokaliseres for å kunne danne en liste over regler for alle dataene i analysen. Det er aldri noen deler av dataene som er avvikende i seg selv, men de blir det når de sees i sammenheng med tilnærmelsen som brukes. Desto høyere validitet eller gyldighet det blir, desto nærmere kommer en det sosiale fenomenet som hendelsen refererer til.

Fortolkende metoder i kvalitativ forskning sikter mot å kunne gi en forståelse av konteksten til infrastrukturen som undersøkes, og prosessen som infrastrukturen er en del av både som den påvirkende part, og som den som blir påvirket (Klein and Myers 1999). Det er tre punkter fra prinsippene til Klein og Myers fortolkende feltarbeid som er relevante for mine studier.

Den første går på det fundamentale prinsippet om *den hermeneutiske sirkelen*. Den foreslår at all menneskelig forståelse oppnås ved å gå frem og tilbake mellom delene og den større helheten delene tilhører. I denne oppgaven vil det si å se på fenomenet bak interaksjonen mellom filtreringsapplikasjoner og brukere på Internett. Det andre prinsippet handler om *kontekstualisering*, altså å presentere en kritisk refleksjon av den sosiale og historiske bakgrunnen for forskningsfeltet. Dette vil gi andre muligheten for å se hvordan utviklingen av fenomenet har foregått. På denne måten vil lesere også få mer ut av oppgaven. Jeg har gått inn for å gi bakgrunnsmateriale der det har vært hensiktsmessig, både for Internett, filtrering og sensur. Det tredje prinsippet går på *abstraksjon og generalisering*. Ved å bruke teori på å tolke datasettene fra casestudiene kan det gjøres generaliseringer. Her vil jeg nevne Walsham (2002) som gir tre andre måter å gjøre generaliseringer på for fortolkende casestudier, og en fjerde som støtter Klein og Myers sistnevnte prinsipp med litt andre ord.

Den første generaliseringen til Walsham er å utvikle konsepter, den andre er å gjøre generaliseringer av teori, den tredje er å skissere opp bestemte implikasjoner og til slutt den som jeg ser mest relevant for denne oppgaven: *oppnå en rik innsikt* i fenomenet det forskes på.

Det er noen faremomenter ved forskere som prøver å innta en objektiv holdning. Først og fremst er mennesker subjektive av natur. Kuhns vitenskapsfilosofi[18] om hvor vanskelig det er å få gjennomslag for noe nytt i vitenskapen generelt er verdt å nevne. Et av hovedpoengene hans er at vi skaper forventninger til hva vi oppfatter slik at vi dermed farger synet på hva vi erfarer. Selv når det er tydelige avvik tilstede vil forventningene våre bli justert til å passe dem (Kuhn 1962, k.4). Slike hindringer vil alltid være tilstede, men ved å være oppmerksom på dem, ved å gi en synlig gjennomgang av forskningsprosedyrene og ved å sammenligne med andres studier, skal det være mulig å kunne verifisere hvor valid og konsistent studien er på en tilnærmet objektiv måte.

4.5 Oppsummering

Denne oppgaven er en fortolkende kvalitativ casestudie som prøver å forstå filtreringsfenomenet som virker på den globale infrastrukturen Internett. Internettforskning i sammenheng med casestudier betyr at felten er Internett, og her har valget falt på to måter å gjennomføre dette på: ved å analysere online arkiver og ved å se på Internettsider som mediauttrykk. Selve datainnsamlingsprosedyren krevde en kritisk tilnærming siden hovedkilden var Internett. Problemer med dette er at det fins veldig mye (uvesentlig) informasjon på Internett, i tillegg til at det kan være vanskelig å bestemme hvem som har lagt ut informasjonen og i hvilken hensikt dette ble gjort. Løsningen falt på å bruke en formålsstyrt utvelgelse og en kvalitativ innholdsanalyse for å oppnå en database som gjør det mulig å komme fram til generaliseringer for temaet. Ved å se nærmere på filtreringsfenomenet på Internett, gå i dybden i datasettene som blir presentert i casestudiene for deretter teste mot teoriene presentert i kapittel tre, er målet at analyse og diskusjonskapittelet skal føre til en dypere og rikere innsikt ved bruk av metodene nevnt i dette kapittelet. Oppgaven vil deduktivt teste teorien fra kapittel fire samtidig som den induktivt vil prøve å komme frem til og gi nye forklaringer og forståelse for forskningsspørsmålet. Ved å gå inn for å oppnå høyest mulig validitet vil også filtrerings-fenomenet bli nærmere studert.

Det dukker opp noen begrensninger i en casestudie som denne som inkluderer andre verdisett enn ens egne, slik at det alltid vil finnes påvirkninger fra egen kultur, tradisjoner og måter å tenke på som kan skape barrierer for å se ”den store sammenhengen”. Personlige synspunkter fra egen bakgrunn vil på noen måter ha blitt reflektert i teksten, til tross for forsøk på det motsatte.

[18] Thomas S. Kuhn (1922-1996) har blant annet gitt ut ”Vitenskapelige Revolusjoners Struktur” som omhandler paradigmeskifter og filosofiske vitenskapelige spørsmål mennesker står ovenfor.

”The basic approach to networking architecture in terms of the Internet can be informally described as ‘every packet is an adventure!’”
Geoff Huston

5 Filtreringsmetoder

I dette kapittelet vil det bli gjennomgått hva som konkret legges i filtrering og filtreringsmetoder for denne oppgaven. Det fins både tekniske og ikke-tekniske varianter av filtrering, og begge kan brukes alene eller i kombinasjon med hver sine undergrupper. Selv om det er mange varianter av filtreringsmetoder baserer de fleste seg på de samme grunnteknikkene. De vil bli gjennomgått her, mens i casene som følger vil det bli presentert *bruksområder* for de forskjellige filtreringsmetodene. Grupperingene filtreringsmetoder kan deles opp i er som følgende (ONI 2008):

1. Teknisk filtrering som inkluderer:
    a. DNS-manipulering
    b. Proxy-basert filtrering
    c. IP-blokkering
2. Sosial filtrering som inkluderer:
    a. Tvang (utført mot for eksempel ISP’er) som fører til take-downs
    b. Påført selvsensurering

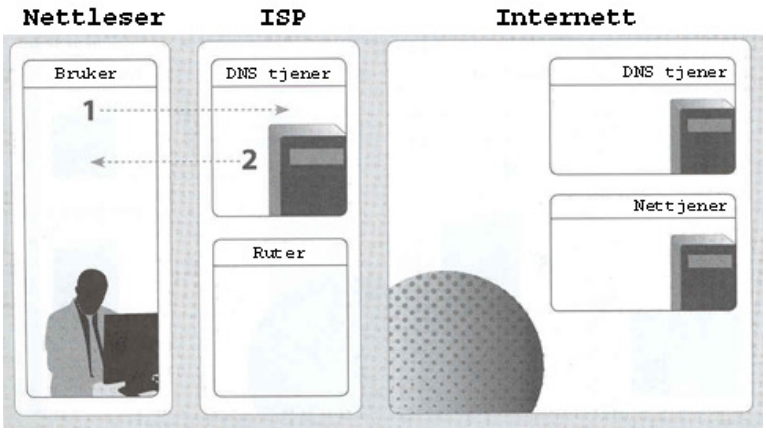
5.1 Teknisk filtrering

Teknisk filtrering er den mest brukte teknikken for å kontrollere innhold på Internett. Metoden baserer seg på de tekniske spesifikasjonene nevnt i kapittel 2 med rutere (noder) som sender pakker videre til andre rutere i en distribuert topologi. Når en forbindelse opprettes fra en datamaskin til nettverket er det flere måter for å avskjære eller påvirke forbindelsen, slik at det blir utført en form for sensur eller blokkering. De neste avsnittene tar for seg de mest vanlige måtene teknisk filtrering kan foregå på.

5.1.1 DNS-manipulering

Domene Navn Systemet, DNS, er ”telefonboken” for Internett. DNS oversetter vertsnavn[19] til IP-adresser som er nødvendige for nettverk som sender og mottar informasjon. IP-adressen, som er et nummer mellom null og fire billioner, er lite brukervennlig for mennesker. DNS ble derfor oppfunnet for å oversette numrene til navn vi klarer å huske. Dette har blitt en stor suksess, og de fleste kommunikasjoner via Internett bruker domenenavnene heller enn IP-adresser, spesielt ved bruk av www.

DNS-manipulering foregår ved at DNS-tjeneren får en liste med adresser som skal blokkeres. Figuren under viser hvordan all trafikk fra brukeren går via DNS-tjeneren. Hvis brukeren har bedt om en IP-adresse for et av domenenavnene på sortelisten kan DNS-tjeneren sende en feilmelding tilbake til brukeren, eller den kan sende brukeren til en annen nettside isteden. Dette kan for eksempel skje hvis en arbeidsplass ikke ønsker at sine ansatte går inn på bestemte nettsider som *youtube.com* eller *poker.com*, og har satt disse adressene til heller å peke til et mer relevant oppslagsverk, for eksempel *wikipedia.org*. Moralen her er at hvis domeneoppslaget kan filtreres kan også adgang til ulovlige eller uønskede sider bli blokkert på en effektiv måte (Deibert, Palfrey et al. 2008).



Figur 4: DNS-manipulering

5.1.2 Proxy-basert filtrering

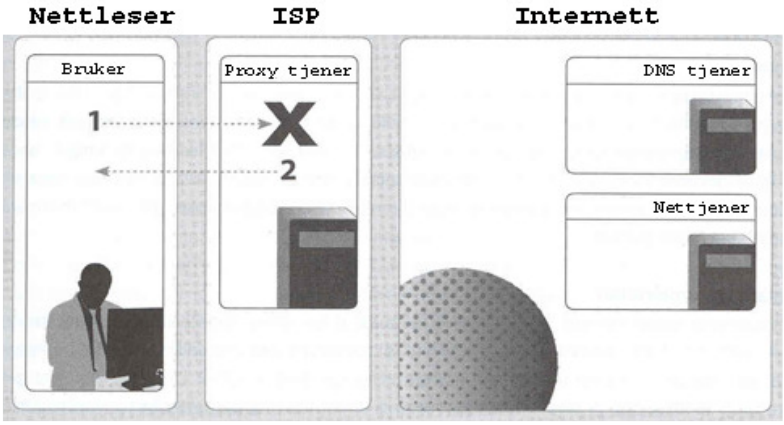
Et normalt oppslag til en nettside på www skjer først ved en DNS-lookup slik at brukeren får forbindelse til ISP’ens DNS-maskin som oversetter domenenavn til IP-adresser. Deretter starter kommunikasjonen mellom nettstedets DNS-tjener for å finne IP-adressen til det

[19] ”Vertsnavn” brukes her som en fellesbetegnelse for alle navnerepresentasjoner av en ressurs på Internett, for eksempel domenenavn, nodenavn og maskinnavn.

forespurte domenenavnet. Når IP-adressen er funnet opprettes kommunikasjonen mellom nettjeneren og den ønskede nettsiden.

En alternativ måte å konfigurere nettverket på er å ikke la brukere få direkte tilgang til www, men heller la dem gå via en proxytjener. I tillegg til viderekoblingsforespørsler kan proxytjeneren midlertidig lagre nettsiden i en cache. En effekt av slik cachebruk er at nettsiden vil vises raskere for alle brukere unntatt den første som ba om den, og ISP'en trenger ikke å kaste bort båndbredde på flere like forespørsler.

Et proxy-oppsett legger også til rette for at nettsteder kan blokkeres. Siden alle forespørsler går via proxy'en kan den bestemme hvilke oppslag som skal godkjennes. Godkjente forespørsler sendes videre til nettjeneren som inneholder de bestemte sidene. En bruker som utsettes for proxy-filtrering kan for eksempel oppleve at all trafikk mot 129.240.*.* (UiO nettet) er blokkert. En proxy legger imidlertid også til rette for mer avanserte former for blokkering, fordi den har tilgang til hele innholdet av forespørselen. Dette betyr at en proxy kan blokkere enkelte nettsider og ikke bare hele domener eller nettjenere. Slike mindre blokkeringer kan være vanskeligere å oppdage og kan få brukeren til å tro det er en teknisk feil, som er en årsak til at proxy-filtreringer er en effektiv måte å "justere" innhold på Internett (Deibert, Palfrey et al. 2008).

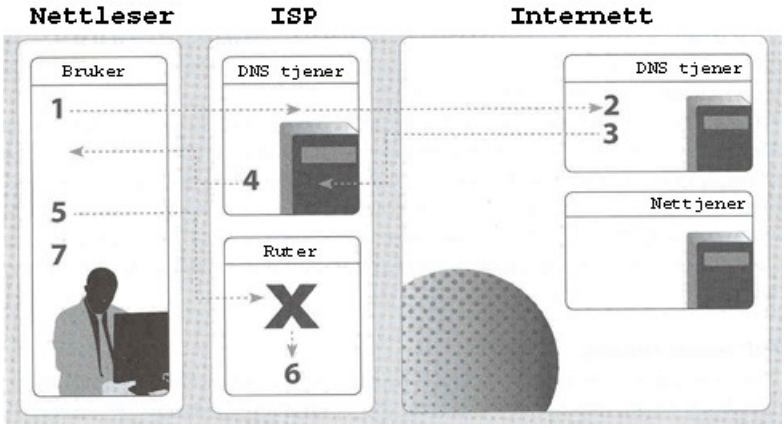


Figur 5: Proxy-blokkering

5.1.3 IP-blokkering

IP-blokkering vil si blokkering av tilgang til bestemte tjenere som er koblet til Internett. En IP-pakke begynner med et adressehode som gir informasjon om destinasjonen for datapakken og hva slags port som skal brukes. Når ruterne inspiserer pakkeadressen kan de sjekke denne informasjonen mot for eksempel en sorteliste av nettsteder som skal blokkeres. Hvis IP-adressen står på sortelisten kan ruterne slippe all trafikk fra de datapakkene dette gjelder, som vist i figur 6. Slike blokkeringer av IP-adresser er meget effektivt, og siden vanlige

applikasjoner bruker karakteristiske portnumre kan "IP-blokkering" inkludere å filtrere på bestemte porter. Hvis for eksempel nettverksansvarlige på en arbeidsplass ikke vil at noen innenfor nettverket skal bruke www, kan de sette ruterne til å stenge all trafikk på port 80 som er den vanlige porten for HTTP.



Figur 6: IP-blokkering

Ulempen ved bruk av IP-blokkering er at det bare er IP-adressen som har blitt sjekket. Fordi flere domenenavn kan dele samme IP-adresse vil alle adressene bli blokkert selv om det som regel er meningen at det skal gjelde et bestemt domene. Et annet problem er at det ikke er lett å vedlikeholde en liste over IP-adresser med ulovlig innhold. Dessuten kan det være noen IP-adresser som er på grensa av hva som kan eller bør blokkeres, slik at det blir upassende å kutte all kommunikasjon til adressen (Deibert, Palfrey et al. 2008).

5.1.4 Muligheter for å omgå teknisk filtrering

Det er ingen generaliseringer for hvordan omgå *alle* typer filtrering. Ofte må det tas hensyn til hva slags filtrering som er blitt brukt i hvert tilfelle. Dette avsnittet gir eksempler på bestemte metoder for å omgå noen former for teknisk filtrering, for eksempel ved bruk av proxy, Virtual Private Network (VPN) eller Secure Shell (SSH). Alle disse metodene forutsetter at bruker har kjennskap og tilgang til en maskin "på utsiden".

Tunnelering er protokoller som bruker datakryptering for å overføre usikre datapakke-protokoller, for eksempel via VPN eller SSH. Det opprettes en sikker tunnel mellom to rutere eller to tjenere på Internett, hvor bare "endepunktene" har nøklene for å kryptere og dekryptere datapakkene som sendes og mottas.

Secure Socket Layer (SSL) teknologi er en sikkerhetsprotokoll som bruker tunnelering eller "pipe". SSL bruker digitale sertifikater for å lage en sikker kommunikasjon mellom to maskiner og har blitt en de-facto standard for å sikre kommunikasjon og overføringer på Internett. SSL har blitt implementert i alle store nettlesere og nettjenere, og spiller dermed en

stor rolle i dagens e-handel på Internett. Data som overføres over en SSL-forbindelse kan ikke bli manipulert eller forfalsket uten at brukerne av maskinene på hver sin side vil bli klar over at noe foregår. Transport Layer Security (TLS) er en kryptert protokoll på samme måte som SSL. Det er noen små forskjeller mellom SSL og TLS, men de virker for det meste likt (Wikipedia 2008).

Andre måter å omgå filtrering på kan være alt fra å ringe en venn med Internett-tilgang, til å ta i bruk effektiv programvare som nmap[20]. Det avhenger av situasjonen og hva slags filtrering som skal omgås. Løsninger kan være å bruke eller bytte til:

- et annet trådløst nettverk. En linux-laptop utstyrt med for eksempel et Atheros nettverkskort og programmet aircrack-ng[21] kan enkelt bryte seg inn i trådløse nettverk med Wired Equivalent Privacy (WEP) kryptering, og gitt litt mer tid også Wi-Fi Protected Access (WPA og WPA2) beskyttede nettverk. Ideen er at disse nettverkene ikke har de samme sperringer som det tidligere nettverket en befant seg på.
- en annen ISP: siden noen ISP'er er strengere enn andre kan det være en mulighet å bytte til en ISP som ikke har så strenge regler. Imidlertid forutsetter dette at det er tid til å vente på en ny leverandør.
- en annen DNS-tjener, hvis en DNS-tjener er satt til å blokkere domenenavn, og brukeren kan IP-adressen til en annen pålitelig DNS.
- mobiltelefon med modem-teknologi som GPRS eller 3G. Det finnes mange mobilnett, her i Norge er det blant annet Telenor, Tele2, Netcom, Vodafone, O2, T-mobile eller Tiscali. Hvis de ikke tilbyr Internett direkte kan for eksempel brukeren bli sin egen ISP ved å ringe til sin egen datamaskin som er satt opp med modem, hjemme eller på jobb. Denne løsningen krever en viss datakyndighet.
- Virtual Dedicated Server (VPS): ved bruk av VPS vil hver DNS-adresse bli digitalt signert slik at DNS-responsen kan valideres som gyldig. Dette avslører om det har foregått DNS-manipulering.
- kryptering: hvis data går igjennom for eksempel en proxy, vil kryptering medføre at all data som passerer blir uleselig, og forblir ufiltrert.
- bruk av programmer som ivaretar nettanonymitet, for eksempel ”Tor node” (Tor 2008)

[20] Nmap er et kraftig verktøy med flere funksjonaliteter. Det kan brukes til å finne svakheter i brannmurer og kartlegge om det brukes IP-filtre som eventuelt blokkerer Internett-tilgang, http://nmap.org, aksess 11.06.2008.

[21] Aircrack-ng er et crackeprogram for 802.11 WEP og WPA-PSK nøkler. Ved å avskjære en viss mengde datapakker klarer programmet å sette sammen gyldige nøkler som kan brukes til å få adgang til trådløse nettverk. Fra http://www.aircrack-ng.org/doku.php, aksess 11.06.2008.

Det er mange måter å bruke tekniske filtreringsmetoder på, men punktene over viser at det også er mange måter å omgå filtrering på. Newtons tredje lov sier; for en reaksjon fins det også en motreaksjon. Denne regelen kan altså til en viss grad også gjelde på Internett for filtreringsmetoder og hvordan omgå filtrering.

5.2 Sosial filtrering

Sosial filtrering har en spesiell plass i case 3 i denne oppgaven. Land som utfører streng Internett-politikk kan være i stand til å bruke sosial filtrering like effektivt som teknisk filtrering. Innbyggere i Norge vil antagelig ikke ta oppfordringer fra myndighetene på en utpreget alvorlig måte. Effekten kan derimot bli en annen når det finnes underliggende trusler, som fengselsstraff, bak enkle meldinger i form av for eksempel en SMS på mobiltelefonen. For eksempel ble det våren 2008 sendt ut SMS fra kinesiske myndigheter til alle brukere av mobiltelefon i Lhasa, Tibet, i forbindelse med at kinesiske myndigheter slo ned på demonstrasjoner i byen. Meldingene oppfordret brukere til å følge reglene og etterkomme loven (Kushner 2008). At slike meldinger også gikk til alle andre med mobiltelefon som befant seg i området, men som ikke var med på demonstrasjonene, viste seg å ikke være noe hinder for å ta i bruk hva noen vil definere som skremselstaktikk.

Sosial filtrering har kommet mer i fokus i senere tid på grunn av Internetts stadige vekst av både brukere og nettverk. Som USA's 42.president Bill Clinton sa i 1996: *"When I took office, only high energy physicists had ever heard of what is called the World Wide Web… Now even my cat has its own page."* Før kunne teknisk filtrering brukes på en effektiv måte, men nå har det kommet et langt større antall nettsteder i tillegg til at brukere har begynt å kommunisere direkte med nettstedene. Utviklingen av Web 2.0[22] teknologi i kombinasjon med User Generated Content (UGC)[23] har bidratt med mer variasjon for brukere av Internett. Web 2.0 har oppmuntret til sosiale nettsamfunn som *facebook.com*[24], *myspace.com*[25] og

[22] "Web 2.0" er et begrep som beskriver hvordan www-teknologien i kombinasjon med nettdesign gir bedre brukergrensesnitt og samarbeid mellom brukere, fra http://en.wikipedia.org/wiki/Web_2, aksess 11.07.2008

[23] UGC er også kjent som Consumer Generated Media (CGM) eller User Created Content (UCC), og referer til forskjellige former for mediainnhold som er produsert av ende-brukere og tilgjengelig for offentligheten, fra http://en.wikipedia.org/wiki/User-generated_content, aksess 11.07.2008.

[24] Facebook er et sosialt nettsamfunn hvor brukere kan opprette personlige profiler og utveksle meldinger fra sin egen til andres profiler.

[25] Myspace er et interaktivt nettsted som lar brukere opprette profil og legge til musikk, bilder og videoer som andre kan se.

youTube.com[26], http-baserte e-post løsninger som *hotmail.com*, *yahoo.com* og *gmail.com*, bloggeaktiviteter og personlige nettsteder. Før ble www hovedsakelig brukt til å formidle informasjon, mens nå har det blitt en multiveis kommunikasjonskanal som gjør det vanskeligere å fange opp og blokkere innholdet. En facebook-profil kan for eksempel inneholde kritikk rettet mot en regjering, og dette spres til andre som står på vennelisten til den brukeren.

Tidligere ble all informasjon online overført til en lokal ISP og lagret lokalt. Da kunne myndigheter eventuelt gå inn, lese innholdet når det passet dem, og hvis ønskelig kutte Internett-forbindelsen til brukeren. Web 2.0 har vanskeliggjort denne prosessen siden mye av innholdet hele tiden oppbevares på tjenere langt unna lokale ISP'er. Utvidelsen av bruksområder for www har åpnet for at sosial filtrering kan være vel så effektivt som de tekniske filtreringsmetodene. Internett-kaféer er spesielt utsatt for sosial filtrering i form av overvåkning, siden alle kan komme inn og se hva som foregår. Ifølge Ethan Zuckerman ved Harvard Universitet, Berkman Center for Internet and Society, har noen nasjoner, som Zimbabwe og Egypt, ansatt sikkerhetsfolk som går rundt i sivil på kaféene og kontrollerer hva folk bruker Internett til (Kushner 2008). Sosial filtrering kan altså være overvåkning, eller som case 3 vil demonsterere; en illusjon av at det foregår en overvåkning, slik at brukerne utsetter seg selv for selvsensurering. De vanligste metodene er listet under.

5.2.1 Påført take-downs

Take-downs i seg selv er ikke sosial filtrering. Sosial filtrering oppstår først når for eksempel myndigheter oppfordrer nettverter til å ta ned nettsider med "sensitivt" innhold, ved å ta i bruk trusler i form av straffer slik at det *fører til* take-downs. Dersom myndighetene har tilgang til, eller kontroll over, tjenermaskinene som inneholder domenenavnene, kan de fjerne registreringen av et domene. Nettleseren vil da ikke vise noe informasjon når det ønskede domenet blir aksessert.

Et eksempel på sosial filtrering kan hentes fra Vietnam. Dette landet har vært preget av skandaler angående økonomisk illojalitet i politiske kretser. Den vietnamesiske regjeringen ønsker ikke at innbyggerne skal få vite om slike skandaler, og for at de skal klare å hemmeligholde det tar de i bruk take-downs. De har tvunget Webmastere til å stenge nettsteder med "sensitivt" innhold[27] ved å gi bøter eller foreta arrestasjoner. Amnesty

[26] YouTube er et nettsted som tillater at brukere laster opp videoer slik at andre kan se dem, også her må det opprettes profil først.

[27] Sensitive temaer for Vietnam er korrupsjon, etniske uroligheter, politiske opposisjoner og menneske-rettigheter (ONI 2006).

International rapporterte om ti personer som ble arrestert for å være politisk aktive, og syv av dem ble dømt til fengsel. Dette har ført til at vietnamesiske bloggere ofte velger å skrive på engelsk framfor vietnamesisk, fordi de er redd for at det blir ettervirkninger fra myndighetene som hovedsaklig *filtrerer vietnamesisk språkinnhold*. Det å ikke kunne velge språk fritt begrenser begrenser bloggevirksomheten, men gir brukerne til gjengjeld en følelse av økt trygghet (Vietnam-ONI 2006).

5.2.2 Påført selvsensurering

Ved å oppfordre til selvsensurering fra brukere når de blogger eller poster andre former for informasjon, kan innhold generelt på Internett få en viss form for kontroll. Med trusler om arrestasjoner og anklager om ulovlige aktiviteter vil kanskje brukere unngå å poste eller aksessere informasjon på Internett som de vet at ikke har blitt godkjent.

Land som ikke fører en streng Internett-politikk vil likevel, som følge av forventninger til oppførsel i et nettsamfunn, ha en viss grad av selvsensurering. Dersom en bruker skriver noe upassende, kan andre brukere reagere og ta kontakt med personen. Dette blir en form for nettikette (se kapittel 2), og kan sees på som en mild variant av selvsensurering.

5.3 Oppsummering

Dette kapittelet tok for seg de vanligste metodene for teknisk og sosial filtrering. Det fins flere måter å omgå tekniske filtreringsmetoder på, men flere krever en viss kjennskap til informatikk. Den beste måten å utføre teknisk filtrering på er å ikke la brukere vite at det har foregått en filtrering. Noen (for eksempel myndigheter, uærlige personer, ISP'er og kommersielle aktører) kan ønske å ha en streng kontroll på hva brukere foretar seg på Internett, men utviklingen av www har gjort dette vanskeligere å få til i praksis. Tidligere kunne det kontrolleres hva brukere lastet ned siden alt ble mellomlagret hos lokale ISP'er. Dette har ført til at mange bloggere i land med streng Internett-politikk valgte å blogge på engelsk, i og med at myndighetene først og fremst overvåker det nasjonale språket. Med utviklingen av Web 2.0 har ikke de tekniske filtreringsmetodene like stor slagkraft lenger. Dette er fordi mye av innholdet blir værende på Internettjenere hele tiden. Som en følge velger noen land i større grad å bruke sosial filtrering, enten i form av skremselstaktikker, eller mer subtilt ved overvåkning av Internett-kaféer.

