Sensur og overvåkning av Internett

Forelesning DRI2010, 15. oktober 2008

Herbjørn Andresen, stipendiat ved
Avdeling for forvaltningsinformatikk

Nærmere om begrepet ”overvåkning”

- Flere ulike betydninger
  - Etterretning; kartlegge *potensielt* skadelig virksomhet/personer
  - Etterforskning; finne ut av noe som faktisk har skjedd
  - Sensur; avskjære/redusere noens menings- og handlefrihet
  - Samfunnskontroll; påse at folk ”er lovlydige” (betaler skatt og barnebidrag, ikke mottar uberettiget trygd, ikke kjører for fort…)
  - Monitorering; følge med på tekniske spor fra bruk av systemer
    - Eks.: hvem skaffet (berettiget eller uberettiget) tilgang til opplysninger?
    - Det er en betydning som brukes her. Monitorering kan også brukes om bl.a. kameraovervåkning og bompengepasseringer osv.
- Betydningene er ulike, men de er også beslektet
- Alle betydningene er i større eller mindre grad relevante for temaet ”kontroll og overvåkning av (/på/med) Internett”

Fem teknologiske/metodeorienterte perspektiver på kontroll og overvåkning

Interception	Filtrering	Trafikkdata	Adferdsdata	Sikkerhets-tiltak
Oppfanging (en parallell til *avlytting)*	Innholds-kontroll, sensur	Logge; IP-adresser, når, hvor	Registrere; brukeres valg og handlinger	Hindre angrep, regulere tilgang osv.

- Disse fem perspektivene brukes gjennomgående i hele denne forelesningen
  - Bedre oversikt enn *av/med/på* (innhold/arena/verktøy) -perspektivet
  - Disse perspektivene er i prinsippet felles for ulike Internett-tjenester: Web-publisering, e-forvaltning og e-handel, e-post, chat, news etc.
- Men (som alltid…): ”Fem kategorier” er ingen fasit, og grensene er ikke absolutte. Det er bare et pragmatisk valg for denne disposisjonen

Første metodeperspektiv: ”Interception”

- Mangler dessverre et ord som dekker godt nok
  - En av betydningene som dette er oversatt med i engelsk-norsk ordbok er *”oppsnapping”*
  - Handler om å fange opp innholdet i det som kommuniseres, oftest uten at de som kommuniserer vet om det
  - Sammenlignbart med *avlytting*, men omfatter alle typer data, ikke bare lyd
- I internett-sammenheng ofte omtalt som *pakkesniffing*
  - Men det uttrykket dekker ikke alle former for *interception*

”Interception” (ark 2)

- ”Interception” kan være ulovlig avlytting, noe som hackere driver med
- Kan også være ledd i feilsøking og monitorering av eget nettverk – helt akseptabelt
- Det er også et verktøy for politi og etterretning
  - Rettslig regulert: Må holde seg innenfor lover og regler om akseptable *metoder* for etterforskning og bevissikring m.m.
  - Mye internasjonalt samarbeid om metode-reglene
    - men likevel en del forskjeller i hva som aksepteres
  - En generell fellesbetegnelse for ”interception”-verktøy som brukes i politiarbeid er *”policeware”*

”Interception” (ark 3)

- Brukt i legitim overvåkning; spaning og målrettet etterforskning
  - Man vet som regel en del på forhånd om hvilke handlinger og/eller personer man trenger å skaffe opplysninger om
  - Målrettet etterforskning er i avgrenset målestokk
    - Normalt avgrenset til en konkret kriminell handling
    - I stigende grad også rettet mot organisert kriminell aktivitet
    - Flere lovendringer de senere år som gir politiet adgang til å bruke mer inngripende overvåkningsmetoder
  - Metodereglene er likevel i hovedsak *teknologinøytrale,* og har mer generell anvendelse enn bare Internett

”Interception” (ark 4)