"Where observation is concerned, chance favors only the prepared mind."
Louis Pasteur

6 Casestudier

Dette kapittelet presenterer tre caser som hver på sin måte vil gi innsikt i hva slags filtrering, overvåkning og sensur som fins på Internett i dag. Målet er å oppnå kunnskap angående nytteverdien og effektene filtrering gir.

1. Case 1 vil ta for seg eksempler fra *allmenn praktisering av filtreringsteknikker* for privatpersoner og selskaper som banker og kommersielle firmaer som er med på å lage nye filtre for kjøp og salg.
2. Case 2 tar for seg *tekniske filtreringsmetoder* gjennom eksempler fra regjeringsprosjekter i større miljø som ett eller flere land.
3. Case 3 tar for seg filtreringsmetoder med fokus på *sosial filtrering*. Landene det blir gitt eksempler fra er Kina og Egypt som på hver sin måte fører en streng sensur- og filtreringspolitikk av massemediene i landene. Kina er valgt fordi landet regnes for å være det mest sofistikerte landet når det gjelder filtreringsteknikker. Egypt er valgt fordi det på overflaten har en relativt fri Internett-politikk, men ved nærmere undersøkelse viser landet tegn på at det begynner å gå i Kinas retning med en økende bruk av (sosiale) filtreringsmetoder.

Casene vil til sammen dekke følgende aktører:

- Individers bruk av filtreringsteknikker mot andre individer og/eller bedrifter – case 1
- Bedrifters overvåkning av de ansatte – case 1
- Myndigheter som samarbeider med kommersielle firmaer – case 2
- Land som samarbeider om en felles overvåkning av innbyggere i andre land – case 2
- Myndigheter som overvåker kriminelle og antatt kriminelle – case 2 og 3
- Operatører som overvåker privatpersoner på vegne av myndigheter – case 2 og 3

6.1 Case 1: Allmenn filtrering til skade og nytte for Internett

I dette kapittelet vil det bli vist eksempler fra bruk og misbruk av de tekniske filtreringsmetodene omtalt i kapittel 5. Bruken av filtreringsprogramvare kan primært deles i kategoriene kommersiell og offentlig. Her vil den første kategorien gjennomgås, samt *privatpersoners* bruk av den. I den neste casen vil den *offentlige* kategorien illustreres med eksempler fra regjeringers bruk av filtre. Oppbygningen av case 1 er som følger:

> **Avsnitt 6.1.1 Kommersielle overvåkningsfiltre**: tar for seg bruk og misbruk av kommersielle overvåkningsfiltre, og hvordan nettsider kan manipuleres blant annet ved bruk av tekniske filtreringsmetoder.
> **Avsnitt 6.1.2 Filtreringsforsvar mot ID-tyveri**: kommer inn på problemstillingen med stadig økende ID-tyveri på Internett, og hvordan filtreringsmetoder kan beskytte mot dette.
> **Avsnitt 6.1.3 Proxy-basert filtrering i store systemer**: beskriver angrep som ble gjort mot to norske norske nettbanker ved bruk av teknisk filtrering. Videre gis det eksempler på hvordan registrere at det foregår et angrep, og eventuelle mottiltak som kan gjøres.
> **Avsnitt 6.1.4 Sikkerhet i databaser**: tar for seg datadirektivsloven og problem-stillinger rundt samordning av databaser. Tekniske filtreringsmetoder kan brukes til å sikre databasene, eller de kan benyttes til å samle inn informasjon. Filtrering kan i tillegg brukes til å kjøre automatisert profilbygging basert på informasjon fra databasene.

Til slutt i kapittelet kommer det en oppsummering av casen, mens selve funnene blir analysert og diskutert i kapittel 7.

6.1.1 Kommersielle overvåkningsfiltre

Kommersielle filtre inneholder forskjellige sett av regler og kriterier som kan stilles til å begrense søkingen. Slike filtre kalles også heuristiske filtre, og brukes i stor grad av alle brukere av Internett, selv om mange ikke er klar over at de gjør det. Kjente programmer er CyberSitter, NetNanny, FamilyClick, Norton Internet Security Family Edition (NIS) og ClickSafe. Noen av programmene har vært i bruk i mange år, deriblant CyberPatrol som ble

tatt i bruk av store leverandører i Norge allerede i 2002[28]. Programmer som har vært i bruk over lengre tid har etter hvert bygd opp store databaser med informasjon[29]. For eksempel hadde WebSENSE en database med over 10 millioner nettsteder organisert i over 90 kategorier allerede i 2005.

I begynnelsen av 2008 ble siste AVG 8.0 Internet Security lagt ut for salg. Den inneholder blant annet Safe Surf og Safe Search. Disse to applikasjonene kan med såkalte antiphising-funksjoner vurdere en nettsides sikkerhet allerede før brukeren klikker på lenken til siden. ”Phishing” er snoking etter sensitiv informasjon, og betegnelsen er en omskrivning av ”fisking” til hackersjargong. Varianter av phishing som ofte blir brukt er leting i søppel, ”pharming”, trojanske hester og hacking. Alle disse metodene kan benytte seg av for eksempel DNS-manipulering for å få tak i informasjon. Når det foretas et Internettoppslag er det første som skjer at DNS finner den tilhørende IP-adressen. DNS-manipulering foregår mellom disse to stadiene, slik at den riktige IP-adressen ikke blir lokalisert for brukeren (DNS-manipulering er omtalt i kapittel 5.1.1). Slik DNS-manipulering kan påvirke alle ressurser som www, filoverføringer og chat[30]. En URL kan for eksempel fremstå som korrekt i brukerens nettleser, mens det i virkeligheten kan være en kopi av den originale siden. For å hindre at nedlastninger til maskinen starter fra en nettside brukeren er inne på, uten at brukeren har bedt om det, har antiphishing blitt integrert i alle store nettlesere som Internet Explorer, Opera og Mozilla Firefox (Gamme 2008). Utviklingen av sikrere nettlesere gir brukere et bedre forsvar mot hackere og ID-tyver.

MAS fra 3ami er et eksempel på hvor effektiv og fleksibel filtreringsprogrammer har blitt. Programmet er utviklet i samarbeid med ”en ledende engelsk politienhet” (Expect-more 2007), og har vist seg å være et godt verktøy for å overvåke maskiner som står i nettverk, for eksempel på en arbeidsplass. Det lar blant annet brukere sette opp og definere egne regler for overvåkningen, sette i gang videoopptak som filmer skjermdumper, lagre stegvise handlinger som en bruker har utført, og overvåke hvilke data som forlater maskinen. Videre kan programmet også vise rapporter over alt en bruker har foretatt seg og få grafer over blant annet hvor mye Internet Explorer blir brukt og hvilke nettsteder som blir mest besøkt (Martinsen 2008). Utgangspunktet for MAS er at det logger alle tastetrykk og handlinger. På

[28] Telenor lanserte filtreringsprogrammet Kidsurf (som inneholder en modifisering av CyberPatrol) for å begrense tilgang til nettsider med voksent innhold, http://www1.vg.no/spill/artikkel.php?artid=7966971, aksess 29.03.2208.

[29] Med ”informasjon” menes det her sorte- og hvitelister over nettsteder, og kategorier av innhold fra sidene.

[30] Imidlertid gjelder andre regler for e-post som ikke lar seg påvirke av DNS-manipulering. Dette er fordi e-post bruker en annen ressurspost enn ’DNS A’ (Address) som peker til IP-adressen. E-post bruker isteden ’DNS MX’ (Mail Exchange), som er ment eksklusivt for e-post, og som peker til domenenavnet slik at hele problemstillingen blir unngått.

hjemmesiden til en av distributørene for programmet reklamerer de med å føre "etisk overvåkning" for å sikre alles interesser (Expect-more 2007). Med dette menes det at MAS verner om brukeres rettigheter ved at alle får tilgang til å se sin egen overvåkningsprofil og dermed hva som blir lagret om dem. I tillegg blir det anbefalt at alle brukere får synlig varsel om at de blir logget, og informasjon om at alle passord som skrives er kryptert også for MAS. Det som derimot er urovekkende er at programmet kan lagre innhold som brukeren selv aldri hadde ment å spare på, for eksempel avbrutte e-poster eller påbegynte dokumenter som brukeren har bestemt seg for å slette istedenfor fullføre. Kort sagt blir alt som foregår på en maskin logget, og ingenting forblir privat utover at passordene ikke vises i klartekst. Informering om overvåkningen gjør ikke at brukere blir gitt mer privatliv, bare at de blir opplyst om hva som foregår.

Med tall som viser at over åtti prosent av små og mellomstore bedrifter opplevde datakriminalitet i 2003, er det likevel ikke vanskelig å se hvorfor mange selskaper føler behov for slik overvåkning. De vanligste lovbruddene var sabotasje og datatyveri, og en tredjedel av alle økonomiske bedragerier involverte ansatte[31]. I en norsk rapport fra Mørketallsundersøkelsen samme år viste det seg at bare tyve prosent av sakene med datakriminalitet ble løst. Slike tall støtter bruken av MAS og lignende programmer i store arbeidsmiljøer, fordi det ikke er så mange andre muligheter til å avsløre når egne ansatte stjeler og selger informasjon.

6.1.1.1 Manipulering av nettsider

Programmene nevnt ovenfor er lovlige og ment for blant annet å ivareta brukernes interesser, eller for å avdekke illojalitet innenfor et miljø. Programvareutviklingen som foregår i kommersielle selskaper åpner for at kriminelle på Internett kan adoptere lignende teknikker, og det er blant annet her problemene og skadene oppstår.

Sikkerhetsfirmaet F-Secure melder om at datakriminelle har begynt å lage nettsider som er flash-baserte[32] framfor å bruke html kode. Dette er for å unngå at antiphishing-verktøy skal klare å analysere innholdet på sidene. To eksempler på slike flash-baserte phishing-nettsteder er *www.ppal-form-ssl.com* og *www.welcome-ppl.com*[33]. Begge sidene har blitt DNS-manipulert til å se ut som ekte PayPal-sider som brukes til å foreta betalinger med visa eller kredittkort over Internett. Kopier av kjente betalingssider gir brukere en økt følelse av

[31] Tallene er hentet fra en undersøkelse av NOP for National Hi-Tech Crime Unit i England.

[32] Flash er multimedia-programvare som brukes til å lage interaktive nettsider, for eksempel animasjoner eller menyer som kan bevege seg. Det er nødvendig med Macromedia Flash spiller for å vise flash-innhold i vanlige nettlesere.

[33] Phishing-nettsteder skifter stadig navn og URL, så de kan være borte i lesende stund.

trygghet, og dermed øker sjansen for at de blir svindlet ved bruk av tekniske filtreringsmetoder.

Tall fra Netcraft[34] viser at de oppdaget 41 000 phishing-nettsteder i 2005. I midten av 2007 var tallet oppe i 700 000. Dette er kun en indikasjon på økningen og den forbedrede teknologien til de kommersielle programmene som oppdager phishing-nettsteder, og ikke på det reelle tallet av slike nettsteder. Det som skiller programmene som kommer nå fra eldre versjoner er at før var fokuset på å ta bort trusler og reparere skader, mens nå er målet å fjerne truslene *før* de lastes ned på maskinen og skadene skjer (Gamme 2008).

Sikkerhetsfirmaet Finjan oppdaget en database med mer enn 8700 brukernavn og passord til ftp-tjenere verden over som lå ute for salg. Nettbutikken lignet på grensesnittet til Ebay, og ved siden av de hackede ftp-serverenes lokasjon ble det også oppgitt Googles rangering over nettstedene. Hackerne hadde brukt NeoSploit 2 toolkit for å hente inn informasjonen, og i tillegg brukte de SaaS-modellen[35] for å gjøre det lettere for seg. NeoSploit legger til rette for at kriminelle kan bruke ftp-opplysningene til å legge inn egne HTML IFrame tag'er i nettsidene for ftp-tjeneren de ligger på. Det betyr at selv om et nettsted ikke har en svakhet som kan utnyttes, kan hackeren komme inn via en bakdør. Kriminelle kan deretter sikte seg inn på en hvilken som helst datamaskin ved å sende e-post som for eksempel inneholder lenke til en korrupt nettside. Slike lenker er vanlig bruk av DNS-manipulering for å lure brukere til å tro de er inne på legitime nettsteder. Ftp bruker ukrypterte brukernavn og passord, og dette gir en svakhet som kan misbrukes til å nå nettjenere (som kan ha stor sikkerhet på alle andre områder). Selve prosedyren med å få tak i brukernavnene og passordene kan gjøres med en enkel og vanlig teknikk med logging av tastetrykk. Installering av NeoSploit på en maskin gjør nettopp dette, og brukernavn, passord og domener kan dermed fanges opp. Dette betyr at alle kan havne på listen som blir lagt ut for salg, uavhengig av størrelsen på bedriften, fordi angrepene skjer via personer som har tilgang på systemene (Lillesund 2008). Sophos-eksperter[36] oppdager 6000 nye infiserte nettsider hver dag. Åttitre prosent av disse nettsidene tilhører bedrifter og individer som ikke er klar over at de har blitt hacket (LeClaire 2008).

---

[34] Netcraft er et Internett selskap som holder til i Bath, England. De har blant annet spesialisert seg på å analysere nettjenere og domenehoteller, foreta sikkerhetstester, utforske Internett og publisere resultatene.

[35] Software as a Service, SaaS, er en modell til hjelp for programvareselgere som kan utvikle en nettapplikasjon for å besørge, uavhengig eller gjennom tredjeparts, applikasjonen til bruk for kunder på Internett, fra http://en.wikipedia.org/wiki/Software_as_a_Service, aksess 02.03.2008

[36] Sophos er et selskap som har basert seg på programvare som beskytter mot virus, spyware, adware, spam, phishing og lignende. http://www.sophos.com, aksess 29.02.2008

6.1.1.2 Enkle mottiltak for å bedre sikkerheten

Organisert kriminalitet på Internett er blitt et økende problem, og det er en utfordring å gjøre folk oppmerksomme på hvor lett det er å skade bedriften de jobber i. Det holder ikke lenger å foreta de samme sikkerhetsforholdsreglene som ble brukt for noen år tilbake, men ofte er det bare små endringer som skal til for å øke sikkerheten betraktelig. Nettsteder ønsker naturlig nok ikke å havne på ulovlige nettmarkeder hvor andre kan kjøpe sensitive brukeropplysninger om dem. Denne risikoen kan minimeres ved å regelmessig sjekke hvem som har ftp-aksess, samt ha retningslinjer for stadig passordbytte. På denne måten vil det ikke utgjøre like stor fare hvis feil personer fanger opp brukernavn og passord, fordi informasjonen vil ikke være gyldig lenge. Likevel vil kort tid være alt som kreves hvis det er et målrettet angrep. Prinsippet bak sikkerhet er ikke nødvendigvis å lage vanntette systemer, men snarere å sørge for at tilgangen til sensitive opplysninger skal være vanskeligst mulig. Det kan også være en ide å bruke alternative autentikasjonsmetoder for å forsikre seg om at personen i den andre enden virkelig er den de sier de er, for eksempel bruk av SSL eller VPN som unngår manipulerings-problematikken (se kapittel 5). Forvekslinger av identiteter er et omfattende problem på Internett, derfor vil neste avsnitt ta for seg eksempler og problemstillinger rundt dette.

6.1.2 Filtreringsforsvar mot ID-tyveri

Ifølge tall fra FTC[37] blir rundt ti millioner amerikanere frastjålet identiteten sin hvert år. Dette vil tilsvare at hver nordmann vil oppleve ID-tyveri to til tre ganger i løpet av livet (Datatilsynet 2008). Med ID-tyveri menes situasjoner hvor en person eller gruppe personer skaffer seg tilgang til andres ressurser, utfører uønskede transaksjoner, eller tilegner seg rettigheter som tilhører andre uten tillatelse fra de ekte identitetshaverne. Det er typisk en eller flere uærlige personer som samarbeider om å gjennomføre ID-tyveriet, og "ofrene" er oftest tilfeldige brukere av Internett som havner i en av "fellene" som er blitt satt ut. Dette delkapittelet viser når slike episoder kan oppstå og hvordan de kan avverges ved enkle forhåndsregler som å ta i bruk filtreringsprogrammer. De vanlige tipsene for å bedre sikkerheten er å hindre tilgangen til personlige opplysninger ved å bruke programmer som benytter seg av filtreringsteknikker, for eksempel brannmurer, anti-phishing og anti-virus. Disse programmene analyserer nettverkstrafikken til og fra maskinen slik at brukeren har

[37] Federal Trade Commission er en uavhengig virksomhet fra den amerikanske regjering viss hovedmål er å beskytte forbrukere i USA i økonomiske hensyn på et globalt marked hvor teknologiene er i stadig endring, fra http://www.ftc.gov, aksess 25.03.2008

kontroll over informasjonen som forlater maskinen. Selv ett av disse vil alene være til bedre hjelp enn ingen.

Personopplysninger kan sees på som ”råvarer” for å utøve svindel av forskjellige slag på Internett. Motivasjonen bak svindel vil som regel være økonomisk vinning, men det kan også være andre grunner som at noen ønsker å ramme en person. Det skal svært lite til for å gjøre ting vanskelig eller tungvint for en annen person, for eksempel stadig å endre adressen til en utpekt målskive. For å lykkes med økonomisk vinning vil det som regel kreves mer finesse, som neste delkapittel med proxy-basert hacking av nettbanker vil demonstere.

For å forebygge ID-tyveri bør en være oppmerksom på når det virkelig er nødvendig å oppgi personlig informasjon. Spesielt fødselsnummer som blir brukt som brukernavn for eksempel ved pålogging til nettbanker, er et spesielt interessant mål for ID-tyver. Ved å få tak i slike autentiseringsnumre kan tyvene utgi seg for å være disse personene og er dermed et skritt nærmere å få tak i annen informasjon, som passord eller kredittkortnummer (Klingsheim and Hole 2008). Mange sider spør om slike opplysninger selv om de ikke egentlig har behov for dem. Sensitive opplysninger som skrives i e-post, blogger eller andre steder tilkoblet Internett vil alltid ha en risiko for å bli fanget opp av uærlige personer. Eksempler på nettsteder som utgjør en stor risiko for privat informasjon er sosiale nettsteder som *facebook.com* eller *myspace.com.* Disse har fått en enormt stor brukergruppe på kort tid.

Et problem som en bruker ikke kan gjøre mye med er når svakheten ligger i selve nettapplikasjonen. Slike lekkasjer må være opp til den som drifter nettstedet å tette så godt som mulig. Sikkerhet må tas spesielt på alvor på nettsider som inneholder personlig informasjon. At det ikke skjer flere innbrudd for slike nettsteder betyr ikke at de er sikre, men heller at hackere ikke har vært interessert i å undersøke hvor lett det er å komme inn i systemet. Et annet problem er at brukere ofte ikke får vite hva slags informasjonsveksling som skjer mellom kommersielle aktører. Informasjon som har blitt gitt én gang kan bli spredt til flere andre nettsteder, for eksempel via samarbeid mellom aktørene. Når informasjonen befinner seg flere steder, øker sjansen for at den kan bli fanget opp og havne i gale hender.

Sommeren 2007 inntraff en slik hendelse hos telekom-selskapet Tele2. Tele2 hadde allerede året før fått kritikk for at de bare brukte fødselsnummer som autentikasjon, men hadde valgt ikke å gjøre noe med det fram til tidspunktet for innbruddet. Hackerne brukte et program som genererte fødselsnumre for å kunne logge på Tele2, for deretter bruke selskapet som portal til Folkeregisteret. ”Innhøstingen” foregikk i to dager hvor de hentet ut navn og adresser som hørte til fødselsnumrene (Datatilsynet 2008). Mediene rapporterte i ettertid om at 140 000 identiteter kom på avveie[38]. Selv om tallet forblir ubekreftet er det grunn til å tro at lekkasjen var mye større enn dette. Også *Monster.com* fikk frastjålet informasjon sommeren

[38] Tele2 har i etterkant opplyst at nettsiden er blitt endret slik at en lignende lekkasje ikke skal skje.

2007. Dette ble gjort av hackere som ble sporet tilbake til Ukraina. Monster har 73 millioner CV-er i sin database, og phishing-angrepet ga hackerne navn, adresser, telefonnumre og e-postadresser tilhørende 1.3 millioner av disse brukerne (e24 2007). Hva som skjer videre med slike opplysninger kan være alt fra misbruk av ID til å utføre pengesvindel eller utpressing.

Forberedelser for ID-tyveri består i å bygge profiler ved å fange opp mer og mer informasjon om innbyggere. Først må det velges ut offer slik at det kan høstes identiteter. Ofte velges ofrene ut basert på alder, kjønn og hvilket geografisk område de tilhører. Hvis det gjelder en pengesvindel kan det være mer attraktivt å velge ut folk i en eldre aldersgruppe som antagelig vil ha mer penger enn unge folk. Opplysninger som fødselsnummer er nok til å kjøre enkle script som kan generere lister over folk i en aldersgruppe helt ned til en bestemt dag. I Los Angeles samlet en IT-sikkerhetskonsulent inn identiteter for å kunne rane til seg penger og kredittkortinformasjon ved å bruke et botnet på 250 000 datamaskiner som han kunne mate med passord og brukernavn. Dermed hadde han nok maskinkraft tilgjengelig til å kjøre repeterende spørringer mot selskaper og nettbanker til han fikk aksess (e24 2007).

Systemer som nettbanker brukes av flere og flere, og vi ønsker alle å tro at det er en ”sikker” tjeneste. Likevel vil ikke dette alltid være tilfelle hvis noen finner en svakhet i autentiseringsprosedyrene, noe neste avsnitt vil gi eksempel på.

6.1.3 Proxy-basert filtrering i store systemer

En autentiseringsmetode for banker kalt BankID er i skrivende stund i ferd med å bli innført over flere elektroniske tjenester i Norge. Dette avsnittet viser eksempel på bruk av proxy-basert filtreringsmetode til å utføre et såkalt Man-in-the-middle (MitM) angrep for å fange opp brukeropplysninger i banksystemet. Til slutt vises det måter MitM-angrep kan omgås på.

6.1.3.1 MitM-angrep

Den nye prisvinnende[39] sikkerhetsinfrastrukturen til banker i Norge kalles BankID. Den er utviklet av banknæringen gjennom BankID Samarbeidet, i regi av Finansnæringens Hovedorganisasjon (FNH) og Sparebankforeningen, og skal fungere som sikker identifisering og signering på Internett (BankID 2008). En nettbankundersøkelse foretatt av Sparebankforeningen i 2008 viste at det er totalt 2.8 millioner nettbankkunder i Norge, og før 2009 forventes det at flesteparten av disse vil bruke BankID som sin elektroniske ID og signatur (FNH 2008). En av egenskapene ved en infrastruktur er at den er i stadig utvikling, og BankID oppfyller dette kravet med bruksområder som stadig utvides til andre områder, for eksempel e-handel og elektronisk stemmeavgivning. BankID lar en kunde ha et fast

[39] BankID vant en europeisk pris ”eema Award for Excellence in Secure Electronic Business” i 2006.

brukernavn i tillegg til den gamle PIN-koden for å gjøre infrastrukturen sikrere. Slike ekstra foranstaltninger gjøres fordi det fins alltid en risiko ved sikkerhet i alle autentikasjonssystemer, utfordringen er å minimere denne risikoen.

Bruk av proxy for å koble opp mot tjenermaskiner er et vanlig Internettelement, som er lett å slå av i nettleseren. Likevel er det mange situasjoner hvor en bruker ikke kommer forbi det hvis en skal bruke bestemte nettjenester, ved siden av at det også kan være nyttig for å øke nettleserkapasitet og minske båndbreddebruk. Bruk av proxy legger til rette for å legge inn filtrerings- og blokkeringsmekanismer fordi brukeren ikke aksesserer innholdet direkte. (Proxy-basert filtrering er omtalt i kapittel 5.1.2) En slik bruk av proxy ble brukt av NoWire-gruppen[40] da de skulle teste sikkerheten ved autentisering i norske nettbanker ved å utføre et "Proof of Concept Attack"[41] mot BankID[42].

Først måtte de finne ut hvordan systemet var bygd opp, blant annet ved å studere en artikkel sluppet av BankID prosjektet selv, og deretter ved å ta i bruk teknikken "reverse engineering"[43] for å finne ut av den udokumenterte delen. BankID er bygd rundt tre entiteter: en sentral infrastruktur, kundene og selgere på Internett. Selve autentiseringsprosedyren bruker en java-applikasjon som ved å studeres nærmere kunne brukes til å avdekke tekniske detaljer ved BankID. For å se hvordan protokollene fungerte mot kundene undersøkte de inn og utdata, kommunikasjonsstrømmen og applikasjonens kildekode. Dette ble mulig ved å reversere java-applikasjonen og ved å inspisere nettsteder som bruker tjenesten. Det viste seg at applikasjonen styres gjennom html parametere. To av dem spesifiserer adressene til infrastrukturtjeneren, som kjører en to-faktor autentiseringsprosedyre, og banktjeneren, som utfører en spørring-respons protokoll (Espelid, Netland et al. 2008). verifisere

Angrepet brukte en blanding av phishing-teknikk bruk av proxy. Dette skjedde ved å endre de to parametrene til applikasjonen slik at den isteden kommuniserte over http med en MitM-proxy satt opp av NoWire-gruppen. Hver gang en bruker laster ned BankID klienten lastes også html koden med parameterne til java-applikasjonen ned. En brukers nettleser vil

[40] NoWire er navnet på en forskningsgruppe opprettet ved Universitetet i Bergen, som blant annet prøver å finne ut hvordan informasjon lekker fra systemer som er tilkoblet Internett. Gruppens interesser inkluderer risk håndtering av informasjonssystemer, personvern og ID-tyveri og Smartphone sikkerhet, fra http://www.nowires.org/, aksess 25.03.2008.

[41] Proof of concept betyr at en metode eller et sett med ideer skal bli testet ut for å demonsterere et prinsipp eller bekrefte at et konsept stemmer.

[42] Angrepet *Proof of Concept* NoWire-gruppen gjorde mot BankID var basert på to tilfeldig valgte norske nettbanker.

[43] Reverse engineering (RE) beskriver en prosess som ofte innebærer å ta (teknologiske) ting, som programvare eller maskinvare, fra hverandre for å se hvordan de fungerer, for eksempel hvis det ikke fins noe dokumentasjon.

ikke være i stand til å oppfatte at html parametre har blitt endret siden *html-koden ikke er signert*. Det er bare selve java-applikasjonen som har signering (Hole, Tjøstheim et al. 2008).

Ved å sette opp en proxy mellom kunden og banken får hackere med seg kommunikasjonen som foregår mellom java-applikasjonen og banken. Dette er tilstrekkelig til å få tak i en autorisert sesjon til banken, men informasjonsstrømmen mellom kunden og infrastrukturen er likevel *kryptert*, slik at en proxy ikke vil få tak i kundedetaljene. En angriper må fange opp minst ett engangspassord og det tilhørende dynamiske passordet for å overføre penger ut av kontoen. Dette kan oppnås ved å gi brukeren beskjed ved slutten av innloggingsprosedyren at det foregående inntastede passordet og engangspassordet var feil, slik at angriperen spør etter dem igjen. Angrepet vil da se slik ut (Espelid, Netland et al. 2008):

1. Lure brukeren til å besøke en nettside med en proxy, og initialisere java-applikasjonen med de endrete parameterne.
2. Starte en https-sesjon mellom MitM-proxy og banken for å få tak i de gjeldende identitetene.
3. Avskjære trafikken til autentiseringen er fullført.
4. Fange opp https-sesjonen til selgeren etter at autentiseringen er fullført.

Denne bruken av proxy-basert filtrering ga aksess til flere kundekontoer i et system som ble antatt å være sikkert. Ved å studere systemet ble det funnet sikkerhetsbrister som var blitt oversett, men alle systemer vil mest sannsynlig ha en eller annen form for svakhet bare en ser nøye nok etter. Bankene ble gjort oppmerksomme på de som ble funnet av NoWire-gruppen, og er i skrivende stund i full funksjon uten at det har blitt rapportert om flere sikkerhetsbrister.

Metoden som er blitt beskrevet trenger noen som er datakyndige til å sette opp MitM-angrepet. Imidlertid kan nesten hvem som helst klare å utføre sofistikerte phishing-angrep med utvalget av programvarer som fins for salg på Internett[44] (Martinsen 2007). I tillegg har metodene blitt mer avanserte og samtidig enklere å bruke takket være brukervennlige grensesnitt på programmene. Markedsplassene på Internett gjør det lett å spre programvaren til alle som er interessert i dem. Når personer uten innsikt eller ekspertise blir i stand til å utføre phishing av antatte ”trygge” nettsteder må sikkerheten forbedres tilsvarende.

[44] Det gjennomsnittelige phishing-offeret mistet omtrent 10 000 kroner i 2007 i motsetning til rundt 2000 kroner i 2005. Phishing har vært i bruk helt fra AOL fikk lekkasje av brukerkontoene sine i 1996, og antallet angrep har økt for hvert år siden da, fra http://www.idg.no/kunnskapssenter/sikkerhet/idtyveri/article49509.ece, aksess 02.03.2008

Sikkerhetsavdelingen RSA[45] ved EMC har meldt at deres Anti-Fraud Detection Center (AFCC) oppdaget en gratis demonstrasjonsversjon av et universelt MitM phishing-sett. Programvaren skal ifølge selskapet ha et brukervennlig grensesnitt og automatiserer programmeringen som trengs for å utføre et ellers vanskelig MitM-angrep. Ifølge RSA kan programvaren brukes på ethvert nettsted uten at det trengs å gjøre justeringer på selve programmet. Angrepet utføres ved å lure brukere til en fikset URL-adresse ved å sende linken i en e-post. Den korrupte URL-adressen kommuniserer med det ekte nettstedet i sanntid for å gjøre svindelen så overbevisende som mulig (Martinsen 2007).

Mediene har tatt opp spørsmålet om hvorfor det ikke blir brukt mer tid og ressurser på å lage sikrere systemer for nettbanktjenester, og viser til eksempelet med hackingen av BankID. En forklaring er at sikkerhet ikke lønner seg, fordi å lage et nytt og sikrere system vil koste mer enn hva mange nettbanker ønsker å investere (e24 2008). En koordinator for BankID sier at de har 300 000 transaksjoner daglig, men har aldri opplevd at noen av kundene deres blitt utsatt for et MitM-angrep (Solli 2008). Likevel hadde DnbNor fem datainnbrudd i 2007, hvor kundene ble svindlet for i overkant av 200 000 kroner. Et nytt system vil bli meget kostbart og kan komme til å koste over 250 millioner. Et sikrere system kan også komme til å gå utover brukervennligheten, da det ville kreve lengre og mer kompliserte autentiseringsprosedyrer. Tall fra DnbNor oppgir at svindelbeløpet i Norge totalt sett ikke er mer enn to millioner kroner, og det er en sum bankene fint klarer å betale (e24 2008).

Internett og www legger til rette for både bruk og misbruk, og med alle programmene som blir utviklet kan de brukes som verktøy for alle som driver med kriminelle aktiviteter. Hvorvidt en nå må ty til nye virkemidler for å ha kontroll på hvordan folk bruker Internett er blitt et nytt punkt på dagsordenen. Dette fører til at vi er i ferd med å etablere nye direktiver og lover i et forsøk på å kontrollere Internett.

6.1.3.2 Hvordan omgå MitM-angrep

I kapittel 5 ble det nevnt noen måter å omgå tekniske filtreringsmetoder på, men dette avsnittet går litt nærmere inn på hva brukere velger å gjøre i praksis, gitt en situasjon med MitM-angrep ved bruk av proxy-filtrering som nevnt over. For å ta et eksempel fra en vanlig nettsesjon: påloggingsinformasjon som brukernavn og passord blir lagt inn på en http side for så å videresendes til en https[46] url for autentisering. For å ta en ”sikker” foranstaltning først:

[45] RSA har spesialisert seg på å lage sikre systemer for bedrifter. De slo seg sammen med EMC Corporation and Network Intelligence for å danne hele sikkerhetsavdelingen for EMC. http://www.rsa.com/, aksess 20.03.2008.

[46] https krypterer data etter at brukeren har trykket send/submit, ikke mens det skrives inn i tabellen. En sikkerhetsforanstaltning brukere kan ta er å konfigurere nettleseren til å gi en advarsel hvis en blir sendt fra en https kanal til en vanlig http. Da vil ikke brukeren trenge å tenke på om informasjonen som gis på en https side vil bli sendt over til http, fordi noe slikt ville utløst en advarsel.

Brukeren kan sjekke kildekoden og verifisere at informasjonen faktisk blir sendt til en https; hvis den gjør dette er transaksjonen gyldig. Dette er imidlertid ikke en god løsning, for de færreste tar seg bryet med å sjekke kildekoden til nettsider. For å ta det et skritt videre kan en si at alle brukere også bør gjøre en sjekk på SSL sertifikatene på de https sidene de kommer innom. Nok en gang kan dette enkelt avvises i praksis ved at brukere antar (om de i det hele tatt tenker på det) at hvis en SSL er ugyldig vil de bli advart om dette.

Ved å bruke proxy-videresending og/eller DNS-manipulering kan brukeren bli sendt til en kopi av https-siden som har et ”gyldig” SSL sertifikat. I slike tilfeller kan det hende at nettleseren ikke advarer om noen feil siden sertifikatet er gyldig for den falske siden.

Likevel vil det ikke være mulig å forfalske DNS navnet, slik at brukeren vil kunne observere om ”https://www.nordea.no” har en annen link, for eksempel ”https://www.nodrea.no”. Problemet oppstår hvis det skjer en DNS-manipulering slik at brukeren går til https://www.nordea.no på IP-adressen ”1.1.1.1”, istedenfor den riktige https://www.nordea.no på ”2.2.2.2”. Gitt en slik situasjon må en angriper likevel klare å finne et gyldig sertifikat for www.nordea.no adressen, og det er her SSL-sikkerheten spiller inn.

SSL (og TLS) blir regnet som sikre for slike typer angrep, og eneste måten en bruker kan gjøre feil er ved at det ikke sjekkes for at det står riktig domenenavn, eller at bruker ignorerer nettleserens advarsel om et ikke godkjent sertifikat. En slik oppfatning er hva som gjør eksempelet med MitM-angrepet på BankID interessant, for brukerne ville ikke fått opp slike advarsler på grunn av sikkerhetshullene som ble benyttet. Heldigvis er det ikke vanlig med dyktige spesifikke angrep da de fleste angripere heller tenker kvantitet framfor kvalitet og går etter mer uforsiktige brukere, men det ble tatt med for å vise mulighetene for de som går inn for å finne svakheter i systemer.

En annen ting å tenke på er at hvis en datamaskin først er blitt infisert med malware[47] kan ingen SSL, TLS, Pretty Good Privacy (PGP)[48], GnuPG[49], Truecrypt[50] eller lignende bli regnet som sikkert. Tastaturloggeprogrammer utgjør en stor sikkerhetsrisiko, og det kan være så enkelt som at noen barn i huset har trykket vilt rundt på lenker på nettsidene og dermed lastet ned noe malware. En stund senere sitter en forelder foran den samme datamaskinen og logger seg inn på sin personlige nettbank, og plutselig vil ingen av de nevnte sikkerhetstipsene hjelpe. Dette gjelder primært hjemmemaskiner, men et spørsmål det er verdt

[47] Malware er en forkorkortelse for Malicious Software og er programvare spesielt designet for å infiltrere eller skade en datamaskins operativsystem.

[48] PGP er et program som kan brukes til å kryptere meldinger, og til å signere en melding digitalt.

[49] GnuPGP (GPG) er åpen kildekode av programvare som gjør mye det samme som PGP.

[50] Truecrypt er et program som kan lage en virtuell kryptert disk inne i en fil og åpne den som en normal disk, for eksempel lage en virtuell disk ”H:” og flytte mappen "Mine Dokumenter" til denne slik at mappen dermed ligger på et kryptert volum.

å stille er: hvor mye informasjon er lagret om den vanlige Internett-brukeren i offentlige databaser, og hva slags sikkerhet har de?

6.1.4 Sikkerhet i databaser

Dette delkapittelet beskriver hvordan mye informasjon som er samlet på ett sted kan utgjøre en trussel for personvernet, blant annet ved bruk av filtreringsmetoder. Etter hvert som det oppstår en konvergering mellom selskaper som samarbeider blir databasene deres samordnet. Dette gjelder også personlig informasjon som blir lagret i store, offentlige databaser som blir samordnet med andre offentlige databaser. I 2009 vil det nye "datalagringsdirektivet" bli innført i Norge. Det legger til rette for at alle våre elektroniske spor skal bli samlet inn, inkludert våre nettvaner. Neste avsnitt beskriver denne loven og tar for seg en av to problemstillinger ved slike databaser. Den første er at databasene risikerer informasjonslekkasje, spesielt siden de bruker varierende sikkerhetstiltak. Datakriminelle kan bruke filtreringsmetoder for å lure til seg opplysninger. Den andre problemstillingen omtales i avsnitt 6.1.4.2 om feil som oppstår når filtreringskriterier brukes på informasjonen i databasene. Dette kan være å lage profiler over hva som (antas) passer til å beskrive for eksempel tyver, sosiopater eller pedofile. Mønstergjenkjenning er evnen til å identifisere ett spesifisert mønster blant mange ved bruk av filtreringskriterier. Automatisk mønstergjenkjenning i kombinasjon med filtrering kan riktignok lage profiler av mange informasjonssegmenter. Imidlertid er det viktig å være klar over at det kan fort skje feilkalkuleringer ved automatiserte verktøy når de behandler store datasett som sentraliserte databaser.

6.1.4.1 Datalagringsdirektivet

Datadirektivet er et nytt direktiv som EU og EØS har pålagt alle medlemsstatene å implementere. Det innebærer at alle landene blir pliktige til å lagre trafikkdata fra telekommunikasjon, som gjelder bruk av fasttelefon, mobiltelefon, Internett og e-post for samtlige innbyggere. I slutten av februar ble direktivet innført i Irland[51], og loven er allerede innført i Storbritannia, Danmark, Spania og Tyskland (Solli 2008). Lovartiklene omhandler blant annet hva slags kriminalitet det gjelder, hva som skal lagres og tidsgrensene for oppbevaring av informasjonen. Virkeområdet skal bare omfatte alvorlig kriminalitet som

[51] Irland og Slovakia har gått til sak mot EU-kommisjonen fordi de mener at det ikke er riktig hjemmel for direktivet. Målsettingen med direktivet er å bekjempe kriminalitet, som ikke kommer inn under EUs justis- og politisamarbeid. Hvis Irland vinner i EU-domstolen så vil direktivet bli erklært ugyldig, fra http://www.idg.no/computerworld/article89143.ece, aksess 05.03.2008.

terrortrussel[52], men erfaring fra andre land viser at det er en fare for utglidning av virkeområdet, i tillegg til at definisjonen for grov kriminalitet er opp til hvert enkelt land å bestemme. Lagringstiden er også opp til myndighetene i hvert land å bestemme, fra seks til maksimalt 24 måneder (Datatilsynet 2008).

I Norge skal direktivet implementeres senest mars 2009. Når det gjelder informasjonen som skal lagres skal ikke selve *innholdet* av kommunikasjonen tas vare på, men brukeridentiteter av e-post, IP-adresser, dato og klokkeslett for kommunikasjonen og lignende. På denne måten vil det ofte være mulig å spore nøyaktig hvilken bedrift som har foretatt kommunikasjonen. Det skal også bli lagret lokaliseringsdata for mobiltelefoner slik at det er mulig å finne ut fra hvor kommunikasjonen fant sted geografisk sett (Jarbekk 2008). Direktøren i Næringslivets Sikkerhetsråd (NSR), Kim Ellertsen, påpeker at mange tror at lagring av trafikkdata ikke vil gi så mye mening siden innholdet av kommunikasjonen er borte**.** I virkeligheten vil en oversikt over elektroniske spor, sammen med andre spor, være nok til å lage en analyse som til slutt gir en profil over for eksempel en mistenkt i en etterforskning (Bye and Sjue 2008, s.131).

Informasjonen som blir lagret skal oppbevares hos teleoperatørene til noen fra myndighetene[53] har hjemmel for å hente ut og bruke bestemte deler av opplysningene. Dette stiller høye krav til at de private aktørene er bevisst ansvaret sitt. Store leverandører som Telenor og Netcom har gode forutsetninger for å klare disse nye arbeidsoppgavene. De har ressurser til å lage nye rutiner i tillegg til store systemer som kan lagre enorme mengder informasjon. Imidlertid vil det dukke opp flere risikoer ved innføring av et slikt direktiv. Mindre leverandører vil få vanskeligheter både med tanke på kostnadene bak langvarig lagring av opplysningene og ikke minst at det vil bli krevende å drifte med tanke på sikkerheten. Hvis opplysninger kommer på avveie, noe som antagelig vil skje før eller senere, er det leverandøren selv som vil få skylden. For at et slikt system skal fungere må det være strenge krav til hvem som får aksess til informasjonen, i tillegg til loggføring for tidspunkt og hvem som henter ut informasjonen (Lillesund 2008). Datatilsynet kritiserer Politi- og Justisdepartementet for at de ikke tar nok hensyn til Personvernloven. Systemene er gamle og det er dårlige sletterutiner på informasjon, som dermed blir liggende lenger enn nødvendig. Datatilsynet har hjemmel i personopplysningsloven til å drive tilsyn med alle virksomheter som behandler personopplysninger, men på grunn av straffeprosessloven har de ikke mulighet til å kontrollere Politiets behandlingsmåter av sensitive personopplysninger (Lillesund 2008).

[52] De store terrorangrepene i London 7. juli 2005 er en av grunnene for opprettelsen av direktivet.

[53] Det er ikke blitt bestemt hvilke myndigheter som skal hente ut informasjonen, men det blir mest sannsynlig Politiet, og kanskje myndigheter som kredittilsynet, skatteetaten og konkurransetilsynet, fra http://www.datatilsynet.no/templates/Page____2230.aspx, aksess 28.03.2008.

Dette vil de heller ikke få gjort i større grad når en eventuell innføring av det nye Datadirektivet skjer. Det vil oppstå en trussel om informasjonslekkasje fra de det er meningen at skal aksessere informasjonen, for eksempel politiet. Lignende problemstillinger vil mest sannsynlig også dukke opp i andre land som innfører direktivet.

6.1.4.2 Samordning av databaser

En foreslått løsning for å forbedre sikkerheten rundt sensitive opplysninger er å innføre en sentral database for de som ikke har kapasitet til å ordne dette selv. Da kan det fort bli snakk om flere databaser som samordnes for å fungere best mulig mot de som trenger å aksessere informasjonen. Det har vist seg å bli en stadig økning i en slik samordning av databaser, og der en database tidligere har blitt opprettet for ett formål er det nå en tendens til at formålet blir endret i etterkant. Eksempler på slike databaser er: Statens lånekasse for utdanning, som får lov til å sjekke oppgitte adresser mot Posten med det formål å avsløre studenter som oppgir feil adresse for å kunne søke om borteboerstipend, skattemyndigheter, som har fått tilgang til data fra bomringer for å undersøke om oppgitte pendlerfradrag er rettmessige, og Politiet, som har fått fullmakter til å benytte utlendingsregisteret på en annen måte enn det opprinnelig var tiltenkt. Før var registeret bare en oversikt over hvem som har kommet til Norge, mens det nå brukes i etterforskning. Til slutt kan samkjøringen av de store systemene Aetat, Rikstrygdeverket og kommunenes sosialkontor nevnes, som førte til en omorganisering av hele arbeids- og velferdsetaten. Dette ble kalt NAV-reformen og førte til opprettelsen av landets største og mest omfattende dataregister for personinformasjon, som blant annet inneholder den enkeltes sosiale og medisinske status (Bye and Sjue 2008, s.133-139).

Det fins i dag programvare som kan gå gjennom opplysninger, gjenkjenne mønster og sette opp analyser for å avsløre spor som går igjen[54]. De elektroniske sporene dekker e-post, økonomiske transaksjoner, forsikring, eiendomsforhold og mye annet. Ved å sette opp filtreringskriterier på forhånd, med varselstegn for hva som karakteriserer alt fra en terrorist til en butikknasker, svindler og pedofil er det mulig å finne personer som passer til profilene. Det har vist seg at det er store feiltreff ved slike automatiske identifiseringer av personer som havner på ”svartelister”. Problemet for uskyldige personer er at det ikke er like lett å komme av listen igjen (Bye and Sjue 2008, s.145). Ulemper med databaser er at de ikke er vanntette sikkerhetssystemer, og slike ”datasiloer” med informasjon vil bli et spesielt yndet mål blant hackere, id-tyver og andre.

[54] Spesielt etter 11. september 2001 ble det populært med automatisk mønstergjenkjenning for å hjelpe til med politiarbeid i USA.

6.1.5 Oppsummering

I dag er det et stort utvalg av lovlige, kommersielle filtreringsprogrammer som alle kan få tilgang på til varierende innkjøpspriser. Noen av disse gjør mer enn hva folk flest tror er mulig, som at uferdige e-poster eller dokumenter som en bruker sletter kan lagres i en sentral database til eventuelt senere bruk. En slik framgangsmåte kan være ønskelig for store arbeidsplasser hvor målet er å avdekke illojale medarbeidere.

Ved å ta i bruk DNS-manipulering kan uærlige personer blant annet lage kopier av kjente nettsider. Formålet kan være å lure brukere til å oppgi kredittkortnummer og andre sensitive opplysninger. Samtidig kan bruk av filtrering beskytte datamaskiner og nettsurfing. Dette kan være tilfeller hvor brukere har installert filtreringsmetoder som kan analysere nettverkstrafikken, for eksempel i form av brannmurer og antiphishingverktøy. På denne måten kan angrep fra uærlige personer som ID-tyveri bli avverget. Det er tilfeller der brukere ikke kan gjøre stort for å beskytte informasjonen om dem selv, annet enn å stole på at andre gjør det fordi informasjonen kan være lagret i store selskapers databaser. Imidlertid er det flere eksempler på at phishing-angrep mot selskaper har ført til lekkasjer av store mengder sensitive brukeropplysninger, fordi sikkerheten har vært for dårlig.

Proxy-basert filtrering kan brukes til å fange opp informasjon mellom to maskiner, i et såkalt MitM-angrep, slik at bruker ikke er klar over at kommunikasjonen er blitt avskjært. Dette kan føre til at brukeropplysninger blir gitt fra seg i god tro, slik det ble demonstrert med en nettbanksesjon hvor sikkerhetsinfrastrukturen BankID ble hacket. Det fins gratis MitM-phishingsett med enkle brukergrensesnitt som alle kan få tak i via Internett. Heldigvis er det mange gode sikkerhetsrutiner på Internett for å beskytte brukere for blant annet MitM-angrep, som bruk av SSL og TLS, selv om det alltid vil være faremomenter i form av malware, for eksempel tastaturloggingsprogrammer.

Databaser bruker forskjellige grader av sikkerhet, og noen vil risikere informasjonslekkasjer i en høyere grad enn andre. En kjent problemstilling er hvordan klare å sikre systemene best mulig, slik at uærlige folk ikke skal klare å lure til seg opplysninger. Nyere problemstillinger som er mindre kjent dukker opp når mønstergjenkjenning sammen med filtreringskriterier brukes til å sette sammen informasjonssegmenter til en større helhet. Formålet kan være å lage profiler basert på tegn som typisk hører inn under visse former for kriminalitet, og hvilke personer som samsvarer med disse kriteriene. Imidlertid er det ingen garanti for at slike automatiserte filtreringsmetoder ikke vil gjøre feil.

Tekniske filtreringsmetoder kan altså både misbrukes og være en nyttig tjeneste. Denne casen ga noen demonstrasjoner på at utfallet av bruken bestemmes av hvem som tar metodene i bruk av uærlige og ærlige individuelle og i hvilken hensikt filtreringen utføres.

6.2 Case 2: Etterretningstjenesters overvåkning og filtrering

"Gentlemen, don't read each others' mail"
Henry L. Stimson[55]

Dette kapittelet vil se på hvordan regjeringer i vestlige land har valgt å gjennomføre kontroll på Internett, for å hindre blant annet organisert kriminalitet og terrorisme, gjennom bruk av Carnivore og ECHELON. Carnivore er navnet på USAs mest kjente overvåkningsprosjekt og står som en fellesbetegnelse for FBIs programvare som har gjennomgått store endringer fra første gang det ble tatt i bruk, i hva som antas å være 1996. Programmet brukes som et hjelpemiddel for FBI for å avlytte innenlandstrafikk for bestemte personer i USA, og vil bli hovedtema for første del av case 2. ECHELON er en del av en global overvåknings-infrastruktur som har vært i bruk i over 60 år. Det er et automatisk avskjærings- og videresendingssystem som brukes av etterretningstjenester i de engelskspråklige landene USA, England, Canada, New Zealand og Australia. ECHELON er designet for å avskjære Internett, faks og telefonkommunikasjon også mellom sivile personer, og vil være hovedtema for andre del av case 2.

6.2.1 Overvåkningsprosjekter i USA

Overvåkningsprosjekter gjenspeiler i dette kapittelet alle versjoner av Carnivore, og "framtidens Carnivore". Innholdet for dette delkapittelet er:

6.2.1.1 Bakgrunn: for Carnivore, og hvorfor FBI lot rundt 600 sider fra de hemmelige Carnivore-filene komme ut til allmennheten.
6.2.1.2 DragonWare og Magic Lantern: er programvaren som Carnivore omfatter. DragonWare består av tre programmer hvor oppgavene de utfører beskrives. Magic Lantern blir også beskrevet, men FBI har aldri innrømmet at de har brukt dette programmet.
6.2.1.3 Carnivores filtermodus: består av seks forskjellige valg; filtrering på pakker på IP-adresse (fast og dynamisk), protokoll, tekststrenger, porter og e-post adresser. Hver og en blir beskrevet.

[55] Utenriksminister under Hoover, 1929 – 1933.

6.2.1.4 Carnivores oppkobling til Internett med ISP samarbeid: beskriver altså samarbeidet men også problemstillinger rundt en slik oppkobling. Carnivore er som en "black box" for ISP'ene, noe som vanskeliggjør implementeringen.

6.2.1.5 Begrensninger ved Carnivore: er meget tydelige, og bruksområdet for Carnivore er klart definert med at bare bestemte individer kan overvåkes når det er grunn til å tro at det foregår noe kriminelt. FBI blir kontrollert at de overholder reglene.

6.2.1.6 Framtidens Carnivore: er hemmeligstemplet informasjon, men det er klart at Carnivore har blitt lagt ned til fordel for sterkere programvare utgitt av (ikke navngitte) kommersielle aktører.

6.2.1.1 Bakgrunn

I USA har myndighetene brukt spesielle programmer til å overvåke Internett-trafikk, og spesielt e-post, fra sine innbyggere i over tolv år. Det første oppsporingsprogrammet som ble brukt av FBI har blitt sporet tilbake til januar, 1996 (Nabbali and Perry 2003). FBI har klassifisert all informasjon angående deres første overvåkningsprogram som hemmelig og ingen har fått bekreftet hvem som er produsenten bak programmet de bruker. Imidlertid er det grunn til å tro at FBI mest sannsynlig baserte seg på nettverkspakkesporingsprogrammet EtherPeek, utviklet av selskapet WildPackets Inc[56] (Tyson 2001).

Allerede året etter, i februar 1997, tok FBI i bruk det neste systemet, Omnivore. Formålet med Omnivore var å bli i stand til å hjelpe de statlige virksomhetene med å fange opp SMTP trafikk, altså e-post. Disse e-postene ble lokalisert ved å oppgi brukernavn, og hvis ønskelig kunne de bli skrevet ut i *real-time*[57] (Nabbali and Perry 2003).

Etterfølgeren til Omnivore ble den ganske like, men mer kjente Carnivore. På samme måte som Omnivore ble Carnivore implementert i ISP nettverk hvor det var mistanke om kriminell nettaktivitet. Den første offisielle uttalelsen om Carnivores eksistens ble framprovosert av Robert Corn-Revere, en partner i Davis Wright Tremaine advokatfirma som representerte EarthLink, som ønsket å holde regjeringens overvåkningsverktøy unna selskapet deres. I et vitneutsagn foran House of Representatives komité den 6.april, 2000 la Corn-Revere press på FBI om det var tilfellet at de brukte EtherPeek. Programmet var utviklet for

[56] Wildpacket reklamerer med at de er den ledende leverandøren av løsninger for nettverks- og applikasjonsanalyse for dagens konvergerende nettverk, 2008, http://www.wildpackets.com, aksess 19.02.2008. EtherPeek var et analyseprogram rettet mot Ethernet nettverkstrafikk og protokoller.

[57] Real-time Computing, RTC, er systemer som må fullføre en oppgave innen en satt tidsgrense fra hendelsen er startet til systemet responderer. En slik oppgave må fullføres innen tidsgrensen uavhengig av om systemet blir overlastet, og er en praktisk måte å kontrollere at viktige systemoppgaver blir fullført, http://en.wikipedia.org/wiki/Real_time, aksess 23.02.2008.

kommersielle grunner og var aldri ment for nasjonal overvåkning, hvilket advokatfirmaet kunne gi flere eksempler på. FBI nektet for at de brukte EtherPeek, i følgende sitat fra Corn-Revere (McCullagh 2005):

"When we [Corn-Reveres firma] challenged it, they [representanter fra FBI] said, 'We're not using that. That would be wrong. We have our own software developed. It's called Carnivore'"

Det ble stor interesse i USA for hva som lå bak Carnivore, og et søksmål fra EPIC gjorde at FBI ble tvunget til å frigi rundt 600 sider fra Carnivore-filene (Meeks 2000). Mye av informasjonen kom med sort overstryking, men en del konklusjoner kunne trekkes.