- Utvikling i retning av å åpne for mer inngripende etterforskningsmetoder på nettet:
  - Her henter Norge i særlig grad inspirasjon fra England
  - Lovforslag om å gjøre såkalt ”grooming” straffbart
    - Straffbart å *avtale* seksuell aktivitet med mindreårig
  - Faremo-rapporten, 30. januar 2007
    - Forslag til tiltak mot overgrep på Internett
    - Ønsker meldetjeneste etter engelsk modell: www.ceop.gov.uk
- Det satses mer på politisk-institusjonelle virkemidler enn rettslige
  - Siste 3 statsbudsjetter; ”Kripos viderefører arbeidet med å etablere *nasjonalt senter for kommunikasjonskontroll*

”Interception” (ark 5)

- Et annet ytterpunkt enn målrettet etterforskning av konkrete saker ville være en ubegrenset ”føre var”-overvåkning
  - PST skal drive etterretning som ”forebygger og etterforsker lovbrudd mot nasjonens sikkerhet og selvstendighet”
  - Krav til at opplysninger som behandles er nødvendige for formålet
  - Lovlig politisk og religiøs aktivitet gir ikke grunnlag for etterretning
  - Underlagt demokratisk kontroll (Stortingets EOS-utvalg)
- I Norge har ingen i dag mandat til å drive ”interception” av hvilken som helst kommunikasjon på Internett
  - Men kanskje dette er noe som vil endre seg…?
    - Økt aksept for overvåkning pga. utviklingen i internasjonal terror?
    - Nødvendig for samarbeid med andre land som har gitt sine etterretningsmyndigheter annerledes mandater?

”Interception” (ark 6)

- Spaning, etterforskning, etterretning osv. er for det meste basert på ”tradisjonelle metoder”
  - Dreier seg ikke først og fremst om ”overvåkning av nettet”, men om overvåkning av personer, miljøer, objekter – Internett er bare en av mange faktorer
  - Likevel er såkalt ”policeware” en voksende bransje
  - Et gammelt og godt kjent eksempel er *Carnivore* (latin for kjøtteter☺), som brukes av amerikanske FBI. Brukes ved at ISP-ene pålegges å installere programmet *Carnivore*, som formidler den kommunikasjonen man vil ha overvåket til FBI
- Det finnes en del myter om ”den totale overvåkningen av Internett”
  - Vanskelig å finne håndfast informasjon, det blir ofte et spørsmål om hva man velger å tro
  - Et artig eksempel: ”Finnes Echelon?”

Andre metodeperspektiv: Filtrering

- Stor og åpen problemstilling:
- I hvilken grad

må eller
kan eller
vil eller
bør

”vi” eller
”de” eller
”man” eller
”noen”

Forhindre, eller *ikke* forhindre, ”fæle greier” på nettet?

Filtrering (ark 2)

- Først en del om filtre, metoder og filtreringsteknologier
- Rettslig regulering
  - ”De store spørsmålene”: Ytringsfrihet, demokrati, personvern
  - Lovforbud mot uønsket innhold, vs. ”alminnelig folkeskikk”?
  - Ferske interessante forslag (Datakrimutvalget, Faremoutvalget)
- Aktører, roller og ansvar
  - Styrt av offentlige myndigheter vs. styrt av private virksomheter?
  - Arbeidsgiver?
  - Foreldre?
  - Nettsteds- eller kommunikasjonsleverandør?
  - … eller eventuelt styrt av brukeren selv?