6.2.1.2 DragonWare og Magic Lantern

Carnivore er et av tre programmer i DragonWare Suit som ble tatt i bruk av FBI i juni 1999, og er USAs tredje generasjons oppsporingsprogram. Programvaren er spesielt rettet mot å undersøke alle IP-datapakker som sendes på bestemte nettverk, og samle opp de pakkene som tilfredsstiller bestemte filtreringskriterier (Smith, Perritt et al. 2000). Forskjellen mellom Omnivore og Carnivore bestod i plattformen den var bygd for. Omnivore kjørte på Solaris X86, hvilket gjorde det tungvint å implementere en mengde kommersiell maskinvare som ikke ble støttet av plattformen. Carnivore var en forbedret versjon av Omnivore som kunne kjøre på Windows NT maskiner med et *brukervennlig grensesnitt* (Meeks 2000). I tillegg til å gjøre det samme som Omnivore, gjorde Carnivore det også mulig å gjenskape nettsider folk under etterforskning hadde vært inne på i nøyaktig rekkefølge som de hadde sett dem. I tillegg kunne det brukes *remote control access*, muligheter for øyeblikkelig nedlasting av arkivdata og lagring av data uten å stanse oppsamlingen og risikere tap av IP-pakker (Nabbali and Perry 2003).

De andre to programmene ved siden av Carnivore var Packeteer og CoolMiner (Smith, Perritt et al. 2000). Oppgavene til disse var å bearbeide dataene Carnivore samlet inn. Packeteer satte sammen datapakkene i riktig rekkefølge slik at e-postene og nettsidene ble leselig informasjon. CoolMiner la til rette for mer dyptgående bearbeiding av dataene som analyse av data funnet i e-post, eller ekstrapolasjon[58].

Fram til 2001 hadde Carnivore spesielt én stor svakhet; den kunne ikke gjøre mye mot brukere som benyttet seg av sterk kryptering på Internett. Magic Lantern er et virus lagd av

[58] Ekstrapolasjon er en mer usikker metode enn interpolasjon, men passer til bruk i denne sammenhengen. Metoden applikeres utenfor selve dataområdet, men ved å se på sammenhengen det står i kan det trekkes antagelser om det manglende innholdet, slik at det kan skaffes større datasett.

FBI ment for å bli installert på maskiner til folk under etterforskning, for eksempel en trojansk hest sendt som et e-postvedlegg eller ved å utnytte vanlige operativsystem-svakheter (Wikipedia 2008). En trojansk hest gjør det mulig å installere virus *fra en annen maskin*, altså en praktisk løsning for FBI i dette øyemedet. Formålet til Magic Lantern var å finne krypteringsnøklene for den gjeldende maskinens bruker, slik at kryptert informasjon sendt over Internett kunne bli dekryptert. Magic Lantern var ifølge kilder som ble lekket til MSNBC[59] et program som loggførte alle tastaturtrykk som ble gjort på maskinen. Ved å loggføre tastaturtrykk på en maskin er det mulig å spore opp nøyaktig hva som er skrevet, og sende informasjonen tilbake til FBI. Imidlertid benekter FBI noen som helst bruk av Magic Lantern og sier at det bare er et arbeidsprosjekt som ikke vil bli tatt i bruk i praksis (Nabbali and Perry 2003). En slik påstand kan ikke offentligheten få kontrollert nærmere uten at det blir opprettet en gruppe til å gjøre en intern utredning, i og med at det fortsatt er mye som går under klassifisert informasjon.

6.2.1.3 Carnivores filtermodus

Informasjon som imidlertid har blitt sluppet er hvordan Carnivores filtreringsinnstillinger fungerer. Carnivore gir muligheten for å filtrere pakker på IP-adresse, protokoll, tekststrenger, porter og e-post adresser (Smith, Perritt et al. 2000). Hver av disse vil nå bli gjennomgått for å gi et klarere inntrykk av programmets filtermoduser.

IP-filtrering baseres på to muligheter; *fast* eller *dynamisk*. Fast IP-filtrering går for å være den enkleste veien til avskjæring av kommunikasjon. Carnivores Graphic User Interface (GUI), altså det grafiske grensesnittet, inneholder blant annet en egen rute for å skrive inn IP-nummer til målet som er under etterforskning. IP-nummer fra 0.0.0.0 til 255.255.255.255 er gyldige adresser, men etterforskeren er under rettsregulerte restriksjoner for hvilke IP-adresser som kan brukes. Når et valg er blitt gjort vil alle pakkene sendt fra den spesifiserte IP-adressen bli samlet opp og lagret for eventuell framtidig analyse. Dynamisk IP-filtrering benyttes når den som er under etterforskning har stilt inn datamaskinen sin på å bruke enten Remote Authentication Dial In User Service (RADIUS), eller Dynamic Host Configuration Protocol (DHCP) for å tilordne en IP-adresse[60]. Både RADIUS og DHCP bruker en start-adresse når nettsesjonen begynner. Hvis Carnivore ikke får tak i start-adressen er det ikke mulig å innhente noe data for resten av nettsesjonen, og man må vente til neste sesjon.

Utover fast og dynamisk filtrering kan det gjøres andre innstillinger som *protokoll-basert filtrering*. Dette gjør det mulig for FBI å samle inn TCP, UDP eller Internet Control

[59] MSNBC er en kombinasjon av Microsoft Network og NBC. Det er en 24-timers nyhetskanal på kabel-tv i USA, som også er tilgjengelig i Canada.. http://en.wikipedia.org/wiki/MSNBC, aksess 23.02.2008

[60] RADIUS er en nettverksprotokoll som vanligvis brukes av ISP'er eller bedrifter for å koble til Internett eller interne nettverk. DHCP er en protokoll som brukes mye av klienter for å oppnå riktige tilkoblingsbetingelser.

Message Protocol[61] (ICMP) data fra et bestemt mål. Protokollfilteret kan stilles inn på tre nivåer; *fullt, penn,* eller *ingen*. Fullt modus betyr at alle pakkene fra en spesifisert IP-adresse samles inn. Pennmodus samler inn adresseinformasjon hvis slik informasjon er tilgjengelig, som hvilke nettsider som har blitt aksessert, eller hva som står i TO og FROM feltene i SMTP e-post. Samtidig samles også alle datapakkene som representerer innholdet i kommunikasjonene inn, men hvert tegn blir erstattet med en 'X'. På denne måten er det mulig å finne ut hvor mange bytes meldingene består av. Den siste modusen samler ikke inn noen datapakker for TCP, UDP eller ICMP protokollene.

Carnivore tillater i tillegg at det kan stilles inn tekstfiltrering, for eksempel at alle TCP-pakker fra en bestemt IP-adresse som inneholder tekststrengen "bombe" skal samles inn. Denne funksjonen har en utvidelse som gjør det mulig å samle inn hele TCP meldingen hvis det blir funnet treff på en tekststreng i meldingssekvensen. Likevel er det en begrensning ved denne måten å søke etter tekstring på. En fullstendig melding kan være delt opp i mange pakker som sendes i en TCP-strøm. Hvis det for eksempel blir funnet treff på en tekststreng i den nest-siste pakken i TCP-strømmen vil bare de to siste pakkene bli fanget opp. Carnivore går ikke tilbake og fanger opp de tidligere pakkene i strømmen fordi de alt er blitt sjekket og avvist. Dette filteret gjør det mulig å fange opp nettbaserte e-poster som blir sendt via *Hotmail.com* eller *Yahoo.com*, slik at Web 2.0 teknologi ikke utgjør en hindring for innsamling av informasjon.

Det kan settes *portfiltrering* på alle porter for TCP- og UDP-trafikk. Portfilteret kan settes til å kopiere data som kommer fra en bestemt port, for eksempel port 25 (SMTP), 80 (HTTP), 110 (POP3) eller om ønskelig; alle porter.

Den siste formen for filtrering Carnivore tillater er *e-post adressefiltrering*. Ved å skrive inn en e-post adresse kan alle e-post pakker fra denne adressen samles inn. Hvis for eksempel portene SMTP eller POP3 er valgt, men ikke noen e-post adresse er blitt spesifisert, vil alle pakkene på portene bli valgt isteden.

Styrken med Carnivores filtrering er at ved å velge de rette innstillingene kan innsamling av kommunikasjon bli svært presist, og overlasting av data unngås. Ved å lagre gamle filtreringsinnstillinger og spesifisere tilleggsopplysninger som en maksimal filstørrelse på hver utfil, vil det bli lettere å bruke systemet effektivt. Videre kan det velges om filene skal skrives til spesialdisker eller sendes til en skriver (Smith, Perritt et al. 2000).

Carnivores arkitektur består av fire komponenter:

[61] ICMP brukes mye av *operativsystemet* til datamaskiner i nettverk til å sende feilmeldinger for eksempel når det ikke oppnås forbindelse til en ruter, eller en tjeneste ikke kan nås. Protokollen skiller seg fra TCP og UDP med at den typisk ikke brukes til å sende eller motta data mellom endepunkter.

1. TapNDIS driver som er skrevet i lavnivåspråket C. Denne er basert på kode fra WinDis 32 som er et produkt fra Printing Communications Associates, Inc[62].
2. TapAPI.dll som er skrevet i C++. Denne gir programmeringsgrensesnittet for å nå NDIS driverens funksjonaliteter fra andre applikasjoner.
3. Carnivore.dll som også er skrevet i C++. Denne gir funksjonaliteten for å kontrollere avskjæringene av datapakker på Internett.
4. Carnivore.exe som er skrevet i Visual Basic. Dette er Carnivores Graphic User Interface (GUI), altså det grafiske grensesnittet. Den store forskjellen fra forgjengeren Omnivore var at det ikke fantes noen GUI for den.

Carnivore kan sees på som en oversiktelig GUI for et *"snifferprogram"*[63] hvor forskjellige filtreringskriterier kan stilles inn. Datapakker som oppfyller filtreringskriteriene blir eventuelt lagret, og alle andre pakker avvises. En vesentlig forskjell mellom Carnivore og andre sniffeprogrammer er at det finnes legitim etterforskning bak oppsporingen av pakker (Villeneuve 2005). Det kan likevel stilles spørsmålstegn om det er tilfeller hvor det skjer urettmessig innsamling som kan true personvernet. For å komme nærmere inn på slike faremomenter er det nyttig å se på hvordan Carnivore kobler opp til Internett.

6.2.1.4 Carnivores oppkobling til Internett med ISP samarbeid

Carnivore er installert på en maskin uten tastatur eller skjerm, og kan sees på som en *"sort boks"*[64] fordi ingen, unntatt noen ansatte i FBI, vet hvordan den fungerer fullt ut. For at Carnivore skal kunne avskjære Internett-trafikk må den være fysisk tilknyttet en enveis tapping til ISP selskapets system. I tillegg er det satt opp en forbindelse til Carnivores tjenermaskin for å kunne sende pakkene videre til bearbeidelse. En ISP vedlikeholder en del av nettverket og kommuniserer med andre nettverk som blir vedlikeholdt av sine ISP selskaper. Carnivore kan i utgangspunktet kopiere alle datapakker på den delen av nettverket

[62] WinDis 32 er forkortelse for Win32 Network Driver Interface Specification (NDIS) Framework. Printing Communications Associates, Inc, også kalt PCA eller PCAUSA, er et utviklingsfirma som opprinnelig jobbet for å forbedre nettverksløsninger for AppleTalk, i tillegg til DOS og Windowsplattformer. I 1996 begynte PCAUSA en overgang fra konsultasjon til lisensiering av spesialiserte nettverksutviklingsløsninger for Microsoft Windows. Lisensen for WinDis 32 forhindrer FBI fra å frigi noe kildekode for deres TapNDIS driver, http://www.pcausa.com, aksess 25.02.2008.

[63] Et pakkesniffer-program er også kjent som nettverksanalyse eller protokollanalyse. For bestemte typer nettverk fins også Ethernetsniffer eller trådløse sniffere. Det kan være dataprogram eller hardware som avskjærer og loggfører trafikk over digitale nettverk, http://en.wikipedia.org/wiki/Packet_sniffer, aksess 22.02.2008.

[64] En "sort boks" er en teknisk terminologi for, i dette tilfellet, et system hvor alt som er synlig er hovedsakelig inn- og utdata. Dette er til forskjell fra fri kildekode som går under termen "hvit boks".

ISP selskapet er tilkoblet. Imidlertid er det noen restriksjoner å ta hensyn til før Carnivore kan installeres på en ISP. Det må spesifiseres *hvem* som skal overvåkes, *hva* slags data som vil bli samlet inn og *tidsrommet* for når dataene vil bli samlet inn. Slike grenser hjelper til med å beskytte personvernet for alle kundene til ISP selskapene. I tillegg har FBI en grense for hvor lenge en rettslig kjennelse er gyldig på 30 dager (DoJ 1968). Det vil derfor være ulovlig av FBI å ha Carnivore installert på et ISP nettverk på permanent basis (Nabbali and Perry 2004).

På grunn av individuelle tekniske innstillinger ved hvert ISP nettverk kan det være vanskelig å få Carnivore til å fungere slik det skal uten å involvere hjelp fra lokale ISP ansatte. ISP selskapene kan være mindre begeistret for å koble Carnivore til sine systemer på grunn av at det er en sort boks. Når de ikke vet hvordan "boksen" fungerer kan de heller ikke vite hvordan den eventuelt vil påvirke systemet deres. ISP selskapene mener også at de er i en bedre posisjon enn FBI for å kunne si når det er nødvendig med en rettslig kjennelse for å etterforske mistenkelig nettaktivitet, fordi de selv forstår best hvordan nettverket deres fungerer. De argumenterer i tillegg med at de har en plikt til å lagre data som kan brukes i en eventuell rettslig kjennelse, samtidig som de skal beskytte kundenes personlige interesser. FBI har imidlertid loven på sin side; "Title III of the Omnibus Crime Control and Safe Streets Act" fra 1968 krever at ISP selskapene samarbeider. FBI uttalte til kongressen i 2000 at Carnivore er overlegent bedre enn de kommersielle snifferprogrammene som fins på markedet som en ISP typisk ville bruke i sin nettverksdrift (Dempsey). Slike snifferprogrammer kan overvåke mye av nettverkstrafikken, men har svakheter i og med at de ikke er ment for å samle inn data som kan brukes i en lovlig sammenheng. Med dette sier FBI at ISP selskapene ikke har dekning for å imøtekomme kravene en etterforskning trenger og at de må samarbeide med FBI og gi fra seg kontrollen over nettverket deres (Nabbali and Perry 2003).

6.2.1.5 Begrensninger ved Carnivore

I motsetning til hva mange tror leser og lagrer ikke Carnviore alle innkomne og utgående e-poster. Det er bare når det blir funnet treff mellom melding og et potensielt mål spesifisert i filtreringskriteriene at datapakkene blir lagret for senere analyse. Vanlige kunder til en ISP som har installert Carnivore vil ikke få overvåket deres bruk av Internett siden systemet er i stand til å gjøre "kirurgiske" utsnitt av relevant informasjon. Imidlertid kan det føre til at det blir samlet inn *for lite* data når det oppstår et overblokkeringsproblem (beskrevet i kapittel 2). Carnivore overvåker eller leser heller ikke annen elektronisk aktivitet som nyhetsgrupper, telnet, handel på Internett, chat eller noe annet som blir rutet gjennom ISP selskapet. Faktisk blir ingen elektronisk kommunikasjon tatt opp annet enn det spesifiserte subsettet av filer fra det bestemte målet som er under etterforskning (Smith, Perritt et al. 2000).

Carnivore fungerer som en *passiv* sniffer; den kopierer data som går forbi uten å påvirke selve trafikken. På denne måten blir ikke nettverkstrafikken langsommere. Det er blitt

sagt at Carnivore kan få hele Internett til å bryte sammen (Murray 2000). Hvis en Carnivore boks skulle inneholde virus vil den likevel bare slå ut deler av nettverket på grunn av den distribuerte nettverkstopologien til Internett (Baran 1964). Nettverkstrafikken ville bare bli rutet rundt den delen av nettverket som er blitt skadet. For å ta ned store deler av Internett ville det kreve virus på mange knutepunkter, og alle måtte bli satt i gang på samme tid. Carnivore inneholder ikke slike angrepsprogrammer (Nabbali and Perry 2003).

FBI fastholder at systemet ikke søker gjennom Internett-trafikk med innholdsanalyse for å se etter nøkkelord. Carnivore er ikke bygd for slike analyser i tillegg til at det står i loven at innholdssøk for kommunikasjon mellom amerikanske innbyggere på denne måten er ulovlig (Nabbali and Perry 2003). Imidlertid har dets innebygde *tekstfilter* modus mulighet for å gjøre nettopp denne typen søk, men funksjonen skal bare bli brukt når FBI har fått rettslig kjennelse til å samle inn data som for eksempel nettbaserte e-poster. På denne måten må Carnivore innordne seg etter lovene i samfunnet, i motsetning til hva det ble gitt inntrykk av den gangen Carnivore først ble kjent.

6.2.1.6 Framtidens Carnivore

I 2001 skiftet Carnivore navn til DCS1000, men siden mange forbinder FBIs overvåkningsprogram med det gamle navnet brukes dette fortsatt mye. FBI har aldri sagt hva DCS står for og overraskende nok har de uttalt at det ”står ikke for noen ting” (EPIC 2001). Journalister har kommet med andre forslag, som at det står for ”Digital Collection System”. Siden Carnivore kunne gi assosiasjoner til en rovdyrjakt inn i folks privatliv var dette en oppmuntring om å bytte til et mer nøytralt kallenavn. Ved å holde Carnivore som en *sort boks* hemmelighet forsterket FBI den negative oppfatningen publikum hadde fått, og Carnivore havnet på listen over FBIs verste punkter over offentlige relasjoner i flere år (Nabbali and Perry 2003).

Overvåkningseksperter i FBI avsluttet Carnivore prosjektet i 2005, for isteden å gå over til kommersielle produkter for å tyvlytte på nettverkstrafikk. Et slikt skifte viser hvor langt programvare som alle kan kjøpe har kommet i dagens marked. To rapporter til den amerikanske kongressen ble skaffet av det Washington-baserte Electronic Privacy Information Center (EPIC) under loven Freedom of Information Act. Rapportene avslørte at FBI ikke brukte Carnivore (alias DCS1000) i det hele tatt i perioden mellom 2002 og 2003. Isteden brukte byrået i tretten tilfeller av kriminell etterforskning på Internett i den samme perioden forskjellige kommersielle produkter som de ikke nevner navnet på (Poulsen 2005).

I tillegg til at FBI har byttet programvare for overvåkning er det satt høyere krav til ISP selskapene for at de skal ha bedre kontroll med sine egne nettverk og rapportere tilbake til FBI (Villeneuve 2005). Carnivore har med dette gått fra å være hva Paul Bresson (en talsmann fra FBI) kalte ”the best product available” til å ikke lenger holde mål i

sammenligning med de nyeste programmene på markedet (Biba 2005). At ISP selskapene beholder mer av kontrollen over sitt eget nettverk samtidig som det holdes høy standard på overvåkningen teller positivt for både FBI og ISP i framtidens overvåkning. Om det teller like positivt for kundene er mer usikkert. Hvem bestemmer hva som er passende mål for overvåkning, og ut i fra hvilke kriterier? Etterforskninger krever ofte hemmeligholdelse for ikke å ødelegge for resultatene. Programvare som brukes i for eksempel overvåkning må også til en viss grad holdes skjult og kan derfor ikke bli åpen kildekode. Dette er fordi Carnivore har svakheter som kan misbrukes hvis systemet skulle bli eksponert i sin helhet. Slike svakheter er vanlig i de fleste systemer, og forklarer hemmeligholdelsen også for mange kommersielle selskaper når det gjelder deres kildekode.

Til nå har det blitt tatt opp Carnivores evne til å tyvlytte på bestemte individers kommunikasjon via avanserte filtreringsmoduser. Et annet system kalt ECHELON fungerer litt annerledes. Istedenfor å sikte seg ut målpersoner fanger det opp ”all” informasjon for å analysere det i etterkant. I en slik analysering er det nødvendig med automatiske filtreringsteknikker for å unngå informasjonsoverlasting. Dette er tema for de neste avsnittene før det til slutt i delkapittelet gis en felles oppsummering av Carnivore og ECHELON.

6.2.2 Global overvåkning med ECHELON

USA og andre medlemsland har lagt ned mye innsats i å holde detaljer rundt arbeidsoppgavene til ECHELON[65] hemmelig. Den amerikanske regjering går så langt at de fremdeles nekter for at ECHELON eksisterer, selv om både Australia og New Zealand har bekreftet systemets eksistens. Dette kapittelet er basert på at ECHELON virkelig fins, og at det dermed er snakk om et system som er i stand til å ta for seg filtrering på kanskje det største og mest omfattende nivået som fins i verden i dag. Mange av kildene som brukes vil være basert på uttalelser fra folk som har vært i kontakt med systemet og journalister og forfatteres bidrag til forskning på dette området. Innholdet for dette delkapittelet er:

6.2.2.1 Bakgrunn: for ECHELON som forteller hvordan et slikt globalt overvåkningssystem har oppstått.
6.2.2.2 ECHELON et lovløst system? Det gis et innblikk i hva slags arbeidsoppgaver ansatte har i ECHELON, og hvordan systemet kan lure overvåkningsloven som skal beskytte personvernet for innbyggere i ECHELON-landene.

[65] ECHELON brukes i denne oppgaven som en fellesbetegnelse for den globale overvåkningsinfrastrukturen.

6.2.2.3 Filtreringens plass i kommunikasjonsetterretning: går gjennom de fem fasene i etterretningssirkelen: Planlegging, tilgang og innsamling, analyse og prosessering, produksjon, og spredning.

6.2.2.4 ECHELONs oppkobling til Internett: NSA tapper de mest sentrale kommunikasjonssvitsjene, ruterne og aksesspunktene til telekom-selskapene, med deres godkjennelse.

6.2.2.5 Begrensninger ved ECHELON: består av at det ikke kan få med seg absolutt all kommunikasjon, og at programmet må klare å koble seg til mediet som skal avlyttes.

6.2.2.1 Bakgrunn

ECHELONs begynnelse går langt tilbake i tid. Etter den andre verdenskrigen var det blitt skapt militære og politiske allianser som la grunnlaget for et videre samarbeid mellom de samme landene (Poole 1999). I 1947 gjorde USA og England en hemmelig avtale som ble kalt UKUSA-alliansen[66] som gikk ut på å fortsette med å utveksle globale etterretningsaktiviteter for kommunikasjon også i etterkrigstiden. Målet var den gangen hovedsakelig å holde oppsikt med aktivitetene til den tidligere Sovjetunionen. Det var ikke før i 1971 at UKUSA allierte startet opp selve ECHELON (Nabbali and Perry 2004). Mens NSA[67] er førstepart til avtalen er Canada, Australia og New Zealand med som andreparts land. Tredjeparter er Tyskland, Japan, Norge, Sør-Korea og Tyrkia. Det er indikasjoner på at også Kina tilhører denne siste gruppen, men på en begrenset basis (Poole 1999).

Det gjøres ingen offentlige uttalelser av at etterretningstjenestene mellom UKUSA-landene jobber sammen for å styre et globalt avskjæringssystem. Derfor var det overraskende da UKUSA avtalen ble offentliggjort mars 1999 da den australske regjeringen bekreftet at deres SIGINT organisasjon Defence Signals Directorate (DSD) (Campbell 1999):

"… [DSD] does co-operate with counterpart signals intelligence organisations overseas under the UKUSA relationship".

Til den dag i dag vet ikke offentligheten nøyaktig hva som står i avtalen, uten at det i seg selv er mistenkelig. Hemmeligholdelse gjør etterretningsarbeid lettere og i mange tilfeller sikrere.

[66] UKUSA står for United Kingdom og USA. Selv om det diplomatiske fundamentet for ECHELON er UKUSA-avtalen har avtalen sine røtter i BRUSA COMINT alliansen som ble dannet i starten av Andre Verdenskrig og ratifisert 17.mai, 1943 mellom Storbritannia og USA (Poole 1999).

[67] NSA er den største partneren i ECHELON med et budsjett på over 3.6 billioner dollar, et større budsjett enn FBI og CIA har, med over 21000 personer ansatt håndhever de først og fremst retningslinjene bak systemet. Det fins ikke oppsyn fra myndigheter eller samfunn utover dem selv og den innflytelsen andrepartslandene har (Nabbali and Perry 2004).

Det å ikke avsløre detaljer er en naturlig del av arbeidet de driver med. Videre analyse av et slikt system kan bare oppnås gjennom å samle så mange tegn som mulig, og dermed bygge opp en overbevisende samling som til sammen utgjør et bevis for hva slags aktiviteter som blir foretatt (Schmid 2001). Dette er i stor grad blitt gjort i dag med samarbeid mellom forfattere, journalister og forskere, som har oppdaget hver sine segmenter av informasjon og lagt dem sammen for å danne et bilde av ECHELON.

Forfatteren Nicky Hager fra New Zealand var den som først nevnte at det fantes et globalt avskjæringsnettverk og han var også den første som tok i bruk navnet ECHELON. I 1996 ga han ut boken "Secret Power – New Zealand's role in the international spy network" som omhandlet dette[68]. Boken skapte oppsikt og allerede året etter ble den første STOA rapporten lagt fram for Europaparlamentet. Rapporten bidro ytterligere til å gjøre folk i Europa oppmerksomme på ECHELON. Forfatteren Steve Wright påsto at alle former for kommunikasjon foretatt i Europa via e-poster, telefon og/eller faks ble rutinemessig fanget opp av NSA. Denne saken førte til en ny omfattende rapport i 1999. En av grunnene for uroen rundt ECHELON var påstanden om at systemet hadde *beveget seg vekk fra sitt opprinnelige formål* som var forsvar mot østblokk-landene, og isteden var blitt tatt i bruk som et verktøy for blant annet industrispionasje (Schmid 2001).

Ved at landene under UKUSA-avtalen deler satellittovervåkningen, kostnader og resultatene av hva som blir fanget opp av opplysninger, får de en maksimal global dekning for overvåkningen sin. Storbritannia har fått oppgaven med å overvåke Afrika og Europa opp til Ural fjellene av tidligere Sovjetunionen, Canada overvåker de nordlige breddegrader og polområdene, Australia og New Zealand overvåker Oseania og områdene rundt det indiske hav, og USA overvåker Nord og Sør-Amerikas overføringer, og også Intelsat sendinger over Stillehavet.

Meldingene som blir fanget opp gjennomgås av datamaskiner for å finne spesielle nøkkelord, hvem som har sendt dem og hvem som mottar dem. Det er i denne prosessen at filtrering har den sentrale oppgaven med å filtrere ut *hva* som er relevant informasjon i massen, noe som ofte kan karakteriseres med å finne "nåla i høystakken". Informasjonen blir prosessert av massive superdatamaskiner driftet av UKUSA og NSA spesielt. Alle basestasjonene[69] vedlikeholder sine egne ordlister med nøkkelord og har en avtale om å

[68] Boken er basert på dokumenter fra offentlige kilder som arkiver og aviser i tillegg til intervjuer med mer enn 50 personer som enten var ansatt ved New Zealands etterretningstjeneste GCSB, eller på annen måte involvert med etterretningsaktiviteter.

[69] Kjente basestasjoner for overvåkningssatellitter er plassert over hele verden: Washington og Vest Virginia (USA), Sebana Secra (Puerto Rico), Morwenstow og Mentwith Hill (England), Geraldton og Shoal Bay (Australia), Misawa (Japan), Waihopai (New Zealand), Leitrim (Canada), Bad Aibling (Tyskland).

videresende etterspurt informasjon til de gjeldende hovedkvarterene som har bedt om opplysningene (Poole 1999).

Det er naturlig å tro at det fins andre avskjæringssystemer i land som ikke er inkludert i UKUSA-alliansen[70], men ECHELON er til dags dato det eneste systemet det fins dokumentasjon om. Det blir antatt at ECHELON samler inn så mye som 3 billioner kommunikasjoner på en dag og sveiper gjennom 90 prosent av all Internett-trafikk (Nabbali and Perry 2004). Dette er ikke tall som kan bevises siden de som styrer systemet ikke har lagt fram slike statistikker. Likevel er det en indikasjon fra folk som har vært i kontakt med systemet om hvilken kapasitet de mener ECHELON har[71].

6.2.2.2 ECHELON et lovløst system?

Etter Watergateskandalen ble det mer politisk overvåkning innenfor landegrensene i USA, slik at ECHELON-ordlistene har fått tilføyd både politisk og kommersielt innhold. Det som ble designet for å overvåke kommunistland og terrorstater har nå blitt utvidet til å gjelde alle borgere i hele verden. Europaparlamentet har vist bekymring for dette, spesielt fordi personvernet for folk i Europa er truet av det (Poole 1999).

Mike Frost jobbet for Communications Security Establishment[72] (CSE) i mer enn 20 år. Han har påpekt noen problemstillinger ved ECHELON. I et intervju med CBS fortalte han at telefonsamtaler, e-poster og fakser over hele verden blir overvåket, og at dette inkluderer sivil kommunikasjon. Selv jobbet han ved ”spionstasjonen” i Ottawa i Canada, hvor det blir brukt store datamaskiner til å fange opp og analysere nøkkelord. Det er nettopp denne automatikken uten menneskelig abstraksjonsevne som kan skape ubehagelige situasjoner. For eksempel forteller han om en dame viss navn og telefonnummer ble lagt inn i ECHELONs database som en mulig terrorist fordi hun fortalte en venn på telefonen at sønnen hadde ”bomba” i skoleoppsetninga (60Minutes 2000). Overvåkningsprogramvaren rekonstruerte konversasjonen da den fanget opp nøkkelordet *bombe* fra ordlisten sin. Han som analyserte det var ikke sikker på hva det gjaldt, og for å være på den sikre siden ble hennes navn og telefonnummer lagt inn i databasen over mulige terrorister til eventuell senere analyse (Schmid 2001). Frost mener at verden har bruk for ECHELON programvare som bidrar til å

[70] Det fins minst 30 kommunikasjonsorganisasjoner i land utenom UKUSA, som Russlands FAPSI som hadde 54000 ansatte alt i år 2000, og Kina som blant annet har to basestasjoner rettet mot Russland og bruker disse i et slags samarbeid med USA. Det er også kjent at flere land i Midt-Østen, spesielt Israel, India og Pakistan, har investert i signaletterretning.

[71] Slike kalkulasjoner er delvis basert på hvordan satellittbasestasjoner er geografisk plassert i verden, kapasiteten til superdatamaskiner og avskjæringsprogramvare.

[72] Den kanadiske etterretningstjenesten.

gjøre etterretning sikrere, men at det mangler et sikkerhetsnett for uskyldige mennesker som blir fanget opp av systemet (60Minutes 2000).

Med et slikt system, hvor de som står bak kan nekte for at det fins, gis ECHELON og lignende systemer muligheten for å stille seg utenfor vanlige lover. Etter hvert som det har kommet frem flere og sterkere bevis for at systemet eksisterer har private organisasjoner og individer blitt bekymret for om ECHELON er lovløst. I et forsøk på å svare på hvilke retningslinjer eller lover ECHELON følger saksøkte EPIC den amerikanske regjering (Wired 1999). De tapte saken og dermed muligheten for å få tilgang på eventuelle dokumenter som kunne si mer om ECHELONs restriksjoner.

I utgangspunktet sier den amerikanske overvåkningsloven at demokratiske land ikke har lov å spionere på sine egne innbyggere. Denne loven kan forbigås hvis et medlemsland av ECHELON ønsker å spionere på en av sine egne borgere ved å få et av de andre medlemslandene til å foreta overvåkningen, for deretter å rapportere tilbake til dem. En slik metode ble ifølge Frost brukt av Margaret Thatcher. Thatcher mente at to av ministrene ikke var ”helt på hennes side” og ville bekrefte dette. For å finne ut mer ba hun den kanadiske etterretningstjenesten CSE om å spionere på vegne av den britiske etterretningstjenesten, Government Communications Headquarters (GCHQ). CSE dro til London og fanget opp all kommunikasjonstrafikk fra de to ministrene. På denne måten kunne det britiske parlamentet benekte at de hadde gjort noe galt siden det kanadiske medlemslandet hadde gjort det for dem (60Minutes 2000).

Den amerikanske kongressen holdt høring for å finne ut mer om aktivitetene til ECHELON, fordi folk ble urolige da det begynte å lekke ut historier om overvåkning av sivile samtaler og annen kommunikasjon. Spørsmålet ble om personvernet for amerikanske borgere var truet, istedenfor om ECHELON bare var ment for utenlandsk aktivitet. Det som overraskende nok *ikke* kom opp var hvilke lover og restriksjoner NSA jobbet under når de foretok overvåkninger. Heller ikke spørsmålet om USA ville bekrefte ECHELONs eksistens ble nevnt. Fordi amerikanske borgere ikke var i målgruppen ble det ikke rettet noen spesiell kritikk mot nettverket ECHELON. Hvorvidt sivile europeiske borgere ble overvåket var derfor ikke noe som skapte bekymring. Resultatet ble at så lenge *innenlandstrafikk* ikke ble fanget opp, var det ikke noe i veien for å la ECHELON fortsette i samme spor (Nabbali and Perry 2004).

6.2.2.3 Filtreringens plass i kommunikasjonsetterretning

Kommunikasjonsetterretning, heretter kalt Comint, er en viktig del av signaletterretning (Sigint). Comint er betegnelsen for å avskjære utenlandsk kommunikasjon fra de som egentlig er mottakerne, altså fange opp flere former for kommunikasjonssignaler som inkluderer alt fra radar til optiske fiberkabler for Internett. Målgruppen til Comint har variert mellom flere

områder. Først var det tidlige militære meldinger og diplomatiske kommunikasjoner, deretter ble 1960 årenes kommunikasjon rundt økonomi og vitenskapelige og tekniske utviklinger i fokus. I dag er temaer som narkotikahandel, pengevasking, terrorisme og organisert kriminalitet inkludert (Campbell 1999).

Det er mulig å sette opp en oversikt som blir kalt ”etterretningssirkelen” som er basert på den samme grunnleggende måten å foreta etterretning på i alle land. Syklusen kan måles i fem deler (Campbell 1999), hvor filtrering er en større del av punktene 2 og 3:

1. Planlegging
2. Tilgang og innsamling
3. Analyse og prosessering
4. Produksjon
5. Spredning

Både ved innsamling og analyse vil filtrering være en uvurderlig behandlingsmetode for å ikke samle inn irrelevant informasjon. Under innsamling er det nødvendig å sette opp filtreringskriterier for søk som skal brukes, og ved analyseringen kan det settes opp videre filtreringsegenskaper for å skille ut de delene som er viktig for akkurat den oppgaven som blir gjort.

Planlegging er å finne ut av hvilke krav som skal gjelde for ”kunder”. Med kunder menes det her de spesielle grenene av regjeringen som jobber med blant annet handel, sikkerhet og forsvar. Dette trinnet i etterretningssirkelen gjør kravene om til mulige arbeidsoppgaver og hva som har prioritering på kort og lang sikt. Allerede her er det nødvendig med en vurdering av hva som antas å være sluttproduktet, og om det vil holde mål for i det hele tatt å kunne starte den gjeldende Comint-operasjonen.

Tilgang og innsamling er et viktig trinn for å ta i bruk filtreringskriterier, for å unngå en altfor stor masse av data å analysere i ettertid. Her brukes ECHELON-ordbøker for å effektivisere søket. Hver ECHELON-ordbok blir programmert daglig med nøkkelord som kan være hva som helst, inkludert navn på personer, lokasjoner, skip, land, organisasjoner, telefonnummer, IP-adresser eller andre bestemte ord av interesse. Datamaskinene leter etter nøkkeord fra sine egne ordbøker i tillegg til ordbøkene fra de andre medlemslandenes stasjoner, siden hver basestasjon har sin egen ECHELON-ordbok. Hvis det blir funnet treff sendes resultatet til den stasjonen som skrev inn det bestemte nøkkelordet (Nabbali and Perry 2004). Styrken ved ECHELON ligger i dens kapasitet til å dekryptere, filtrere og undersøke meldinger til bestemte kategorier for videre analyse fra de byråene som har etterlyst informasjonen. Tilgangen må ofte skaffes via dyre og avanserte metoder siden de på samme tid må være sikre og raske, spesielt med tanke på at forskjellige typer informasjon er

uavhengig av like fysiske måter å kommunisere på. For eksempel er det mulig å overføre trafikk av typen tv, video, telefon, faks og data via internasjonale satellittlinker eller via fiberoptiske undervannskabler. Det å bestemme hvilke meldinger som skal samles inn er i de fleste tilfeller en automatisk prosess med filtreringsteknikker og bruk av store databaser til å oppbevare informasjon om interessante målgrupper.

I dagens moderne nettverk er det snakk om store mengder informasjon i tillegg til komplekse signaler som brukes i overførselen. For at det skal bli tid til å samle inn det som viser seg å være relevant er det blitt vanlig å bruke høyhastighetsopptagere, eller ”snapshot” minne. Denne teknikken gjør det mulig å midlertidig holde på store mengder datasett til det er tid til å prosessere dem. Prosesseringen er rett og slett forvandlingen fra innsamlet informasjon til en passende form for analyse. Dette kan som nevnt skje automatisk eller under menneskelig oppsyn, men ofte brukes det en kombinasjon av begge. I prosesseringen foregår det også en form for avskjæring og filtrering. På tidlige tidspunkt, når det ikke er selvforklarende i meldingen eller samtalen, blir hver avskjæring beskrevet med en standard bokstavnotasjon[73] (Campbell 1999). En slik merking av innhold, eller bruk av ”tagger”, gjør det lettere å behandle opplysningene videre i automatisk filtreringssortering. Veksling mellom bruk av maskiner og mennesker viser seg å gi best resultat for både analyse og prosesseringstrinnene.

Produksjon involverer analyse, evaluering, oversetting og tolking av rå data til ferdig etterretning. Det siste skrittet er spredning, som betyr å sende rapportene til etterretningsforbrukerne (Campbell 1999). UKUSA-landene har en begrensning for spredning som sier at Sigint byråer ikke kan samle inn, ta opp eller spre informasjon om ”lovlige personer”. Begrepet inkluderer innbyggere og selskaper registrert i en UKUSA nasjon. Det viser seg at det kan brukes ”smutthull” hvis vedkommende har kommet i målgruppen til et Comint byrå. Et eksempel fra Hager beskrev hvordan tjenestemenn i New Zealand ble instruert til *å fjerne navn som identifiserte dem* som UKUSA innbyggere eller -selskaper fra rapportene deres. Isteden satte de inn ord som “en kanadisk innbygger” eller “et amerikansk selskap” (Campbell 1999).

Innenfor UKUSA systemet er spredning av Comint begrenset til folk med høye sikkerhetsnivåklareringer. Siden bare disse kan se Comint rapporter er det bare de som kan sette krav og kontrollere arbeidsoppgavene, og da kommer dilemmaet med hvem som kontrollerer kontrollørene. Samfunnet generelt er ikke sikkerhetsklarert og har derfor bare et

[73] De to første bokstavene forteller hvilket land kommunikasjonen foregikk i, den tredje bokstaven forteller hva slags generell klasse kommunikasjonen tilhører, C for Commercial, D for Diplomatic, P for Police og så videre. Den fjerde bokstaven forteller hva slags type kommunikasjon det er, for eksempel S for multi-channel. Deretter følger det tall som forteller bestemte linker eller nettverk det gjelder.

beskjedent innsyn i arbeidsoppgavene og ingen oversikt til å foreta kontroller. Dette er igjen for å ivareta den nasjonale sikkerheten ved hemmeligholdelse av etterretningsoperasjoner. Likevel gir det rom for tvil for om systemer som ECHELON brukes i høyere grad enn nødvendig, siden det ikke fins noen større kontroll for bruksområdene.

6.2.2.4 ECHELONs oppkobling til Internett

New York Times skrev i 2006 om hvordan NSA hadde ”tyvlyttet” på amerikanske borgeres sivile kommunikasjon både over telefon og Internett. Dette var en skandale som førte til spørsmål om hva NSA egentlig jobbet ut i fra, og hvordan de klarte å tyvlytte på kommunikasjonene. Avsløringer fortalte om hvordan organisasjonen hadde fått tilgang via direkte oppkobling til infrastrukturene til USAs største telekom selskaper. Dette ble mulig ved at telekom selskapene samarbeidet ved å gi NSA tillatelse til å tappe de mest sentrale kommunikasjonssvitsjene, ruterne eller aksesspunktene deres. Ved å gi NSA tilgang til hoved-gateway’ene, både inn og ut av USA, kunne de samle inn kommunikasjonsmønstre etter filtreringskriterier som ikke er blitt gjort kjent (Lichtblau, Risen et al. 2006).

Dette viser at NSA ikke lenger bare fokuserer på utenlands kommunikasjon, men har utvidet overvåkningen til å inkludere USAs sivile kommunikasjonsinfrastrukturer. Det er ikke en sikker påstand at de i tillegg har tilgang på svitsjer som styrer uten- og innelands kommunikasjoner som går gjennom Internet Exchange Points (IXP) eller ISP’er. Likevel, ifølge undersøkelser gjort av American Civil Liberties Union (ACLU), antas det at NSA fører overvåkning også her.

6.2.2.5 Begrensninger ved ECHELON

Den første rapporten om ECHELON til Europaparlamentet påsto at systemet hadde kapasitet til å avskjære ”alle e-poster, telefoner og fakskommunikasjoner” innenfor Europa. Dette har vist seg å være feil, verken ECHELON eller Sigint systemer kan gjøre dette. Det fins heller ikke utstyr med kapasitet nok til å prosessere og kjenne igjen innhold av alle samtalemeldinger eller telefonoppringinger (Campbell 2000). Hager støtter dette ved et utsagn han ga 24. april 2001. Her spesifiserte han at avskjæringssystemet ECHELON ikke har fullstendig oversikt over all global kommunikasjon som foretas. Det er begrensninger på systemet som gjør at ressursene må brukes mest mulig effektivt, og det gjøres ved å sikte seg inn mot ønskede meldinger som blir antatt å gi mest mulig viktig informasjon. Dette tilsier at sivile innbyggere ikke er i målgruppen for slik overvåkning ved første filtrering. Målgruppen er altså mer politisk og diplomatisk rettet (Schmid 2001).

Ut i fra dette kan to hovedbegrensninger ved et system som ECHELON utledes; første punkt er at systemet er begrenset ved adgangen til kommunikasjonsmediumet. Slike medier kan bestå av kabelkommunikasjon, radiokommunikasjon, kommunikasjon som overføres via

geostasjoners telekommunikasjonssatellitter, avskjæring via mobile fartøy som fly eller skip eller avskjæring via spionsatellitter. Punkt to er at det er begrensninger gjennom nødvendigheten av å filtrere ut relevant informasjon fra en stor masse av kommunikasjoner som skjer på samme tid (Schmid 2001).

6.2.3 Carnivore og ECHELON oppsummering

FBI og DoJ mener Carnivore (og dens for- og ettergjengere) er nødvendig i kampen mot kriminalitet på Internett. Carnivore er ment for innenlands bruk og bare når det foreligger en godkjent rettsordre til å utføre overvåkningen for et bestemt individ. Når etterforskningen er i gang kan de bli kontrollert av de som utstedet rettsordren for å sjekke at alt går riktig for seg. FBI har uttalt at verktøyet ikke vil bli brukt på en feilaktig måte til å avskjære beskyttet, privat kommunikasjon. Når Carnivore blir installert hos en ISP er det ikke på permanent basis men for et bestemt tidsrom og med bestemte mål som skal overvåkes. Kryptert data som hentes fra en mistenkt må vente med å bli dekryptert til etterforskerne har fått innvilget søknad til å gjøre dette. Fordi Carnivore har flere filtermodus som kan justeres til å foreta meget spesifikk kopiering av datapakker, risikerer de heller å samle inn for lite informasjon enn for mye.

Carnivore leter ikke igjennom store mengder Internett-trafikk etter nøkkelord eller bestemt innhold slik som ECHELON. Carnivore er ikke bygd for slike analyser i tillegg til at innholdssøk for kommunikasjon mellom amerikanske innbyggere på denne måten er ulovlig. ECHELON er i motsetning til Carnivore ment som et globalt overvåkningsnett, utført i samarbeid mellom (hovedsakelig) alle de engelskspråklige landene i verden. På grunn av at systemet ikke engang har blitt bekreftet å eksistere av alle medlemslandene finnes det lite til ingen form for oppsyn med hvordan de jobber. ECHELON muliggjør omgåelse av lover, for eksempel i tilfeller hvor USA trenger informasjon om en amerikansk innbygger. De kan spørre et av de andre medlemslandene i ECHELON om å finne informasjonen. Når avskjæring av kommunikasjon ikke blir foretatt av innbyggerens egen regjering vil det ikke være brudd på noen lov, selv om det i praksis er nettopp det som skjer. ECHELON mangler et sikkerhetsnett for mennesker som blir fanget opp av systemets store automatiske innhøstinger av data. Når først noen har blitt registrert i systemet som en potensiell terrorist er det vanskelig å bli fjernet fra databasen igjen. Det er bare sikkerhetsklarerte som kan se Comint rapporter, noe som gjør det vanskelig for allmennheten å vite detaljene rundt hvordan de jobber. ECHELON er fortsatt et hemmelig system, men det er ingen grunn til å tro at overvåkningen har blitt avviklet i de siste årene. Tvert imot antyder tegn i tiden at overvåkningen bare fortsetter å øke. FBI har for eksempel uttalt at de går over til å ta i bruk (ikke navngitt) kommersiell programvare som har kommet lenger i utviklingen på grunn av den økende konkurransen som finnes på markedet i dag.

6.3 Case 3: Land som fører streng Internett-politikk

Dette avsnittet tar for seg filtreringsmetoder som bruker teknisk filtrering, men som også går videre til *sosial filtrering*. For å illustrere slik bruk mest effektivt vil det bli presentert eksempler fra land som fører en streng Internett-politikk; Kina og Egypt, med hovedvekt på Kina. Sosial filtrering inkluderer fjerning av søkeresultater, take-downs og påført selvsensurering hvor spesielt sistnevnte er verdt å merke seg, for den har ført Kina inn i en helt ny overvåkningspraksis av folket. Kina utpeker seg som et land verdt å se nærmere på fordi de har den mest sofistikerte formen for filtreringssystemer i verden. Egypt på sin side fører en annen form for overvåkning enn Kina. De går ikke inn for å oppmuntre folk til selvsensurering, men benytter seg heller av tekniske filtreringsmetoder og straffesanksjoner i etterkant for brukere som er for frittalende på Internett. Bruken av Internett i Egypt viser at det er et land som støtter opp om teknologien, men som likevel ønsker å kontrollere bruken av den. Det blir nevnt eksempler på hvordan regjeringen slår ned på politiske utsagn, især bloggere. Landet i seg selv driver ikke med sensurering på det planet Kina gjør, men i likhet med andre land (for eksempel Vietnam) viser Egypt tendenser til å gå i samme retning som Kina.

6.3.1 Internett og filtrering i Kina

Innholdet for dette delkapittelet er som følger:

6.3.1.1 Bakgrunn: for Kina om hvordan landet setter pris på og videreutvikler ”nyskapninger” inkludert Internett.

6.3.1.2 Kinas infrastruktur og tilgang til Internett: beskriver hvordan Internett teknisk sett fungerer i landet, og hvordan ruterne deres legger til rette for filtrering.

6.3.1.3 Teknisk filtrering og sosial filtrering: tar for seg hvordan begge disse kategoriene av filtrering blir påført brukere i Kina.

6.3.1.4 Tiananmen-massakren: gir et konkret eksempel på en av Kinas største tabusaker i nyere tid, og hvordan informasjonen rundt hendelsen effektivt ble filtrert.

6.3.1.5 Jingjing, Chacha og Panoption-effekten: presenterer Internett-politikonstablene Jingjing og Chacha som vennlig oppfordrer brukere på Internett til selvsensurering, og hvordan dette kan knyttes opp mot en digital Panopticon-effekt hvor alle tror de blir overvåket hele tiden.

6.3.1.6 Bruken av Internett: forteller om kontroll og tvangsnedlegging av Internett-kafeer, fengselsstraffer for brukere som ikke følger retningslinjene til myndighetene, og hvordan blogging brukes til å formidle meninger.

6.3.1.1 Bakgrunn

Kina er verdens eldste fortsatt eksisterende sivilisasjon. Siden kommunistseieren i den kinesiske borgerkrigen som endte i 1949 har Kina vært delt i to. Det er Folkerepublikken Kina med hovedstaden Beijing, og Republikken Kina med hovedstaden Taipei. Landets befolkning er verdens største med sine 1,4 milliarder, med over 6 milliarder mennesker i verden totalt.

Gjennom de siste to tusen årene har Kina hatt en av de beste økonomiene i verden. Financial Times har hevdet at "China has been the world's largest economy for 18 of the past 20 centuries", og The Economist har uttalt at Kina var ikke bare den største økonomien i store deler av historien, men inntil det 15. århundre hadde landet også den høyeste inntekten per innbygger og var verdens teknologiske leder. Kina står bak mange oppfinnelser fra gammel tid som resten av verden har hatt stor nytte av, blant annet kompasset, boktrykkerkunsten, papiret, kruttet, armbrøsten og rustningen. I dagens samfunn har Kina fortsatt med sine produktive evner, og landet produserer nær sagt alle tenkelige varer og tjenester for hjemmemarkedet, i tillegg til en betydelig eksport. Av høyteknologiske varer produserer Kina særlig elektronikk og maskinvare, deriblant datamaskiner og telekommunikasjonsutstyr (Wikipedia 2008). Kina holder seg oppdatert og ligger godt an på det vitenskapelige og teknologiske markedet på verdensbasis, og lærte seg raskt teknologien Internett er basert på da det kom. Med de store ressursene Kina har til rådighet har landet videreutviklet applikasjoner som filtreringsteknikker for å overvåke og holde kontroll med hva innbyggerne foretar seg på Internett.

6.3.1.2 Kinas infrastruktur og tilgang til Internett

Dette avsnittet tar for seg Kinas infrastruktur for at det skal bli tydeligere på hvilke nivåer blokkeringer og sensurering av Internett skjer. De som overvåker infrastrukturen til Internett i Kina heter Ministry of Information Industry (MII). Tall fra China Internet Network Information Center (CNNIC 2007) rapporterer at det totalt er:

- 137 millioner Internett brukere i landet[74]
- 90.7 millioner har tilgang på bredbånd.
- 210 millioner personer bruker Internett totalt, dette er også inkludert de som ikke eier egen datamaskin (Kushner 2008).
- Det er syv statlige lisensierte Internet Access Providers (IAP) med tre til under konstruksjon, hver av disse har minst en forbindelse til et utenlandsk Internett backbone.
- Tre Internet Exchange Points (IXP).

[74] Hentet fra den siste offentlige rapporten til CNNIC i 2007, men tallet er antagelig en god del større i dag.

MII tillater fire statlige organisasjoner å ha nettverk som kan forbindes til det globale Internett. Med bare tre IXP'er å overvåke (til sammenligning kan det nevnes at det er seks IXP'er i Vietnam, et langt mindre land) er det lettere å kontrollere innholdet brukere finner fram til på Internett. IAP'ene gir regionale ISP'er tilgang til backbone forbindelser. I november 2006 uttalte Ministry of Public Security at de var ferdig med første skritt i deres nye prosjekt "Golden Shield". Dette prosjektet går ut på å lage et digitalt nasjonalt overvåkningsnettverk med nesten fullstendig dekning for alle offentlige sikkerhetsenheter i hele landet (Deibert, Palfrey et al. 2008).

Kina ble akseptert av WTO (World Trade Organization) i 2001. Dette åpnet for mer samarbeid mellom vestlige selskaper og Kinas egne, blant annet er Cisco-systemet blitt en integrert del av deres Internett utvikling. Spesielt har de landsdekkende ChinaNet og CERNet tatt til seg denne teknologien. Videre har Cisco et prosjekt i Kina for deres "nestegenerasjons nettverk" kjent som CN2. Dette samarbeidet mellom vestlig teknologi og Kina har fått sterk kritikk fra aktivister og menneskerettsorganisasjoner. De ser dette som en måte å bidra til Kinas utvikling av overvåkningssystemer og sensur mot folket. Cisco (og selskaper som Microsoft) sier på sin side at de verken vil eller burde kontrollere hvordan kundene deres bruker hva de har kjøpt, og at Kina er nettopp dette; en kunde av deres produkter. Ruteren til Ciscos 12000 serie har blitt solgt til Kina i 1998 og i 2004, de har:

- muligheter for pakkefiltrering
- kan filtrere toveis på pakkenivå (kan påvirke både trafikk inn og ut av Kina)
- kan implementere opptil 750 000 forskjellige filtreringsregler
- designet for å håndtere Internett angrep av forskjellige slag (som DoS, spredning av ormer og virus eller blokkering av phishing sider) siden ruteren kan konfigurere Access Control List (ACL).

I tillegg til å blokkere IP-adresser kan Cisco 12000 ruteren også blokkere bestemte deler av http get-forespørsler. Dette er hva som er antatt å være svaret på hvordan Kina kan implementere nøkkelord-filtrering. Med denne muligheten til http-filtrering kan det legges ennå et punkt til listen over; blokkering av politiske sider.

Med teknologien fra Cisco kan en si at i Kina ligger sensuren i selve ruteren. Likevel, selv om ruterne er designet for å kunne takle DoS-angrep er det også en ulempe med denne funksjonen. Kinas filtrering av nøkkelord kan misbrukes til fordel for DoS-angrep ved å forfalske opphavsadressene for deretter å gjøre forespørsler som inneholder forbudte nøkkelord. Slike masete forespørsler sliter ut tjeneren slik at den ikke klarer å behandle alle

sammen, noe som fører til at kommunikasjonen mellom to tilsiktede endepunkter blir blokkert. Tjeneren kan forsvare seg ved å bruke for eksempel en IP-blokkeringsteknikk og dermed slippe all trafikk fra et punkt i nærheten av kilden for angrepet, og dette kan fortsette i en sirkel av forholdsregler, tiltak og mottiltak. Eksempelet med DoS-angrep er verdt å nevne for å påeke at alle store og avanserte systemer har sine svakheter, også i Kina. Dette landet har ved bruk av filtreringsteknikker skapt en effektiv kontroll over Internett. Likevel har Kina tatt et skritt videre til ”andregenerasjons filtreringsteknikker” som er demonstrert senere i kapittelet.