Filtrering (ark 3)

- Et filter er et verktøy for siling
- Filtrering på Internett er siling av *innholdet*
  - Kan hindre at man mottar innhold fra angitte personer, firmaer, adresser etc.
  - Eller hindre at man mottar noe som inneholder nærmere angitte ord, bilder, filtyper
- Utfallet av filtrering kan være forskjellig:
  - Enten får brukeren ingen beskjed om at filtreringen har skjedd (oppleves som om dette innholdet ikke eksisterer)
  - Eller brukeren varsles om at innholdet er filtrert ut, helst med angivelse av hvilke egenskaper filteret har reagert på
- Hvor skjer filtreringen?
  - Kan være et filtreringsprogram installert på brukerens maskin
  - Eller man kan anvende en ferdig filtrert nettaksess

Filtrering (ark 4)

- To hovedstrategier for filtreringsprogrammer:
  - filter basert på **automatisk analyse** av innholdet
  - filter basert på (manuell) **vurdering** av innholdet
  - Noen programmer, for eksempel en del spam-filtere, bruker begge disse strategiene i kombinasjon
- Typisk for filter basert på **automatisk analyse:**
  - Kan anvendes på både kommunikasjons- og innholdstjenester
  - Baserer seg på ordlister
  - Ofte telling av antall forekomster, eventuelt også ”vekting” av visse ord og kombinasjoner for å avsløre uønsket innhold
  - Automatisk analyse av bilder, lyd, video etc. for å avdekke uønsket innhold er svært vanskelig og ressurskrevende

Filtrering (ark 5)

- Fordeler og ulemper med automatisk analyse
  - man prøver å ”ta ballen, og ikke mannen”, fordel at aktører og adresser ikke blir stengt ute på forhånd
  - Kan ikke brukes effektivt på annet innhold enn tekst
  - Stor fare for å filtrere bort noe som skulle ha gått gjennom
    - Metaforer, ironi, ord med flere betydninger, blanding av språk
    - En fare for at filtrering gir oss fattigere språk, fordi vi vil gardere oss mot at det vi skriver blir filtrert vekk?
  - Fare for å slippe gjennom noe som skulle vært filtrert
    - Filteret kan lures ved å skrive koder. (*V1agra* osv.)
    - Bare et pragmatisk valg hvor ”strengt” filteret skal være

Filtrering (ark 6)

- Filter basert på vurdering av innhold
  - Manuell, menneskelig vurdering av det enkelte nettsted eller den enkelte siden
  - Statisk prinsipp: Filtreringen fjernes ved ny manuell vurdering, det holder ikke bare å endre innholdet
  - Passer kun for innholdstjenester
    - Kommunikasjonstjenester er for dynamiske
- To hovedmekanismer for statisk filtrering
  - Svartelister (”opt-out”)
    - Blokkerer adresser/sider som står på listen (mindre strengt)
  - Hvitelister (”opt-in”)
    - Slipper bare inn adresser/sider som står på listen (strengere)

Filtrering (ark 7)

- Filterets ”innhold” kan være lister med adressen til nettstedet som skal sperres eller som skal slippes inn
  - Ofte angis en del av adressen, for eksempel

    http://www.afin.uio.no/forskning...

    som sperrer (svarteliste) eller slipper inn (hviteliste) alle dokumenter og alle underkataloger til denne katalogen

Filtrering (ark 8)

- Eksempel på svarteliste:
  - Kripos’ såkalte ”barnepornofilter”
  - Frivillig samarbeid med ISP-er, de som deltar i samarbeidet sperrer alle nettsteder som står på listen
  - Tekst fra Tele2 standard tjenestvilkår:

  - ’Tele2 har i samarbeid med "Nye Kripos" installert "barnepornofilter". Dette filteret medfører at Kunden ikke vil kunne aksessere web-sider, som av "Nye Kripos" er å anse som brudd på norsk regelverk’

Filtrering (ark 9)

- Eksempel på hviteliste:
  - Telenors program ”Kidsurf Barnefilter”
  - Lastes ned til brukerens maskin
  - Fungerer slik at foreldre skal godkjenne, og legge til i filteret, hvert eneste nettsted som de vil at barnet skal kunne gå inn på. Alle andre nettsteder stenges ute

  - Frivillig å bruke, helt opp til foreldre (eller andre som administrerer filteret på lokal datamaskin) hvilke nettsteder som skal slippes gjennom

Filtrering (ark 10)