6.3.1.3 Teknisk filtrering og sosial filtrering

Kina skiller seg fra andre land når det gjelder filtrering på Internett ved at de er meget dynamiske i sine valg av nettsider som blir blokkert. En side som er tilgjengelig en dag kan være blokkert dagen etter. Mange av de store amerikanske mediesidene blir derimot ikke blokkert, som CNN, MSNBC og ABC, eller nettsteder som inneholder menneskerettigheter (Kina-ONI 2005). Ofte er de samme sidene mulig og aksessere ved samme tidspunkt utenfor Kina. Kina bruker et ukjent og dermed uforutsigbart filtreringsmønster som retningslinjer, hvor både DNS-manipulering, IP-blokkering og proxy-basert filtrering er i bruk. Et land som konstant skifter taktikk gjør at det blir vanskeligere å se hva som sensureres. Søkemotorene filtrerer innhold av nøkkelord og kan fjerne enkelte søkeresultater fra listen slik at brukere ikke engang får vite at de eksisterer. I tillegg returnerer Kinas filtrerte nettsider en nettverks ”timeout”. Dette er forskjellig fra andre land med streng Internett-politikk som heller returnerer en blokkert side, eller at siden ikke eksisterer (den kjente ”404 error”). Siden det ikke er noen spor etter at noe har blitt blokkert vil ikke nettsurfernes nysgjerrighet bli vekt i motsetning til hva en ”this page has been blocked” beskjed ville ha gjort. Det har blitt funnet tegn på nøkkelordsøk som er blitt blokkert av Kinas gateways og ikke av selve søkemotorene, det vil si at filtreringen skjer sentralt og ikke bare hos den enkelte ISP’en. Dermed vil hele landet oppleve den samme filtreringen hvis det er en internasjonal gateway. Det er også funnet tilfeller med at det blir gjort blokkering av bestemte URL’er mens selve toppdomenet til disse URL’ene fortsatt er tilgjengelig, dette bekrefter en nøye utvalgt form for filtrering som ofte betyr bruk av mennesker til å velge ut helt bestemte sider (Kina-ONI 2005).

Alle samfunn har sine egne regler for hva som er rett og galt, og Kina har en mengde reglementer, forskrifter og lover for sine innbyggere. De har regler for Internett-kafeer som sier at de må spare på informasjon om all bruk av Internett for de siste seksti dagene, i tilfelle noen har postet eller aksessert sensitive opplysninger. Dette fører til sosial filtrering ved at brukere hos Internett-kafeer sensurerer seg selv i frykt for å bli innrapportert. Sensitive temaer i Kina er politiske bevegelser, informasjon om kontroversielle statlige aksjoner som frigjør Tibet, kritisisme av Kinas menneskerettigheter, støtte av demokratiske styresett eller andre

former for vestlige tanker. Spesielt media må være forsiktig med hva de skriver med tanke på den påvirkningen de faktisk har på publikum. Det å være en journalist i Kina kan være en farlig jobb fordi journalister ofte blir straffet hvis de har skrivd noe ”upassende” myndighetene eller det offisielle kommunistpartiets doktrine ikke vil godkjenne. Journalister som setter spørsmålstegn ved partiets politikk risikerer å miste jobben siden kommunistpartiet ikke tolererer noe som helst kritikk av dem selv. Avstraffelser av journalister kan også skje i form av fabrikkerte bevis som fører til fengselsstraffer (Kina-ONI 2005). Med dette i tankene skapes det en form for sosial filtrering som fører til at mange journalister *sensurerer seg selv* i frykt for effektene av hva de skriver.

6.3.1.4 Tiananmen-massakren

Et eksempel på sensurering utført av myndighetene er omstendighetene rundt hva som kalles for ”Tiananamen-massakren”: Det hele startet med at en populær politiker blant studentene i Beijing sovnet stille inn. I kjølvannet av hva politikeren hadde kjempet for, med å få en bedre hverdag for folket, oppsto det studentdemonstrasjoner på Tiananmen-plassen i Beijing. De fleste deltagerne i demonstrasjonene var imot den autoritære og økonomiske politikken til det kinesiske kommunistpartiet, og det var ønske om en mer demokratisk styreform (Wikipedia 2008). Studentene slo seg ned på hva som i dag er kjent som ”Den himmelske fredsplass” og flyttet seg ikke på flere dager til myndighetene bestemte seg for å sende inn soldater som skulle drive dem bort. Dette resulterte i en blodig massakre som varte i fem dager fra 4. til 9. juni, 1989. De fleste har sett bildet av en ung student som står midt i veien foran en kolonne med tanks og som nekter å flytte seg. Bildet gikk verden rundt og har, sammen med datoen 4. juni 1989, blitt et symbol for opptøyene de fem dagene på Tiananmen-plassen.

Dette har blitt en av Kinas største tabusaker i nyere tid. Myndighetenes sensur av Tiananmen-massakren har vært effektiv til den grad at mange unge kinesere i dag ikke har fått vite om hva som foregikk. Det skyldes at mediene, inkludert Internett, ikke har lov til å skrive om det. Et utdrag fra en blogg på nettstedet ”Internet Censorship Explorer” skrevet av Adam Ehrlich, 21.april 2006 forteller om hans personlige erfaring med filtrering i Kina:

[…] If you log onto a computer in downtown Beijing and try to access a Web site hosted on a server in Chicago, your Internet browser sends out a request for that specific Web page. The request travels over one of the Chinese pipelines until it hits the routers at the border, where it is then examined. If the request is for a site that is on the government's blacklist — and there are lots of them — it won't get through. If the site isn't blocked wholesale, the routers then examine the words in the requested page's Internet address for blacklisted terms. If the address contains a word like "falun" or even a coded term like "198964" (which Chinese dissidents use to signify June 4, 1989, the date of the Tiananmen Square massacre), the router will block the signal. Back in the Internet cafe, your browser

will display an error message. The filters can be surprisingly sophisticated, allowing certain pages from a site to slip through while blocking others. While I sat at one Internet cafe in Beijing, the government's filters allowed me to surf the entertainment and sports pages of the BBC but not its news section. […]

Myndighetene har iverksatt en blanding av sosial selvsensurering og bruk av tekniske filtreringsmetoder for å skjule alle spor av "hendelser" som ikke passer inn med verdier de synes innbyggerne deres skal ha. At dette ikke har endret seg i dag illustreres med blokkeringen av Zilins nettside: En dame ved navn Ding Zilin mistet i 1989 sin 17 år gamle sønn, Jiang Jielian. Han og kameratene hans hadde møtt en gruppe demonstranter som var i konfrontasjon med soldater på vei til Tiananmen-plassen, og det endte med at han ble skutt i ryggen. Zilin og andre mødre som har mistet noen under denne massakren gikk sammen for å lage en nettside. De gjorde den klar til 19-års markeringen for massakren 4. juni 2008 for å gjøre historiene deres kjent via Internett. Med dette ønsket de å holde presset på myndighetene ved like, som aldri har gitt ofrene noen form for kompensasjon eller oppreisning[75]. Tiananmen-mødrenes hjemmeside *www.tiananmenmother.org* ble blokkert for kinesiske brukere etter tre timer på nettet (Rønneberg 2008).

Amerikanske organisasjoner som har prøvd å sette press på kinesiske myndigheter angående denne saken får støtte fra Bao Tong. Han var en høytstående tjenestemann i det kinesiske regjeringsapparatet i 1989, men måtte sitte åtte år i fengsel fordi han sympatiserte med demonstrantene. Til nyhetsbyrået Reuters sa han nylig at kinesiske myndigheter må lære av åpenheten de har vist etter jordskjelvet i Sichuan-provinsen, og at de må vise en tilsvarende åpenhet i forhold til det som skjedde 4. juni, 1989. Bao påpekte at dette var en menneskeskapt katastrofe, men i likhet med naturkatastrofer bør den bli kjent for alle kinesere og alle andre rundt om i verden.

Proxy-tjenerne i Kina blokkerer alle nettsider som inneholder noe om "Falun Gong" eller "198964" uten unntak. Likevel kan andre sider som også inneholder "sensitive temaer" være mulig å aksessere i forskjellige tidsperioder, noe som betyr at det er en dynamisk sensur som utføres fra myndighetenes side. Selv om Kinas filtreringssystem er meget avansert klarer det ikke å filtrere alt. For eksempel kan flere sensitive nøkkelord komme igjennom søkesystemene med noen få justeringer til hvordan de skrives. Kina har altså problemer med å innføre en total kontroll over Internett kun med tekniske filtreringsmetoder.

[75] Myndighetene har ennå ikke frigitt opplysninger om hvor mange som ble drept, arrestert eller på annen måte meldt savnet som en følge av massakren.

6.3.1.5 Jingjing, Chacha og Panopticon-effekten

Kombinasjonen av økende Internettbruk og mange innbyggere i Kina har ført til en ny tilnærming for å kunne holde følge med overvåkningen av Internett. *Panopticon* var opprinnelig navnet på et fengsel tegnet av Jeremy Bentham som levde på 1700-tallet (Cartome 2001). Arkitekturen var formet slik at cellene var plassert i en sirkel rundt bevoktningsrommet som var sentrum for bygningen. Ideen med fengselet var at ingen av fangene skulle kunne se fangevokteren, og dermed ikke vite om eller når de ble overvåket. På denne måten ville det bli en mental sperre for fangen å finne på noe, med vissheten om at kanskje han ble observert akkurat da. For å forsterke denne følelsen skulle fangen fra cellen alltid kunne se konturene av tårnet hvor fangevokteren var plassert, men selvfølgelig uten å kunne se selve personen i tårnet.

Kina har tatt Panopticon-effekten med seg til Internett, som et digitalt Panopticon. Før var Internett-historien til Kina å drive mest mulig teknisk filtrering, slik at myndighetene hele tiden hadde full kontroll på sine innbyggere. Med den hurtig økende bruken av Internett står Kina overfor et nytt problem. I likhet med resten av verden har massemediet Internett klart å oppnå en brukerskare som ikke lenger lar seg kontrollere like enkelt som for noen år tilbake. Med dets distribuerte struktur og lette tilgang til Internett er det allmenn tro om at dette vil være med på å styrke ytringsfriheten i Kina og andre land hvor slikt ikke har vært like lett før. Dette er likevel ikke tilfelle i praksis, for Kinas myndigheter har fortsatt god kontroll på hva folk bruker Internett til ved hjelp av Panopticon. Meningen bak Panopticon når det påføres Internett er at det oppfordrer til selvsensurering, og dette legger til rette for flere nye virkemidler. Et interessant spørsmål er: hvordan er det mulig å få mennesker til å føle at de blir overvåket hele tiden? En del av løsningen Kinas myndigheter har kommet fram til er de animerte politikonstablene Jingjing og Chacha. Politikonstablene er basert på automatiserte metoder som kan sikte seg ut individer på en effektiv måte. De ble synlige på Internett ved starten av 2006. Hvis en bruker kommer inn på en nettside, hvor domenet er under en ISP som har avtale med myndighetene om å bruke Jingjing og Chacha, kan en av dem plutselig dukke opp på skjermen med velmenende råd om nettikette som landet støtter, eller som Jingjings blogg sier (Kushner 2008):

"We will send kind reminders to people to establish online safety and to respect online laws and regulations by regulating themselves to create a healthy Internet circumstance and to maintain harmonious order"

Ifølge sjefen for Internett sikkerhet og overvåkning i den sørlige byen i Shenzhen, Chen Minli, er poenget med Jingjing og Chacha å la alle Internett-brukere vite at Internett ikke er et

sted utenfor loven. Videre sier han at Internett-politiet vil overholde lov og orden for alle deler av Internett.

Andre momenter for selvsensurering i Kina for å tydeliggjøre hvordan Panopticon slipper til, er meldingen direktøren for det kinesiske Internettprosjektet, Xian Qiang, sa alle universitets funksjonærene skulle sende ut til sine studenter (Kushner 2008):

"This weekend, public-security authorities will install security software on our system. You don't know how well it works or what it does, but you certainly know every student is being warned."

Om det ble installert noen sikkerhetsoppdateringer på systemene er ikke klart, men når trusselen om fengselsstraff ligger i bakhodet vil de fleste tenke seg om før de uttaler noe på nettet som kan utgjøre en fare når myndighetene leser det. Denne oppfordringen gikk til studenter, men mediafolk må være spesielt oppmerksomme på hva de velger å skrive om. Likevel, som en observatør kommenterte: selv om Kina setter flest journalister i fengsel i verden tar de på samme tid og skriver "manualen" for hvordan en kontrollerer pressen og innbyggere og dermed nasjonens kurs ved "bare" å fengsle et minimum av personer (Deibert, Palfrey et al. 2008).

6.3.1.6 Bruken av Internett

Tilfeller med razziaer på Internett-kafeer og fengsling av personer er sterke midler som støtter opp under selvsensureringen. I april 2001 satte Kina i gang en aksjon hvor 40 000 politifolk deltok i kampen mot uønsket innhold hvor over 56 800 Internett-kafeer ble oppsøkt. 6071 ble stengt, mens mange andre fikk installert spesielle overvåkningssystemer som skal skanne etter pornografi og kontroversiell informasjon. (Staksrud 2002).

Minst 8 personer ble dømt til fengselsstraff i 2006 for å ha brukt Internett til å distribuere informasjon myndighetene ikke vil vedkjennes. Fra 2005 og til 2007 økte antall Internett-brukere fra 94 millioner til 137 millioner. På landsbasis er det nå 10,5 prosent som bruker Internett, men dette tallet varierer fra provins til provins, spesielt fra storbyene til fattige områder. Dette tallet kan virke lite hvis en sammenligner med for eksempel siste tallene fra Norge hvor to av tre husstander har tilgang på bredbånd. Likevel er det høye tall det er snakk om siden det er 10.5 prosent av 1.4 millioner mennesker som bor i Kina (Deibert, Palfrey et al. 2008).

Kjønn og alder spiller en faktor i hvem som bruker Internett i Kina som andre steder. Tallene viser at 58,3 prosent av menn og 41,7 prosent av kvinner bruker Internett, og spesielt personer i alderen 18-24 år er blant de ivrigste brukerne. Denne aldersgruppen holder 35 prosent av alle brukere. Det er blitt en stor andel som bruker Internett fra hjemmene sine, hele 76 prosent, men 30 prosent bruker også Internettkafeer som hovedaksesspunkt.

Det har vært en eksplosiv utvikling ved spesielt bloggevirksomheten i Kina som nådde 20,8 millioner blogger ved slutten av 2006 (Deibert, Palfrey et al. 2008). Veksten av Internett i kombinasjon med den økende bruken av andre teknologier som SMS har vært med på å gi næring til hva som kan anses som et nytt fenomen i Kina, å ha en *offentlig mening*. På denne måten virker blogging i Kina som en motvekt mot Panopticon-selvsensuren.

Internettbrukere i Kina proklamerer at Internett er deres beste kilde for informasjon, og at det er viktigere enn både aviser og TV. I Kina brukes søkemaskiner mye, Bulletin Board Services (BBS), online spilling, blogging og e-handel. Kina har også det største antallet av Voice over Internet Protocol (VoIP) i verden. I et forsøk på å kontrollere bruken av VoIP blant innbyggerne bestemte kinesiske myndigheter at ingen lisenser for betalte datamaskin-til-telefon tjenester ville bli utgitt på to år. Dette ble gjort fordi de påsto at det ville bli betydelige finansielle tap for hovedselskapene for telekommunikasjon slik at bare China Netcom og China Telecom ble tillatt et prøveprosjekt av kommersiell VoIP tjenester i utvalgte byer (Deibert, Palfrey et al. 2008). Stadig nye reguleringer blir innført av myndighetene i et forsøk på å øke (eller i det minste beholde) kontrollen over brukerne på Internett, som med tilfellet av VoIP. Internett legger imidlertid til rette for flere måter å uttrykke seg på. Ivrige Internettbrukere går inn for å bli kjent med dem alle, som med bruk av blogging, i håp om å komme forbi reguleringene, blokkeringene og sensureringene.

6.3.1.7 Oppsummering

Kina har problemer med å kontrollere hele Internett (innenfor egne landegrenser) på grunn av at det er stor nettverkstrafikk og nærmere 140 millioner Internettbrukere. Derfor har de innført en skremselstaktikk som sier at ”storebror ser deg”, selv når dette ikke er tilfelle, for å skape en Panopticon-effekt som oppfordrer til selvsensurering. Tilfeller med razziaer på Internett-kafeer og fengsling av personer er også sterke midler for å støtte opp under selvsensureringen. Teknisk filtrering fungerer som førstegenerasjons filtreringssystem, mens andregenerasjon i praksis er en kombinasjon av teknisk og sosial filtrering. Brukere har imidlertid klart å finne ”smutthull” i form av bloggevirksomhet hvor de får uttrykt sin mening. På grunn av det store volumet av bloggere kan ikke myndighetene gjøre mer enn å ta stikkprøver. Dette viser at et land som praktiserer streng kontroll på Internett kan likevel ikke overvåke alle deler av nettet til alle tider når det har oppstått store nok skaleringer. Av alle land i verden er likevel Kina på toppen når det gjelder teknisk og sosial filtrering, og skiller seg fra andre land ved at de blant annet har en meget dynamisk filtrering ved at forskjellige nettsider blir blokkert fra dag til dag.

6.3.2 Internett og filtrering i Egypt

Egypt har fungert som en modell for mange utviklingsland med tanke på hvordan de har fått opp bruken av Internett. Deres ambisiøse Internett-prosjekt har vist seg vellykket og har gitt en kraftig vekst av Internett-bruken på kort tid. Egypt ønsker ikke å hindre bruken av Internett, men de vil derimot ha kontroll på hva brukerne foretar seg på Internett. På mange måter er Egypt i fase 1 der Kina kan sies å være i fase 2, der fase 1 tilsvarer tekniske filtreringsmetoder, og fase 2 er en blanding av teknisk og sosial filtrering. Likevel vises det tendenser til at også Egypt går i retningen Kina har valgt. Innholdet for dette delkapittelet er:

6.3.2.1 Bakgrunn: for Egypt om storbyenes bruk av Internett, styresettet og en begrenset ytringsfrihet.

6.3.2.2 Internett prosjekter i Egypt: har hjulpet egyptere til et bedre nivå på teknologi-kompetanse i forhold til sine naboland. Det beskrives hvordan myndighetene ønsker en konkurransedyktig nasjon i vår nye teknologiske tidsalder.

6.3.2.3 Filtrering og blogging i Egypt: beskriver hvordan innbyggernes versjon av ytringsfrihet er å ta i bruk blogging, og myndighetene som sensurerer alle sine massemedier svarer med å ta i bruk både teknisk og sosial filtrering.

6.3.2.4 Lover og reguleringer i Egypt: tar for seg ”Penal Code and the Emergency Law” som gir myndighetene rett til å begrense og overvåke kommunikasjon for sine innbyggere.

6.3.2.1 Bakgrunn

Republikken Egypt er Afrikas nest største land målt etter befolkning. De har over 80 millioner innbyggere hvor omtrent alle bor langs Nilen eller i Nildeltaet. Befolkningen i Egypt kan skilles etter hvor de bor, byene eller landsbygda, og etter religiøs tilhørighet med 95 prosent islamske og resten kristne (Wikipedia 2008). Hovedstaden er Kairo og har vært kjent for å være et senter for læring, kultur og handel i århundrer, den er også Afrikas største by. Myndighetene i Egypt eksperimenterer med WiMax teknologi som kan gi øde steder trådløs høykapasitets Internett-tilgang. Likevel, til tross for denne innsatsen foregår mesteparten av Egypts Internettbruk i de største byene; hovedstaden Kairo, Alexandria, Luxor, Port Said, Suez, Asyout, El Mansoura og El Zagazig.

Egypt har først nylig holdt presidentvalg med mer enn en kandidat. Flere politiske partier, blant dem det muslimske brorskapet, er forbudte, og opposisjonen beskylder regimet for valgfusk. I dag er Hosni Mubarak president, statsoverhode og øverste leder for landets militære styrker. Som president er det han som utnevner visepresidenten, statsministeren, regjeringen, og ti medlemmer av nasjonalforsamlingen, som i alt har 454 medlemmer og er et ettkammers parlament (Wikipedia 2008).

Ytringsfrihet for folk og presse har tradisjonelt sett hatt store begrensninger i Egypt, spesielt når det kommer til religion og politikk. Bloggere og menneskerettighets-organisasjoner benytter nå Internett til å spre sine budskap. I mange tilfeller har journalister kritisert myndighetene uten at det har fått følger, men det er unntak hvor myndighetene har overvåket kommunikasjonen på Internett, og i noen tilfeller har de forfulgt og arrestert folk for deres uttalelser på Internett (Deibert, Palfrey et al. 2008).

6.3.2.2 Internett prosjekter i Egypt

Egypt er et land hvor mesteparten av befolkningen ikke har råd til å kjøpe en personlig datamaskin eller å ha oppkobling til Internett som ble introdusert for egyptere i 1993. En ny datamaskin kan koste mer enn et års lønning og er dermed ikke en prioritert eiendel. I en verden hvor datamaskiner og Internett har blitt hverdagslige elementer, har til sammenligning Egypts befolkning liten tilgjengelighet til begge deler. Afrika har blitt karakterisert som kontinentet som *"suffers the most from … the digital divide in a world that has increasingly become wholly based on knowledge"*. Bare 0,7 prosent av Egypts innbyggere brukte Internett i år 2000, men tallet steg til syv prosent i 2006. Med dette har Egypt en betydelig større mengde brukere enn Afrika generelt, hvor bare 3,6 prosent av befolkningen brukte Internett i 2006. En slik merkbar økning av brukere viser at Egypt har kommet inn på et nytt spor hvor myndighetene går inn for at informasjonsteknologi-kompetansen skal økes blant befolkningen. Av mangel på personlige datamaskiner bruker de fleste Internett via Internett-kafeer, oppringingstjenester eller mobile tjenester. Dette betyr at skolene ikke har bidratt med veksten av brukere, mye på grunn av at myndighetene i utviklingsland ofte mangler ressurser til å utstyre utdanningsinstitusjoner med teknologi (Ford 2007).

Myndighetene i Egypt har bidratt med å få Internett ut til folket med sitt "Free Internet Program" som tillater alle egyptere med datamaskin, et modem og en telefonlinje å få tilgang på Internett til samme pris som en lokal telefonsamtale. I 2004 bidro også "PC for Every Home" ytterligere med å øke Internett-bruken da de tilbød billige datamaskiner til 120.000 innbyggere. Dette var mulig takket være en kombinasjon av lavpriset maskinvare og finansiering fra myndighetene. Egypt ønsker at innbyggerne sine skal ha tilgang på ny teknologi som datamaskiner og Internett på grunn av nytteverdien det vil bringe til samfunnet i den videre utviklingen (Deibert, Palfrey et al. 2008).

I 2005 det var kjent at sider som inneholdt informasjon om det muslimske brorskapet ble blokkert i Egypt. For eksempel ble den offisielle siden *www.ikhwanonline.com* blokkert av samtlige ISP'er i landet. Likevel, da ONI gjorde en undersøkelse av Egypt i 2006 fant forskningsgruppen ingen spor av at det foregikk Internett-filtrering av politiske eller sosiale temaer i landet. Derimot kunne bloggene fortelle mer om sensurering, forfølgelse og fengselsstraffer som gjør at Internett-brukere må vurdere selvsensurering før de poster innlegg

med ”sensitive” opplysninger. Neste avsnitt demonsterer at Egypt i likhet med Kina utfører sosial filtrering, og landet viser tegn til at dette vil øke etter hvert som Internett-bruken øker.

6.3.2.3 Filtrering og blogging i Egypt

Myndighetene i Egypt lar ikke kritikk mot autoritetene i landet passere i noen av sine massemedier. I følgende eksempel demonstreres det hvordan det først brukes teknisk filtrering, og deretter sosial filtrering på en blogger ved navn Hala Helmy Botros som kritiserte myndighetene på Internett:

Botros er en 43 år gammel dame som skrev under pseudonymet Hala el-Masry. Bloggen som skapte oppsikt het *”Aqbat Bela Hodood”* som oversatt til norsk betyr ”koptere uten grenser”. I bloggen ble det antydet hvordan politikere og politiet hadde samarbeidet om et angrep på kristne, koptiske minoriteter som holdt til i en landsby nærme Luxor. Kopterne hadde prøvd å gjenoppbygge en kirke, men fikk isteden flere hus brent ned i tillegg til at kirken ble fullstendig ødelagt. Det endte med at to koptere ble drept, og flere ble skadet. Botros ønsket å fortelle om skjebnen til den koptiske minoriteten, siden temaer mellom kristne og muslimske ikke blir tatt opp i massemedier som aviser og tv. Antagelig har bloggen hennes skapt stor irritasjon hos myndighetene, for det neste som skjedde var en målsiktet, teknisk filtrering mot Botros fra telekom- og ISP-selskapene. Først mistet hun tilgang til telefonlinjene, og deretter ble Internett-forbindelsen brutt. Botros fant imidlertid en slik krenkelse av ytringsfriheten uakseptabelt. Hennes måte å omgå den tekniske filtreringen på var å bruke Internett-forbindelsen hos sin far, slik at hun kunne fortsette å skrive bloggen sin. Imidlertid var hun også blitt satt under overvåkning, og en natt ble hennes far banket opp av to fremmede som lot han få vite det var på grunn av datterens uttalelser. I ettertid har Botros lagt ned bloggen sin fordi hun fryktet for sin egen og familiens sikkerhet. Før hun gikk til dette skrittet prøvde faren å gå til politiet for å anmelde forholdet. Politiet ga ham et blankt ark han skulle signere, for deretter å legge til at han anklaget sin datter for å være ansvarlig for overfallet. Botros ble arrestert og anklaget for at hun planla å ta livet av faren sin. Kort tid etter at hun prøvde å fly til USA for å være med på en konferanse som handlet om koptiske minoriteter i Newark, New Jersey (hvor politifolk kom om bord og tvang henne av flyet før avgang), ble hun arrestert igjen. Denne gangen ble hun anklaget for å spre falske nyheter og forstyrre harmonien mellom muslimske og kristne samfunn, og for å undergrave det nasjonale samholdet. Etter at Botros la ned bloggen har hun blitt utsatt for teknisk filtrering i form av avlytting av telefonlinjen, og overvåkning av e-poster hun mottar og sender (RSF 2006).

Myndighetene er altså i stand til å ta i bruk sterke midler for å hindre at negative vinklinger angående styresett og religion blir fortalt videre. Det ble først tatt i bruk teknisk filtrering ved å kutte Botros nettaksess, og deretter ble hun utsatt for sosial filtrering i form av streng oppfordring til selvsensurering etter rekken med hendelser beskrevet over. I 2006 var

det bare 3.78 prosent av befolkningen som hadde personlige datamaskiner. De fleste brukere får aksess til Internett via en av de 400 Internett-kafeene, via en mobil Internett-enhet, eller gjennom en av de 1300 offentlige informasjonsteknologiske klubbene. Disse klubbene tillater brukerne å aksessere Internett for en liten avgift som medfører at de må registrere seg hos Ministry of Communication og at de oppholder seg i offentlige bygninger slik som skoler (Deibert, Palfrey et al. 2008). I likhet med mange andre innbyggere i Egypt benyttet også Botros seg innimellom av Internett-kafeer for å skrive bloggene. På grunn av at hun hadde postet flere av sine blogger fra to kafeer, ble de stengt av myndighetene. Det er saker som denne som er med på å skremme andre som har Internett-kafeer. Selv om kaféeierne ikke ønsker å overvåke kundene sine, vil de heller ikke havne i en situasjon hvor de må legge ned arbeidsstedet og levebrødet deres. Derfor føyer de fleste seg etter myndighetenes restriksjoner. Dette betyr i praksis at alle Internett-kafeer må gi daglige rapporter om hva kundene deres foretar seg på Internett (RSF 2008).

Eksempelet med Botros blogg er ikke unikt i Egypt. I februar 2008 ble 22 år gamle Abdel Karim Nabil Suleiman (alias Kareem Amer) den første til å bli dømt for blogging, og med sine fire år fikk han den lengste fengselsstraffen som en kan få for slike aktiviteter på Internett. Suleiman ble dømt for å ha fornærmet president Mubarak, og for å skrive negativt om islam (Kushner 2008). Han oppfordret blant annet til at arabiske og muslimske kvinner ikke skulle bli diskriminert. Bloggen hans var ikke så forskjellig fra de hundrevis av andre bloggene skrevet av landets unge befolkning som protesterer mot landets styresett og gamle tradisjoner. Siden februar har Suleiman blitt en populær figur og et symbol for online undertrykking for resten av landets bloggere.

Landet kan se ut til å begynne å gå i Kinas fotspor med å utvide sine filtreringsmetoder over i sosial retning. Et eksempel på dette er hva som hendte med bloggeren Wael Abbas som holder til i Kairo. Han er kjent for å poste innhold som kritiserer president Mubarak, som blant annet inkluderer videoer med torturscener utført av politiet (Kushner 2008). En slik video som viste hvordan fanger i et fengsel ble torturert førte til at to politifolk ble arrestert og sendt i fengsel selv. Abbas var klar over at han risikerte overvåkning og straffeforfølgelse fra sine egne myndigheter ved å poste slike videoer, men noe overraskende ble hans YouTube-konto en dag sperret av YouTube. En mengde brukere hadde over en kort periode klaget over innholdet han lastet opp. Spørsmålet ble hvem disse brukerne var. Abbas trodde heller det var myndighetene i Egypt enn at andre brukere på YouTube hadde klaget. Det endte med at YouTube åpnet kontoen til Abbas igjen etter at han hadde overbevist dem om at han var en målskive for myndighetene i landet hans. Etter dette begynte det å sirkulere anonyme, falske utsagn om at Abbas hadde skiftet religion tre ganger, fra protestant til ortodoks til katolikk, og at han var homofil. I et konservativt samfunn hvor homofili fortsatt er tabu å snakke åpent

om, og hvor rotering av religioner blir sett på med forakt, gjorde ikke dette ting enklere for Abbas. Slik fokusering på et bestemt individ fra ukjente bakmenn, men hvor myndighetene vinner på det, kan sees på som en oppmuntring til selvsensurering. I så tilfelle har også Egypt tatt skrittet over til sosial filtrering i tillegg til den allerede eksisterende tekniske filtreringen.

6.3.2.4 Lover og reguleringer i Egypt

Internett har gjort det mulig for journalister og bloggere å skrive om alt som ikke kan nevnes i tradisjonelle massemedier. Myndighetene har i mange tilfeller vist en lav terskel for å iverksette fysisk overvåkning av bloggere som skriver kritiske innlegg. Bloggere i Egypt vet riskene hvis de skriver noe kritisk, og at det kan få konsekvenser som ofte fører til at bloggene legges ned. Det er ingen lover som kan hjelpe eierne til blokkerte nettsider, tvert imot er loven i aller høyeste grad på myndighetenes side med ”Penal Code and the Emergency Law”. Denne loven tillater myndighetene å begrense og overvåke kommunikasjon, som å arrestere personer uten å tiltale dem og la være å føre dem for retten på ubestemt tid. Loven tillater også sensurering, konfiskering eller å legge ned alle publikasjoner, inkludert innhold på Internett, som MII ønsker (Deibert, Palfrey et al. 2008). I praksis betyr dette at myndighetene kan filtrere og blokkere alt de finner støtende på Internett, uten å trenge å gi nærmere forklaring i rettslig forstand. Loven har blitt fornyet av presidenten Mubarak hvert tredje år, fra 1981 og til i dag. I tillegg skrev han under på Egypts ”presselov” i 2006 som sier at journalister skal kunne fengsles hvis de kritiserer presidenten eller utenlandske ledere, eller ”sprer falske nyheter”.

6.3.2.5 Oppsummering

Egypt er et land hvor det satses på teknologi. Myndighetene har oppfattet hvor viktig det er å ha et visst nivå på blant annet datakunnskap blant sine innbyggere, hvis dem skal kunne bidra i den videre utviklingen til samfunnet. Likevel blir det i det skjulte foretatt omfattende sensurering av politisk og religiøst innhold, både ved bruk av tekniske filtreringsmetoder og ved en stadig økende bruk av sosial filtrering. Dette gjelder spesielt bruk av blogging som er egypteres kommunikasjonsmiddel for å kunne uttrykke sine meninger, og slippe unna den strenge sensuren i de tradisjonelle massemediene. Av mangel på personlige datamaskiner bruker mange egyptere Internett via Internett-kafeer. Eierne av Internett-kafeene jobber under strenge reguleringer fra myndighetene, og må oppgi daglige rapporter over hva kundene benytter Internett til. Lovverket i Egypt gir myndighetene rett til å drive en streng kontroll, sensur og eventuell konfiskering av publikasjoner for alle sine massemedier, inkludert Internett. Egypt som fortsatt er i startfasen av å introdusere Internett til befolkningen viser med dette tendenser til å gå i Kinas fotspor ved bruk av filtrering.

"Global communication with local trust"
David Clark

7 Analyse og diskusjon

De fem første kapitlene i denne oppgaven presenterte bakgrunn og teori knyttet opp mot casestudiene i kapittel 6. De empiriske datasettene som ble presentert i casestudiene beskrev bruksområder til filtrering og situasjonsbetingede faktorer som hvordan filtreringen applikeres. Ved å gjøre dette er det bare implikert den nåværende tilstanden filtrering har på Internett. Dette kapittelet vil dukke dypere ned i funnene ved blant annet å bruke teorien fra kapittel 3. Målet er å få en rikere innsikt for å kunne svare på forskningsspørsmålet som ble lagt fram innledningsvis i oppgaven:

Har filtrering en konkret påvirkning på hvordan den globale infrastrukturen til Internett utvikles videre, og hvordan brukes filtreringsmetodene i praksis for individer, private aktører og myndigheter i forskjellige land?

Dette spørsmålet har fungert som retningslinje for de tre hypotesene som ble utledet i kapittel tre basert på tidligere forskning for dette området:

(1) Selv om formålet med filtrering er å få mer kontroll bidrar det til en mer komplisert nettverksstruktur og er med på å skade generativiten for Internett.
(2) Internett er fritt for alle, e2e-arkitekturen gjør at tredjeparter ikke kan avskjære kommunikasjonen mellom endepunktene og verner om integriteten i nettverket.
(3) Filtreringsapplikasjonene fortsetter å utvikle seg fordi de kan, ikke fordi de må på grunn av etterspørsel. Teknologien/ingeniørene styrer brukerne og ikke motsatt.

7.1 Diskusjon fra casestudiene

Internett kan manipuleres, det være seg fra individers kriminelle handlinger som ID-tyveri og oppfanging av kontonummer til nettbanker, til hvordan myndigheter i mange land kontrollerer hva innbyggere får tilgang til. De neste avsnittene diskuterer casene én etter én.

7.1.1 Case 1

Case 1 beskriver hvordan filtreringsmetoder kan brukes i uredelige hensikter, som for eksempel når DNS-manipulering benyttes til å lure brukere inn på korrupte nettsider. Mottiltak i form av kommersielle filtreringsprogrammer, som for eksempel antiphishing, antivirus og brannmurer, kan hjelpe mot slike angrep. Kommersielle firmaer har kommet langt i utviklingen av programvare som benytter seg av filtreringsmekanismer. Dette bringer oss tilbake til problemstillingene nevnt i kapittel 2 angående over- og underblokkering. De største utfordringene ved bruk av filtre er å stille dem inn riktig. En løsning kan være å bruke innholdsfiltrering og sette opp alle nettsteder som ikke tilfredsstiller kravene (gjerne bedømt etter kategorier som for eksempel PICS) på sortelister. De som utvikler disse listene er nøye med å holde dem hemmelig fordi det koster mye tid og ressurser på å generere slike lister, i tillegg til å stadig måtte holde dem ved like.

Ved å bruke Internett risikerer vi å laste ned ondsinnete programmer som kan gjøre skade, enten ved å ødelegge filer på datamaskinen, eller ved å fange opp personlig informasjon om oss. Ordet ”sikkerhet” i forbindelse med datateknologi er ikke lenger begrenset til å gjelde datamaskiner og systemer, men omfatter nå også sikkerhet av informasjon. Dette gjelder ikke bare det å beskytte informasjon på private datamaskiner. Personvernet vårt kan stå i fare for å bli skadet av at det også er for dårlig sikkerhet rundt samordning av databaser som inneholder informasjon om oss. Slike databaser blir bygget blant annet ved innsamling av opplysninger om hva vi foretar oss på Internett til daglig. Hvis det er kommersielle firmaer som står bak innsamlingen, blir informasjonen gjerne solgt videre til andre aktører i prosessen med å tjene penger. Ved bruk av filtreringsmetoder kan slike opplysinger komme på avveie. Det har vist seg å være en utfordring å gjøre folk oppmerksomme på hvor lett lekkasjer kan skje, fra private opplysninger til bedriftsrelatert informasjon. Alle systemer vil mest sannsynlig ha en eller annen form for svakhet bare en ser nøye nok. Dersom datakyndige folk, som det etter hvert har blitt mange av, går inn for å utnytte sikkerhetshullene, kan det føre til store skader på systemet.

Case 1 viser at programvaren har kommet langt, og at teknologien er tilgjengelig for ”alle”. Økende sikkerhet vil kunne hjelpe mot uønsket spredning av informasjon hvis en tenker på at prinsippet bak sikkerhet ikke er å lage vanntette systemer, men heller å sørge for at tilgangen til sensitive opplysninger skal være vanskeligst mulig. Det ble demonstrert at tekniske filtreringsmetoder både kan misbrukes og være en nyttig tjeneste. Utfallet bestemmes gjerne av hvem som tar metodene i bruk av uærlige og ærlige individuelle og i hvilken hensikt filtreringen utføres. Hvis det er med tanke på å sikre sine egne eiendeler som en datamaskin og bruk av nettjenester for eksempel betale regninger, skrive innlegg og sende e-post, kan

filtreringsteknikker være en stor hjelp til å sikre brukeren. Det brukeren sikres mot kan være korrupte nettsider som inneholder malware i form av tastaturloggingsprogrammer, virus, ormer eller e-poster med trojanske hester. Felles for slike faremomenter er gjerne at de har blitt laget av kriminelle individer som er ute etter å få en økonomisk gevinst, eller det kan være et ønske om å plage en bruker av personlige grunner. Når det gjelder organisert kriminalitet på Internett vises dette vanligvis i "større format", for eksempel et nettsted som inneholder tusenvis av brukernavn, passord og lignende sensitive opplysninger til andre nettsteder og selskaper. Dette er nettmarkeder som driver med salg av sensitiv informasjon til andre uærlige personer.

Filtrering er en sentral del i det å skape kontroll over nettverkstrafikken. Teknologien bak programmene på markedet i dag har blitt avansert nok til at også statlige avdelinger velger å bruke dem, noe som tar oss over på case 2.

7.1.2 Case 2

Felles for alle land i dag er at det er ønskelig med en viss form for kontroll over hva innbyggere foretar seg på Internett. Grunnene til et slikt ønske varierer med hvilke lokale verdier som er viktig. I noen land er drivkraften at det er ønskelig å skjerme sine innbyggere for bestemt innhold som finnes på Internett, fordi dette oppfattes som informasjon som vil gjøre mer skade enn godt. Denne casen bringer oss inn på et gjennomgående tema av hemmeligholdelse og mangel på åpenhet og gjennomskinnelighet[76]. Myndigheters rutiner og bruk av programmer for å overvåke Internett går under klassifisert innhold. Likevel har det blitt offentliggjort enkelte rapporter etter press fra organisasjoner som jobber for personvern og ytringsfrihet. USA har to kjente prosjekter som har fått mye kritikk, Carnivore[77] og ECHELON. Målet med disse er å spore opp og bekjempe kriminalitet på Internett, men midlene som brukes i denne kampen er verdt en nærmere analyse. Carnivore måtte følge et sett med lover og regler, og var under stadig oppsyn, i motsetning til ECHELON. Det er kun sikkerhetsklarerte som kan se Comint-rapporter og bare de som kan sette krav og kontrollere arbeidsoppgavene. Med dette dukker det opp et spørsmål; hvem kontrollerer kontrollørene? Tidligere ansatte ved ECHELON-prosjektet har gitt uttrykk for viktigheten av arbeidet ved at det gjør etterretning sikrere, og at det dermed er behov for en slik tjeneste. Framgangsmåten er først og fremst bruk av tekniske filtreringsmetoder, og ikke sosial filtrering. For å oppnå best mulig filtrering brukes det en kombinasjon av maskiner og mennesker for både analyse-

[76] Ordet "gjennomskinnelighet" vil i denne oppgaven bli brukt i betydningen av *å ha innsyn i* noe, som i hvordan et system fungerer.

[77] Carnivore brukes som fellesbetegnelse for FBI's system i denne diskusjonsdelen, da systemet ble mest kjent under dette navnet.

og prosesseringstrinnene. Problemet oppstår når uskyldige mennesker blir fanget opp av automatikken, og den menneskelige faktoren av etterretningsarbeidere ikke klarer å se nyansene. På samme måte som med case 1 har også case 2 en nøkkelfaktor i form av databaser. Med ECHELON-systemet hentes det inn enorme mengder informasjon fra Internett som analyseres og lagres i databaser. Av og til vil det gå galt, og kritikken her er at det ikke har blitt laget noe sikkerhetsnett for mennesker som urettmessig blir fanget opp av systemet og plassert på "terrorlistene". En slik mangel på tilpasningsdyktighet ved å kunne endre opplysninger i ettertid antyder at det er lite fleksibilitet i systemet.

7.1.3 Case 3

Lokale verdier påvirker hvordan forskjellige land velger å håndheve kontrollen på Internett. Case 3 har vist hvordan land med streng Internett-politikk har valgt å styre brukere ved en blanding av tekniske og sosiale filtreringsmetoder. Felles for land som Egypt og Kina er at de begge fører en streng overvåkning av det nye massemediet Internett, og de må ta i bruk utradisjonelle midler for å kunne henge med. I Kina har de valgt å bruke makten ved innbildning ved siden av de gamle tekniske filtreringsmetodene. Det som skiller Egypt og Kina kom fram ved observasjon av noen uttrykk som stadig dukket opp på blogger. De kinesiske bloggene omhandlet ikke selve overvåkningen, men myndighetenes advarsler om overvåkningen deres. I Kina har de ikke lenger skikken med å holde det skjult, folket skal få vite at de blir overvåket og at det vil bli konsekvenser for de som tråkker på den "nasjonale lojaliteten". Overvåkningen i Kina har et problem ved at det er et stort antall brukere på Internett, og med dette har de valgt en ny retning for deres filtreringsprosess. Kina utnytter faktumet at det er lettere å skremme brukere til lydighet, enn faktisk å måtte filtrere absolutt hele nettverket.

I Egypt har de ikke kommet til dette stadiet, men de er der Kina var noen år tilbake. Det er ingen åpenbare advarsler eller formaninger som de kinesisk-animerte Jingjing og Chacha, men det er derimot spor som viser at flere ISP'er bruker teknisk blokkering mot sider med politisk innhold fra tid til annen. Egypt lar sine innbyggere bruke Internett relativt fritt, og oppfordrer faktisk til det med sine prosjekter for å bygge opp bruken. Samtidig fører de overvåkning med hva brukere foretar seg på Internett, og har ved flere tilfeller fulgt opp med sanksjoner, fengselsstraffer eller trusler om det. Spesielt folk som skriver blogger i Egypt har følt at de har blitt forfulgt og fått problemer hvis de har skrivd noe kritiserende mot deres egen regjering.

I det hele tatt har casestudiene vist at filtreringsteknologi er meget effektivt for å innføre en viss form for kontroll i (mindre) subnettverk av Internett. Samtidig kommer filtreringsteknologi til kort når det gjøres forsøk på å kontrollere store deler av Internett som

hele land. Kina har lagt inn store ressurser i form av teknologi og menneskelig arbeidskraft i et forsøk på å innføre kontroll over hele Internett. Imidlertid har selv Kina måttet erkjenne at Internett er meget stort og med mange muligheter, og alle deler lar seg ikke kontrollere hele tiden. Selv om Kina har klart å lage et svært presist filtreringssystem, som går for å være blant et av verdens mest avanserte, er det altså ikke perfekt. Dette skyldes også at filtreringsmekanismer kan omgås med metoder som av og til ikke engang krever avanserte datakunnskaper, som å gjøre små justeringer på blokkerte søkeord slik at ordene likevel kommer igjennom søkesystemene og viser ønskede resultater.

En observatør nevnte at myndighetene i Kina stiller seg annerledes til naturkatastrofer enn til menneskeskapte katastrofer (Rønneberg 2008). Selv om jordskjelvet 12. mai 2008 tok livet av over 68.000 mennesker, håndterte de det med en ressurssterk redningsiver (Bjørnås 2008), uten at det ble gjort forsøk på å sensurere informasjon rundt katastrofen. På den andre siden er Tiananmen-massakren 4. juni 1989 blitt et tabubelagt tema som blir sensurert fortløpende på Internett så snart myndighetene finner noe om det. Kina utfører altså fortsatt massiv teknisk filtrering, men de er i tillegg kommet inn på denne nye stien av sosial filtrering som kan sees som en slags form for masseutsending av propaganda. Sosial filtrering er derfor ingen presis teknologi.

Case 3 viser også at det har blitt en økende geografisk avgrensning av Internett, selv om Internett i seg selv ikke følger landegrenser (Villeneuve 2005). Filtrering utført av individuelle brukere beholder et visst nivå av valg og kontroll, men innholdsfiltrering på Internett på nasjonalt nivå blir tvunget på hele befolkninger, ofte med lite pålitelighet.

7.2 Sammenlikning

Mangel på gjennomskinnelighet og åpenhet går igjen i alle casene. Case 1 viser at det er stor hemmelighet mellom kommersielle aktører rundt listene deres, siden disse koster tid, ressurser og penger å lage. Det blir samlet inn informasjon om brukere, og informasjonen utveksles mellom aktører med formål å tjene penger. Case 2 og case 3 omhandler filtreringsmekanismer styrt av etterretningstjenester og myndigheter, og det sier seg selv at de må holde et høyt nivå. I dag fins det programvare som kan gå gjennom opplysninger, gjenkjenne mønstre og sette opp analyser for å avsløre spor som går igjen. De elektroniske sporene dekker e-post, økonomiske transaksjoner, forsikring, eiendomsforhold og mye annet. Sporene samles inn og det lages profiler med formål å drive overvåkning (eller kommersiell handel), men som nevnt mangler det sikkerhetsnett for uskyldige mennesker som kan ende opp med en ”mistenkelig” profil. Denne problemstillingen går også igjen i den første casen, med den nye dataloven som gir rett til å lagre trafikkdata for å sette opp profiler. Felles for

liste- og databasebruken er at ingen vet hvem som er på dem, hva kriteriene er for å føye noen til dem, eller om det gjøres noe for å rette opp eventuelle feil.

Både case 2 og case 3 viser at det er lite oppsyn med aktivitetene som foretas når det er myndighetene som står bak overvåkningen. ECHELON blir ikke kontrollert av andre enn NSA, som drifter systemet, antagelig med en mindre påvirkning fra andrepartslandene. Case 3 viser at det ikke er mye innbyggere skal ha sagt når myndigheter i et land først går inn for å sensurere, blokkere og filtrere Internett med alle midler de har til rådighet. Ofte er det ønskelig å skjule at det skjer en filtrering, som en kontrast til case 1 hvor den kommersielle siden tenker mer på nytteområdet brukeren kan ha av filtrering.

Case 2 viser at land implementerer filtrering på nasjonale nivå i forsøk på å oppnå kontroll over hvordan Internett brukes. Når det gjelder nasjonal filtrering brukes det ”usynlige” filtreringsmetoder for å oppnå sensur, regulering eller blokkering av Internett. Case 2 og 3 kan sees under ett med at de begge går inn for å oppnå kontroll over hele land. Case 2 tok for seg myndigheter, spesielt USA, siden det har blitt utgitt offentlige rapporter om hvordan noen av deres filtreringssystemer som Carnivore fungerer. Selv om case 3 har den samme vinklingen, med myndigheter som til en viss grad overvåker innbyggere, fokuserte denne casen mer på å utøve kontroll over innbyggernes bruk av Internett, og effektene av dette.

Det er mulig å bruke alle typer filtrering for alle områder, men noen typer vil utpeke seg til å passe bedre for gitte situasjoner. Valg av filtreringsmetode er altså situasjonsavhengig. DNS-manipulering er den vanligste tekniske filtreringsmetoden å bruke med formålet å få brukere inn på falske sider. Proxy-basert filtrering blir også brukt til misbruk i form av avskjæring av kommunikasjon fra brukere til tjenermaskiner. Case 3 ga eksempler på at det foregår mye sosial filtrering i kombinasjon med teknisk filtrering (typisk IP-blokkering).

Programvaren i dag gjør at alle kan bruke filtrering, men spesielt bedrifter kan ha nytte av de mest avanserte filtreringsprogrammene som gjør nettverksanalyse, for eksempel for å analysere nettrafikken til ansatte. Case 2 tok for seg regjeringsstyrte filtreringssystemer, og case 3 viste den samme bruken fra myndigheter, dog fra en annen vinkel. I hovedsak kan alle bruke filtrering også til den grad at det kan påføres andre, selv om dette ikke skulle være ønskelig fra den andre parten.

Den siste sammenligningen som skal gjøres er dragkampen, eller spenningen, mellom de forskjellige aktørene som er omhandlet i casestudiene:

- Individer som sender ut virus, ormer, trojanske hester, spamming og lignende programmer, og individer (og/eller bedrifter) som unngår slike programmer gjennom sikkerhetsforanstaltninger som filtreringsprogrammer.
- Kommersielle aktører som er ute etter kunder, og kunder som oppgir falske e-poster for å ivareta anonymiteten.
- Land som samarbeider med hverandre, og land som ikke gjør det
- De som vil påføre kontrollen, og de som vil unnvike kontrollen.
- De som vil begrense tilgang til bestemt innhold, og de som vil aksessere det.

Casestudiene har demonstrert at denne striden mellom forskjellige aktører ikke har én vinner, men at det er en vekslende balansegang mellom partene.

7.3 Problemstillinger ved bruk av filtrering

Kapittel 2 tok for seg de mest vanlige problemstillingene ved filtrering, mens her settes det fokus på andre problemstillinger som dukket opp gjennom arbeidet med casestudiene. Det har som nevnt vist seg å være store feiltreff ved automatiske identifiseringer av personer som havner på svarte- eller terrorlister. Problemet for uskyldige personer er at det er vanskelig å komme av listen igjen. Problemene blir tydelige å se når det går utover egenskapene som gjennomskinnelighet, åpenhet og pålitelighet. Vi må *stole* på at filtreringskriteriene er satt riktig, men casestudiene viser at dette er alt annet enn sannheten i mange tilfeller.

Filtrering blir ofte sett på som en ”teknisk fix” til utfordringene som den raske utvidelsen av Internett gir. Svakheter med filtrering, og innholdsfiltrering især, er over- og underblokkering. For å blokkere innhold må spesifikke nettsteder bli identifisert før blokkering skjer. På grunn av den økende informasjonsmengden på Internett vil det alltid være noen nettsteder som ikke blir blokkert – selv om de oppfyller blokkeringskravene satt av det gjeldende filtreringsprogrammet. Dette betyr at det ofte vil være innhold tilgjengelig som ligner på det blokkerte innholdet. Det er mange muligheter for de som går inn for å oppsøke filtrert innhold, noe som til tider gjør bruk av filtrering vanskelig.

Et gjennomgående spørsmål i oppgaven har vært: hvor sikkert er det vi foretar oss på Internett? Det vi leser kan ha blitt redigert og sensurert til å bli hva andre mener er ”passende” innhold for oss, slik at det opprinnelige budskapet ikke lenger kommer fram. Blokkeringskriterier blir sjelden offentliggjort, og dette gjør det vanskelig å vite hvor grensene settes.

7.4 Internetts fleksibilitet

Kapittel 3 omtalte flere implementasjoner i e2e-arkitekturen til Internett. Flere av disse applikasjonene viser seg å gjøre stor nytte for brukere av Internett. Casestudiene har spesielt påpekt filtreringens rolle for disse applikasjonene, og hvilke fordeler og ulemper disse bringer. Et større spørsmål blir effektene slike applikasjoner vil ha på Internett over tid. At Internett er en vellykket struktur blir bevist av hvor mange som velger å bruke tjenesten. Den har, for å nevne noen bruksområder, åpnet en helt ny verden av e-handel og sosiale virtuelle miljøer. Kritikken mot en utvikling i samme spor går på at generativiteten til Internett kan bli skadet av "lettvint" bruk av midlertidige "fixer" i form av applikasjoner i nettverkskjernen. Det finnes alternative løsninger som ikke ville krevd slike implementeringer, men disse betyr ofte mer tid og penger - to stikkord som gjør at spesielt kommersielle aktører velger å ignorere slik kritikk. Noen spørsmål er: vil vi brenne oss på en slik utvikling om for eksempel 15 år? Hvor fritt vil det være å bruke Internett da? Vil det være mye infiltrasjon av suspekt programvare i nettverkskjernen, slik at ingen lenger kan være sikre på om det foregår ekte e2e-kommunikasjon? Internett vil ha mistet sin integritet hvis dette blir en realitet, og hypotese (2) vil ikke være riktig.