- Mer komplekse filtersystemer: Kombinerer ulike strategier (analyse, sperring, hvitelister)

Eksempel:
Filterprogrammet
CyberPatrol

-Svartelister
-Hvitelister
-"Tillatte ord"
-"Forbudte ord"
-Merket innhold

Filtrering (11)

- Strategien "merking" av innhold – et eksempel ("Platform for Internet Content Selection

	Violence Rating Descriptor	Nudity Rating Descriptor	Sex Rating Descriptor	Language Rating Descriptor
Level 4	Rape or wanton, gratuitous violence	Frontal nudity (qualifying as provocative display)	Explicit sexual acts or sex crimes	Crude, vulgar language or extreme hate speech
Level 3	Aggressive Violence or death to humans	Frontal nudity	Non-explicit sexual acts	Strong language or hate speech
Level 2	Destruction of realistic objects	Partial nudity	Clothed sexual touching	Moderate expletives or profanity
Level 1	Injury to human being	Revealing attire	Passionate kissing	Mild expletives
Level 0	None of the above or sports related	None of the above	None of the above or innocant kissing; romance	None of the above

Filtrering (ark 12)

- Merking
  - Egner seg til statiske innholdstjenester, oppdateringsproblem
  - Fordel: Kan brukes på bilder og video, ikke bare tekst
  - Hovedproblemet: Hvem skal merke?
    - En del innholdsleverandører merker selv, frivillig ("vi driver med porno og vedstår oss det, vi setter nivå 4 i de html-dokumentene dette gjelder")
    - Kan også være filterleverandøren eller en uavhengig tredjepart som merker – da settes de merkede nettestedene på svartelister, egen liste for henholdsvis nivå 1, nivå 2 osv.
  - Et annet problem: Kulturforskjeller
    - Oppfattes "clothed sexual touching" likt i Sverige og USA?

Filtrering (ark 13)

- Ytringsfrihet
  - Filtrering av statiske innholdstjenester er en form for forhåndssensur, og det er strenge grenser for å kunne drive forhåndssensur i norsk rett
  - Grunnlovens § 100, fjerde ledd: "Forhaandscensur og andre forebyggende Forholdsregler kunne ikke benyttes, medmindre det er nødvendigt for at beskytte Børn og Unge imod skadelig Paavirkning fra levende Billeder. Brevcensur kan ei sættes i Værk uden i Anstalter"
  - Beskyttelse av barn og unge er altså et mulig unntak
  - Ellers må man forutsette stor grad av frivillighet

Filtrering (ark 14)

- Rammes ikke av vernet mot forhåndssensur:
  - At man selv velger å beskytte seg med filter
  - At foreldre filtrerer barnas bruk av nettet
- Litt mer i grenselandet:
  - Arbeidsgivers filtrering av ansattes nettilgang
    - Arbeidsgiveren har en styringsrett, og kan iverksette tiltak for å hindre at firmaets omdømme blir skadet, eller for å unngå at de ansatte kaster bort arbeidstiden
    - Men det er ikke like akseptabelt å iverksette forhåndssensur for å "unngå skadelig påvirkning" eller fri meningsdannelse
    - Arbeidsgivers adgang til å filtrere må derfor ses i sammenheng med det aktuelle formålet

Filtrering (15)

- Andre rettslige og styringsmessige spørsmål:
  - Har tredjeparter som "merker" innhold noe ansvar for å informere innholdsutgiveren om merkingen?
  - I prinsippet kan det være et rettslig ansvar for den som filtrerer, dersom merkingen ikke er riktig
    - Ikke helt opplagt hvordan et slikt rettslig spørsmål skal løses
- Behov for ny lovgivning?
  - Et *mindretall* i "datakrimutvalget" (NOU 2007:2), foreslår rettslig adgang til nasjonal filtrering av utenlandske nettsteder med innhold som strider mot norsk lovgivning

Tredje metodeperspektiv: Trafikkdata

- Krav om at leverandøren av nettjeneste skal logge trafikkdata, og ta vare på dem en viss tid
- Også krav om at de skal slettes etter en viss tid
- Logger brukes også til andre formål enn overvåkning, men det er for å støtte etterforskningsformål at det nå har kommet krav til lagringstid
- Trafikkdata kan som regel avdekke følgende:
  - IP-adresse (brukerens datamaskin-identifikasjon)
  - Tidspunkt
  - Hvilken brukerkonto (hos leverandør av nettjenester) som er pålogget med den identifiserte datamaskinen på dette tidspunktet
  - Hvilke nettsider som er besøkt

Trafikkdata (ark 2)

- EUs datalagringsdirektiv
  - Fører til lenger lagring av trafikkdata (2 år), med det formål å kunne få brukbare spor til etterforskning
- Heftig debattert i mediene i godt og vel to år
  - Til å begynne med var nesten alle som deltok i debatten motstandere:
    - Universitetsfolk, Datatilsynet, interesseorganisasjoner…
  - Tilhengerne har meldt seg på i den offentlige debatten omtrent fra begynnelsen av 2008
    - Økokrimsjef Høgetveit, replikk til leder i Aftenposten 30.1
    - Økokrim og Kripos i felles kronikk **"Datalagring må til"**, 8.9

Fjerde metodeperspektiv: Adferdsdata

- Kan til dels bruke noe av den samme typen logging som trafikkdata, men:
  - Det er (normalt) *nettstedets* behandlingsansvarlige, og ikke ISP, som logger
  - Nettstedet vet ikke hvem som egentlig er abonnenten bak et kontonavn
  - Det som logges er bevegelser, valg, søkestrenger etc.
- Personvernøkende teknologier
  - Et slags "mottiltak" mot registrering av adferdsdata;
    - Ikke for å unngå eller forby registrering og bruk av det
    - Men for å gi brukeren selv kunnskap om og kontroll med hvilke adferdsdata som registreres (personvernhensyn)

Adferdsdata (ark 2)

- Innholdsutgiver kan plassere "cookies" (små tekstfiler) på brukerens datamaskin
  - Ikke konkret "skadepotensiale", men et visst inngrep å plassere informasjon ubedt på andres maskin
  - Brukeren kan selv velge å ikke ta imot dem – men det kan i visse tilfeller redusere funksjonalitet
  - Ofte er det ikke nettstedet selv, men noen de har solgt annonseplass til, som skriver og leser cookies
  - Oftest helt legitim bruk: Huske hva brukeren valgte sist vedkommende var innom nettsiden og lignende
  - "Slemmere varianter" – såkalt spyware

Femte metodeperspektiv: Sikkerhetstiltak

- Virksomheter (firmaer, offentlige etater, universiteter osv.) legger oftest opp sikkerhetstiltak i sitt driftsmiljø:
  - Viruskontroll, hindre skadelig programvare
  - Brannmurer, og IDS ("Intrusion detection system")
  - Spamfiltrering, hindre uønsket/meningsløst innhold
  - Passiv beskyttelse, for eksempel "herding" av driftsmiljø
  - Ikke alle sikkerhetstiltak har spesifikt med virksomhetens bruk av eller tilgjengelighet på Internett å gjøre
    - Likevel er "sikkerhet" alltid en egenskap ved *helheten,* derfor er også slikt som ansattes holdninger, behandling av kasserte papirutskrifter m.m. viktig

Sikkerhetstiltak (ark 2)

- For en virksomhet som det er "attraktivt å angripe", er dette ganske omfattende og krevende aktiviteter:
  - Logging av informasjon, aktive valg om å utestenge enkelte avsendere, kontakte nettleverandører for å fortelle at de gir "husly" til en hissig angriper osv.
- Nasjonal sikkerhetsmyndighets enhet NorCert
  - Norsk "critical emergency response team"
  - VDI ("Varslingssystem for digital infrastruktur")
    - Frivillig ordning, en del store firmaer og etater som deltar
    - Offentliggjør månedlige, anonymiserte rapporter (se www.nsm.stat.no)