Det virker urealistisk at applikasjonene som allerede er implementert i nettverket vil bli fjernet, siden de nå har oppnådd bruksverdi. Flere har blitt nevnt; streaming av lyd og video og lignende tjenester som e2e-utviklere fra 1960-årene ikke hadde forutsetninger til å spå at ville bli nødvendig. En mulig utvikling vil være om applikasjoner altså finnes i nettverkskjernen, men med alternative måter for å sikre integriteten til Internett. Som nevnt i kapittel 3 vil økende integrasjon ofte gi økende kompleksitet, og et ønske om å skape mer kontroll kan slå tilbake i form av at en mister oversikten over II'en, og dermed ender opp med mindre kontroll. Likevel, med casestudiene i denne oppgaven har det blitt vist at filtrering har kommet langt i å skape kontroll. Faktisk er det svært få områder av Internett som ikke kan bli kontrollert når det først settes fokus på dem, hvis en antar at flertallet av brukere ikke vet hvordan filtrering kan omgås. Problemet er å ha en kontroll over absolutt hele nettverket for alt som skjer hele tiden. Dette er ikke mulig å oppnå slik det ser ut i dag, og vil antagelig heller ikke være det om for eksempel 15 år[78]. Men er en slik kontroll nødvendig eller ønskelig å skape? Å få til en slik kontroll kan sies å være en del av målet i case 2 og 3, men dette var sett fra myndighetenes side, og ikke fra folkets. Antagelig vil de fleste innbyggere i alle land sette pris på at ikke alt kan overvåkes, akkurat som vi setter pris på at ingen på forhånd har åpnet og lest brevene vi får i postkassen.

[78] Selv med stadig bedre filtreringsmetoder vil det likevel være en tilsvarende økende informasjonsmengde som skal filtreres.

Filtreringsapplikasjoner i nettverkskjernen bryter med e2e-prinsippene, men samtidig er de på enkelte måter med på å øke programmerbarheten til terminalene. Et synspunkt er at konseptet generativitet til en stor grad kan bli sett på som summen av e2e *og* programmerbarheten til terminalene, slik at tjenestene som nettverket tilbyr også vil ha en slagkraft og vil tilby noe til fleksibiliteten (Hanseth and Nielsen).

Det er hovedsakelig to fordeler med e2e; det at slike nettverk kan øke antall og typer av grupper som kan bruke en slik arkitektur, og at e2e-nettverk kan gjøre det mer vanskelig for uønskede tredjeparter å kontrollere kommunikasjonen på nettverket, fordi slike filtreringsapplikasjoner ikke vil bli implementert inne i nettverket. (Sandvig 2006). Dette vil si at alle oppgaver en ISP gjør utover det å videresende pakker vil være en form for brudd på e2e-prinsippene. Dette var nøyaktig hva case 2 og 3 gjorde; de gikk inn i nettverket og implementerte filtreringsapplikasjoner hos ISP'ene. Et viktig spørsmål er hvor dekkende e2e egentlig er for å oppfylle alle krav for generativitet, som er et middel for å oppnå fleksibilitet. Fra starten av har e2e-argumentene handlet om betingelser som kunne bli implementert korrekt ved endepunktene. Applikasjoner som ikke kan fungere skikkelig uten at de blir implementert i selve nettverket fører med seg en ny problemstilling. Slike implementasjonskrav vil gjøre at e2e-argumenter ikke kan valideres, og at en mer kompleks og funksjonell høynivåarkitektur har overtatt (Clark and Blumenthal 2000).

Noen Internett-entusiaster vil si at restriksjoner som blir overført til Internett-tjenester gjennom filtreringsapplikasjoner i nettverket er moralsk feil (Clark and Blumenthal 2000). En slik argumentasjon av umoral kommer i skyggen av Orlikowskis resonnement. Hun sier at strukturene i et nettverk vil vokse frem på en naturlig måte, basert på adferden til aktørene i nettverket og samspillet mellom dem (Orlikowski 2000). Det vil si at en slik utvikling av bruken av Internett ikke er umoralsk på grunn av e2e-designen, men en naturlig utvikling av en nettverksarkitektur for å oppfylle etterspørselen til brukerne av teknologien. Dette er i samsvar med II-teorien og den installerte basen som vokser og utvikler seg videre, også innenifra kjernen.

7.5 Teknologisk determinisme i samfunnet

Case 3 demonstrerte hvordan myndighetene kan klare å innføre kontroll på Internett; det man trodde skulle være et ukontrollerbart miljø. Ved å filtrere nettsider kan meninger endres til å gi et nytt budskap enn det opprinnelige, eller bestemte nettsider kan bli blokkert slik at de ikke vises. På denne måten støttes hypotese (3) med at teknologien styrer brukerne. Flere land blir påvirket av en teknologisk deterministisk kraft, men den vil ikke kunne generaliseres til å gjelde for alle land i verden i like stor grad. Hypotese (3) kan likevel utledes til å gjelde i flere

tilfeller og land. Med systemer som ECHELON og Carnivore er det blitt vist at alle land i verden til en viss grad er under observasjon og kontroll fra disse teknologiske filtreringssystemene. Samtidig kan ikke alle bli kontrollert hele tiden. Det er for mye informasjon til at dette er mulig, og mengden øker stadig. Dette betyr at selv om det kommer bedre prosesseringsprogrammer til å bearbeide informasjon, vil det ikke nødvendigvis gå raskere å lete gjennom den større informasjonmengden. Dermed støttes ytringsfriheten når ikke alt kan kontrolleres, og utviklingen av større brukergrupper og lettere aksess til Internett har bidratt til at Internett fungerer som et massemedium selv i land under streng overvåkning. Likevel, teknologisk determinisme er en faktor med tanke på at filtreringsmetoder kan brukes mot innbyggere i hele land, og dermed kan påvirke samfunner direkte. Et motargument mot å bruke begrepene teknologisk determinisme er i dette tilfellet at det er myndighetene som styrer teknologien som brukes på samfunnet. Dette er en vanlig sirkel av argumenter når det gjelder teknologisk og sosial determinisme, og det virker riktigere å si at det foregår en gjensidig påvirkning mellom teknologi og samfunn enn å si at hypotese (3) er sann.

"The End of End to End?"
Huston

8 Konklusjon

Denne studiens forskningsspørsmål ønsket å finne ut hvordan filtrering påvirker den globale infrastrukturen til Internett og dens videre utvikling. Casestudiene presenterte et bilde av bruksområdene for filtreringsmetodene i praksis for individer, private aktører og myndigheter i utvalgte land. Funnene fra analysen har vist at e2e-designen har flere fordeler, men også at brudd på e2e-arkitekturen ikke utelukker all fleksibilitet, gjennomskinnelighet eller åpenhet. Det ligger mye tradisjonell tankegang bak e2e som har vært en viktig støttepilar for Internetts utvikling. Nå har imidlertid utviklingen tatt et nytt skritt i form av applikasjoner i nettverket, og selv om framtiden er usikker er det lite hensiktsmessig å insistere på en teknologisk *status quo* framfor å gjøre et forsøk på å styre endringene i en positiv retning.

Det er ikke en ønskesituasjon at ISP'er skal kunne holde et jerngrep over nettverkstrafikken, enten i et forsøk på å bekjempe virus eller for å påføre kontroll over brukere på Internett. Som casestudiene har vist foregår det flere parallelle prosjekter som forsøker å skape kontroll på Internett, som Carnivore, ECHELON og Kinas nye Golden Shield. Felles for disse prosjektene er at de benytter seg av filtrering som hovedvirkemiddel for å oppnå den nevnte kontrollen. Casestudiene viser også at dette er ikke en enkel oppgave, selv med programvare som har kommet langt i bruken av avanserte filtreringsmetoder. Internett-bruken i Kina er så omfattende at ytringsfriheten ikke blir tiet i hjel. Myndighetene har ikke mulighet til å overvåke all kommunikasjon til alle tider, selv om de ønsker å gi inntrykket av at de kan. Implementering av filtrering på nasjonalt nivå skjer ofte i det skjulte og mangler dermed de tre nevnte egenskapene fleksibilitet, gjennomskinnelighet og åpenhet, noe som fører til mindre pålitelighet.

Det har vært lite fokus på hva innsamling av trafikkdata egentlig kan bety for individer. En oversikt fra elektroniske spor er nok til å kjøre en analyse og se hvem som passer til for eksempel kriminelle profiler. Opplysningene kan skaffes fra samordnede databaser viss formål kan ha endret seg fra de først ble dannet. I slike tilfeller risikeres det at personvernet er i fare, og reguleringene har gått over til å bli en uvelkommen sensur.

I introduksjonen ble det nevnt eksempler på datainnsamling, som bøker vi låner på bibliotek eller hvor vi reiser, som deretter blir slått sammen til å lage en profil. I løpet av denne oppgaven har det ikke blitt funnet noen konkrete bevis for at slikt skjer, annet enn indisier for at dette antagelig er en nyttig del i blant annet etterretningsarbeid. Tidligere

ansatte i ECHELON forsterket dette inntrykket ved å fortelle om en lav terskel for å registrere personer på listen over terrormistenkte.

Årsaker til lite pålitelighet er mangler i utvelgelsesprosessen for hva som skal blokkeres, som at utvelgelsene helst skjer i hemmelighet og at det utføres lite korreksjon hvis det er blitt gjort feil ved blokkeringer. For eksempel er det i mange land en vag og tilfeldig utvelgelse av sider som blir blokkert, og med en utvelgelse som ikke kan rettferdiggjøres ved nærmere granskning. Casestudiene viste også at det mangler sikkerhetsnett for selskaper/individer som feilaktig blir satt opp på sorte- og terrorlister (av myndigheter eller kommersielle firmaer), slik at ingen kan vite hva som egentlig blir lagret. Det kom fram at det ikke blir brukt nok ressurser på korreksjon av lister i ettertid, noe som viser en lite tilpasningsdyktig tilnærming til bruken av slike lister. Dette skader også pålitelighetsfaktoren til filtreringssystemene. Videre blir blokkeringslistene som brukes av kommersielle selskaper sjelden offentliggjort, fordi det er forretningshemmeligheter eller produsenten har opphavsrett på det. Risikoen er at slike selskaper ofte gjør feil, i tillegg til at deres utvelgelseskriterier ikke er åpne for gjennomgang – altså den manglende åpenheten. Samtidig må det tas hensyn til at en større åpenhet rundt filtreringsprogramvare ikke skal føre til en større sikkerhetsrisiko. Det bør legges inn mer ressurser på å tette sikkerhetshullene, framfor å prioritere å legge vekt på en økt hemmeligholdelse. Spesielt siden en skjult agenda fører til mistro og mistillit blant brukere, hvor det stilles spørsmålstegn om hva som egentlig blir overvåket om oss, og hva som gjorde at en slik overvåkning ble satt i gang.

Med dette er konklusjonen at det ikke er noe som tyder på at vi går tilbake til den opprinnelige enkle e2e-arkitekturen. Vi går heller mot en dyrere og mer komplisert nettverksstruktur. Dette er et valg brukere, ISP'er og myndigheter sammen har tatt ved å stadig presse Internett i denne retningen. Bruksområdene og nytteverdiene for Internett, slik den globale infrastrukturen ser ut nå, har blitt for store til at "den nye e2e-arkitekturen" kan avvikles og erstattes på en diskré eller billig måte. Spørsmålet er om vi vil gjøre det vanskeligere for alle brukere å bidra til nytenkning og innovasjon for Internett ved å gå vekk fra en enkel e2e-arkitektur. Før satt utviklere alene og jobbet uten behov for noen spesielle ressurser forbi en datamaskin og Internett. I dag gjøres mye av Internettutviklingen i felleskap av grupper som lager kompliserte og funksjonelle løsninger, med god hjelp fra sine arbeidsgivere i form av penger og maskinvare. En slik trend viser at den nye e2e-arkitekturen ikke tar vare på de små innovatørene. Likevel, slik Internett ser ut i dag er det ingen tegn på at det har blitt mindre innovasjon for funksjonaliteten til Internett. Den nye e2e-arkitekturen har heller ført til at det har blitt en ny arbeidsprosess. Filtreringsapplikasjoner bidrar med en nyttig tjeneste ved å øke brukerkontrollen over Internett og vil være en sterk ressurs også i framtiden. Casestudiene har demonstrert at det pågår en strid mellom de forskjellige aktørene

som bruker filtrering og de som det blir brukt filtrering på. Imidlertid er det ikke én vinner som kan utpekes, isteden er det en vekslende balansegang mellom partene.

En av de viktigere utfordringene ved bruk av filtreringsapplikasjoner nå og i fremtiden er å innføre mer åpenhet og gjennomskinnelighet til hvordan filtreringskriteriene blir satt. Ved å gjøre dette vil det føre til en mer fleksibel og pålitelig nettverksstruktur som lar flere få delta i designen, samtidig som brukere vil få økt tillit til tjenestene Internett tilbyr. Internett har eksistert i nesten 40 år, og i løpet av denne tiden har det oppstått en mer kompleks nettverksstruktur gjennom en utvikling ingen kunne forutsett. Om denne utviklingen bidrar til et fundament for et helt nytt Internett i framtiden er ennå for tidlig å si. Internett i dag har i aller høyeste grad en stor generativitet som gir fleksibilitet til nettverket til tross for at det ikke lenger finnes en ”ren” e2e-arkitektur. Ved å trekke ut den funksjonelle styrken i slike applikasjoner som filtrering bringer, vil de kunne bidra til en fleksibel, tilpasningsdyktig og pålitelig nettverksstruktur også i framtiden, slik de første Internett-arkitektene mente det skulle være.

Referanser

60Minutes. (2000). "Transcript of 60 Minutes on ECHELON." from http://cryptome.org/echelon-60min.htm.

BankID. (2008). "BankID Samarbeidet." from http://www.bankid.no/.

Baran, P. (1964). On Distributed Communications: Introduction to distributed communications networks, The RAND Corporation.

Beck, U., W. Bonss, et al. (2003). "The theory of reflexive modernization: Problematic, Hypotheses and Research Programme." Theory, Culture & Society **20**(2): 1-33.

Benkler, Y. (2006). The Wealth of Networks. How Social Production Transforms Markets and Freedom., Yale University Press.

Biba, E. (2005). "Stopping Carnivore Doesn't Stop FBI Surveillance." Medill News Service, from http://www.pcworld.com/article/id,119404-page,1/article.html.

Bjørnås, S. I. (2008). "Over 68000 døde i jordskjelvet i Kina." from http://www.vg.no/nyheter/utenriks/kina/artikkel.php?artid=195619 [aksess 25.06.2008].

Bush, V. (1945). "As We May Think." Atlantic Monthly **176**(1): 101-108.

Bye, R. and F. Sjue (2008). Overvåket, Gyldendal Norsk Forlag.

Campbell, D. (1999). "Interception Capabilities 2000." STOA Panel **2/5**.

Campbell, D. (2000). Inside Echelon.

Cartome. (2001). "Theory of Surveillance: The PANOPTICON." from http://cartome.org/panopticon1.htm [aksess 21.05.2008].

Ceruzzi, P. E. (2005). "Moore's Law and Technological Determinism - Reflections on the History of Technology." Technology and Culture **46**: 584-593.

Chandler, D. (2002). "Technological or Media Determinism." from http://www.aber.ac.uk/media/Documents/tecdet/tdet01.html [aksess 23.06.2008].

Clark, D. D. and M. S. Blumenthal (2000). "Rethinking the design of the Internet: The end to end arguments vs. the brave new world." TPRC.

CNNIC (2007). Statistical Survey Report on The Internet Development in China. C. I. N. I. Center.

Costello, J. (1991). "Issues of censorship vs privacy on computer networks."

Datakrimutvalget (2007). Lovtiltak mot datakriminalitet. 5.13.2 Filtreringsmetoder.

Datatilsynet. (2008). "Datalagringsdirektivet - personvern og informasjonssikkerhet." from http://www.datatilsynet.no/templates/Page____2109.aspx [aksess 05.03.2008].

Datatilsynet. (2008). "Personvern og informasjonssikkerhet." ID-tyveri, from http://www.datatilsynet.no/templates/article____1943.aspx [aksessert 05.03.2008].

David, P. A. (2001). "The Beginnings and Prospective Ending of "End-to-End": An Evolutionary Perspective on the Internet's Architecture." Oxford Review of Economic Policy **17**(2).

Deibert, R., J. Palfrey, et al. (2008). Access Denied: The Practise and Policy of Global Internet Filtering, The MIT Press.

Dempsey, J. X. (2000). "The Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age." from http://www.cdt.org/testimony/000906dempsey.shtml [aksess 25.02.2008].

DND. (2008). "Etiske regler for Internett." from http://dataforeningen.no/-mwtnUWZ.ips.

DoJ. (1968). "Title III of the Omnibus Crime Control and Safe Streets Act of 1968." from http://www.nd.edu/~pbellia/cyberlaw/Chapter7/TitleIIIprovisions.pdf.

e24. (2007). "Hacker kan få 60 år. Har hacket seg inn i en kvart million PC-er." from http://e24.no/it/it/article2095006.ece [aksess 27.03.2008].

e24. (2008). "Sikkerhet lønner seg ikke for nettbanker." IT - Telekom, from http://e24.no/it/article2233891.ece [aksess 02.03.2008].

EPIC. (2001). "DCS1000: The Device Formerly Known as Carnivore." Refuse & Resist! , from http://www.refuseandresist.org/resist_this/021601carnivore.html.

Espelid, Y., L.-H. Netland, et al. (2008). "A Proof of Concept Attack against Norwegian Internet Banking Systems." NoWires Research Group.

Expect-more. (2007). "Monitoring & Audit System (MAS)." from http://www.expect-more.no/index.php?option=com_content&task=view&id=15&Itemid=1 [aksess 29.02.2008].

FNH. (2008). "BankID i offentlige elektroniske tjenester." from http://www.fnh.no/FullStory.aspx?m=1043&amid=964214 [aksess 05.05.2008].

Ford, D. M. (2007). "Technologizing Africa: On the bumpy information highway." Computers and Composition **24**: 302-316.

Gamme, I. (2008). "AVG 8.0 Internet security er ute." Sikkerhet, from http://www.idg.no/produkter/sikkerhet/article89042.ece [aksess 29.02.2008].

Grindley, P. (1995). Standards, strategy, and policy: Cases and stories, Oxford University Press.

Hannemyr, G. (2005). Hva er Internett, Universitetsforlaget.

Hannemyr, G. (2006). "Internet Research." from http://www.uio.no/studier/emner/matnat/ifi/INF5220/h06/undervisningsmateriale/lecturenotes.html [aksess 2006].

Hanseth, O. and C. Ciborra (2007). Risk, Complexity and ICT, Edward Elgar Publishing.

Hanseth, O. and K. Lyytinen (2004). Theorizing about the design of Information Infrastructures: design kernel theories and principles.

Hanseth, O. and E. Monteiro (1998). Understanding Information Infrastructure.

Hanseth, O. and P. Nielsen (Work in progress). Infrastructural Innovation. Flexibility, Generativity and the Mobile Internet.

Hole, K. J., T. Tjøstheim, et al. (2008). Next Generation Internet Banking in Norway. Banking Security. D. o. I.-U. o. Bergen.

Huston, G. (2008). "The End of End to End?"

Jarbekk, E. I. E. (2008). "Datalagringsdirektivet - mer enn et spørsmål om lagringstid." Lov&Data **93**(1).

Kina-ONI (2005). Internet Filtering in China in 2004-2005: A Country Study. O. Initiative.

Klein, H. K. and M. D. Myers (1999). "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems." Mis Quarterly **23**(1): 67-94.

Klingsheim, A. and K. J. Hole (2008). Personal Information Leakage: A Study of Online Systems in Norway. The NoWires Research Group, Department of Informatics, University of Bergen.

Kuhn, T. S. (1962). Vitenskapelige Revolusjoners Struktur, University of Chicago Press.

Kushner, A. B. (2008). Repression 2.0 - Totalitarian states are learning to control citizens by creating the impression of ubiquitous surveillance. Newsweek.

Larsen, B., P. Wik, et al. (2000). IN166 Informasjonsteknologi og samfunn.

LeClaire, J. (2008). "Hackers Use SaaS To Auction FTP Passwords, Inject Code." Network Security, from http://business.newsfactor.com/news/story.xhtml?story_id=11000003U2JG [aksess 01.03.08].

Lichtblau, E., J. Risen, et al. (2006). "Eavesdropping 101: What Can The NSA Do?" from http://www.aclu.org/safefree/nsaspying/23989res20060131.html [aksess 05.03.2008].

Lillesund, M. (2008). "Datatilsynet: - Ingen kontrollerer politiet." from http://www.idg.no/computerworld/article86405.ece [aksess 05.03.2008].

Lillesund, M. (2008). "Lagring vil ramme de små." from http://www.idg.no/computerworld/article89246.ece [aksess 05.03.2008].

Lillesund, M. (2008). "Selger 9.000 ftp-passord." Nyheter, from http://www.idg.no/nyheter/article89254.ece [aksess 01.03.08].

Martinsen, S.-R. (2007). "Neste generasjon phishing." Sikkerhet | ID tyveri, from http://www.idg.no/kunnskapssenter/sikkerhet/idtyveri/article49509.ece [aksess 02.03.2008].

Martinsen, S.-R. (2008). "Kan overvåke det meste." Nettverk og Telekom | Nettverksadministrasjon, from http://www.idg.no/produkter/nettverktelekom/nettverksadministrasjon/article88617.ece [aksess 29.02.2008].

McCullagh, D. (2005). "Carnivore gone--but it's not dead." Security, from http://news.zdnet.com/2100-1009_22-5557496.html?tag=btxcsim.

Meeks, B. (2000). "FBI's Carnivore hunts in a pack." Technology News, from http://news.zdnet.com/2100-9595_22-524798.html.

Monteiro, E. (1998). "Scaling Information Infrastructure: The Case of Next-Generation IP in the Internet." The Information Society **14**(3): 229-245.

Murray, E. (2000). "FBI's Carnivore Probably Can't Shut Down Internet." from http://www.ine.com/ericm/papers/carnivore.html [aksess 15.03.2008].

Myers, M. D. and D. E. Avison (2002). An Introduction to Qualitative Research in Information Systems, Sage.

Müller, V. C. (2006). "Some Information Is too Dangerous to Be on the Internet."

Nabbali, T. and M. Perry (2003). "Surveillance Systems. Going for the throat: Carnivore in an Echelon World - Part I." Computer Law & Security **19**(6).

Nabbali, T. and M. Perry (2004). "Surveillance Systems. Going for the throat: Carnivore in an Echelon World - Part II." Computer Law & Security **20**(2).

Nettikette. (2006). "Netiquette Home Page, the do's and don'ts of online communication." from http://www.albion.com/netiquette/.

ONI. (2008). "OpenNet Initiative." from http://opennet.net/.

Orlikowski, W. J. (2000). "Using Technology and Constituting Structures: A Practice Lens for Studying Technology in Organizations " Organization Science **11**(4).

Peace, G. A. (2003). "Balancing Free Speech and Censorship: Academia's Response to the Internet." Communications of the ACM **46**(11).

Poole, P. S. (1999). ECHELON: America's Secret Global Surveillance Network.

Poulsen, K. (2005). "FBI retires its Carnivore." from http://www.securityfocus.com/news/10307.

RSF. (2006). "Months of harassment force Copt blogger to censor herself." from http://www.rsf.org/print.php3?id_article=18563 [aksess 30.06.2008].

RSF. (2008). "Middle East press releases 2008 archives." from http://www.rsf.org/archives-en.php3?id_rubrique=44&annee=2008 [aksess 30.06.2008].

Rønneberg, K. (2008). "Aftenposten: Tiananmen-massakren." from http://www.aftenposten.no/nyheter/uriks/article2463288.ece [aksess 07.07.2008].

Saltzer, J. H., D. P. Reed, et al. (1981). "End-to-End Arguments in System Design." ACM Transactions on Computer Systems **2**(4): 277-288.

Saltzer, J. H., D. P. Reed, et al. (1984). "End-to-End Arguments in System Design." ACM Transactions on Computer Systems **2**(4): 277-288.

Sandvig, C. (2006). "Shaping Infrastructure and Innovation on the Internet." Shaping Science and Technology Policy: The Next Generation of Research: 234-255.

Schmid, G. (2001). Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system). Temporary Committee on the ECHELON Interception System. E. Parliament.

Silverman, D. (2005). Doing Qualitative Research, SAGE Publications.

Smith, S. P., H. H. Perritt, Jr., et al. (2000). Independent Review of the Carnivore System. Final Report. D. Department of Justice, IIT Research Institute, IITRI.

Solli, M. (2008). "Hacket BankID - igjen." Bransjenyheter, from http://www.idg.no/bransje/bransjenyheter/article88543.ece.

Solli, M. (2008). "Norge kan unngå snokeloven." from http://www.idg.no/computerworld/article89143.ece [aksess 05.03.2008].

Spilling, P. (1995). Fra ARPANET til internett.

Staksrud, E. (2002). Ytringsfrihet og sensur på Internett - politisk regulering og kommersiell filtrering. Digital Makt - informasjons- og kommunikasjonsteknologiens betydning og muligheter, Gyldendal Norsk Forlag**:** 64 - 94.

Star, S. L. (1999). "The Etnography of Infrastructure." American Behavioral Scientist **43**(3).

Statistisk_Sentralbyrå. (2007). "Informasjonssamfunnet." from http://www.ssb.no/ikt/.

Tor. (2008). "Tor: nettanonymitet." from http://www.torproject.org/ [aksess 25.06.2008].

Tyson, J. (2001). "How Carnivore Works." from http://www.howstuffworks.com/carnivore.htm.

VG. (2007). "Spam-bølgen roer seg." from http://www1.vg.no/teknologi/artikkel.php?artid=187219.

Vietnam-ONI (2006). Internet Filtering in Vietnam in 2005-2006: A Country Study. O. Initiative.

Villeneuve, N. (2005). "Carnivore Replaced with Commercial App." Internet Censorship Explorer, from http://www.nartv.org/2005/01/16/carnivore-replaced-with-commercial-app/.

Villeneuve, N. (2005). The Filtering Matrix: Integrated mechanisms of information control and the demarcation of borders in cyberspace.

Walsham, G. (2002). Interpretive Case Study in IS Research. Qualitative Research in Information Systems. Myers and Avison, Sage.

Whorf, B. L. (1956). Language, Thought and Reality, MIT Press.

Wikipedia. (2008). "Egypt." from http://no.wikipedia.org/wiki/Egypt [aksess 27.05.2008].

Wikipedia. (2008). "Kina." from http://no.wikipedia.org/wiki/Kina [aksess 27.05.2008].

Wikipedia. (2008). "Magic Lantern (Software)." from http://en.wikipedia.org/wiki/Magic_Lantern_(software).

Wikipedia. (2008). "Massemedier." from http://no.wikipedia.org/wiki/Massemedia.

Wikipedia. (2008). "Tiananmen Square protests of 1989." from http://en.wikipedia.org/wiki/Tiananmen_Square_protests_of_1989 [aksess 07.07.2008].

Wikipedia. (2008). "Transport Layer Security." from http://en.wikipedia.org/wiki/Transport_Layer_Security [aksess 09.07.2008].

Wired. (1999). "EPIC Sues NSA Over Snooping." from http://www.wired.com/science/discoveries/news/1999/12/32905 [aksess 29.04.2008].

Yin, R. (1994). Case study research: Design and methods, Sage Publishing.

Zittrain, J. (2006). The Generative Internet. University of Oxford Faculty of Law Legal Studies Research Paper Series, Berkman Center Research Publication.

Øien, M. K. (1998). Internett filtrering. T. Forskningsnotat.