Sikkerhetstiltak (ark 3)

- Tilgangsstyring
  - Man bruker ofte en nettleser, med html-dokumenter, som port inn til andre tjenester: Nettbank, nettbokhandel, samordna opptak osv. – med en form for *pålogging*
  - En nettleser er "tilstandsløs", og ikke egentlig varig "påkoblet" det systemet det snakker med
  - Etter pålogging til nettjenesten, når man navigerer videre "innover" i samme tjeneste, må man *fortsette* å fortelle "for hvert klikk" at man stadig er samme påloggete bruker: Dette gjøres som oftest ved hjelp av "cookies"
    - Omtales gjerne som session cookie, den har begrenset varighet og slettes etter avlogging
  - En god del "teknisk monitorering" er helt nødvendig for at nettjenester med innlogging i det hele tatt skal fungere

To ulike eksempler på bruk av "cookies"

- Eks 1: Regjeringen.no (Regjeringens web)
  - Filnavn på min maskin: `herbjora@odin.dep[1].txt`
  - Filens innhold:
    `odinskake129.240.178.96.642511404266059830din.dep.no/153639066553602984059028969441602976716 5*`
- Eks 2: Feide (Uninetts felles innloggingstjeneste for en rekke nettsteder – "Single Sign On")
  - Filnavn på min maskin: `herbjora@moria2[2].txt`
  - Filens innhold:
    `MoriaDenySSOCookiefalselogin.feide.no/moria2/153614314195202977025522480083522977018 8*MoriaUserOrganizationCookieuio.nologin.feide.no/moria2/153618802755842977159622481083522977018 8*`

Noen "rettslige stikkord"

Interception	Filtrering	Trafikkdata	Adferdsdata	Sikkerhets-tiltak
Straffe-prosess krav til at det foreligger (tilstrekkelig alvorlig) mistanke	*Ytrings-friheten*, (og dens grenser) offentlighets-prinsippet styringsrett (i arbeidsgiver-forhold etc.)	*Ekomloven* fra 2003 (+ straffeprosess) Utgangspunkt i flere EU-direktiver ("e-kompakken"). Datalagrings-direktivet fra 2006	*Pol § 21* (om person-profiler) Også mer generelt er bestem-melser i pol relevante	*Ulike regler* Svært ofte er *Pol § 13*, med *pof* kapittel 2, mest relevant (*Sikkerhetslov* med forskrift, for det som gjelder rikets sikkerhet)

Noe om typiske aktører

	Inter-ception	**Filtrering**	**Trafikkdata**	**Adferds-data**	**Sikkerhets-tiltak**
Hvem overvåker?	Politiet. Sivil og militær etterretning + hackere?	"Lite åpne regimer" + etterretning? + foreldre + arb.givere?	ISP Utleverer til politi i etter-forskning	Systemeier/ ansvarlig for tjenesten. Annonsører	Systemeier/ ansvarlig for tjenesten + NSM/NorCert for VDI
Hvem overvåkes	Må være konkret mistenkt for noe alvorlig	Kan variere - Alle? - Mistenkelige? - "sarte sjeler"?	Alle!	Alle (men særlig kunder og ofte tilbakevend-ende brukere)	Bruker/ kunde Mulige hackere
Hvem kan være "typisk bad guy"?	Terror-mistenkte, Organiserte kriminelle	Oppviglere "Moralsk fordervede" Kriminelle	Kriminelle	Annonsører o.l. (hvis de tar for lite hensyn til personvernet)	Hackere. Utro tjenere

Noen (sterkt forenklede) "skalabetraktninger"

	Inter-ception	**Filtrering**	**Trafikkdata**	**Adferds-data**	**Sikkerhets-tiltak**
Inngrep i brukers personvern	Høy	Høy	Middels	Middels	Lav
Brukerens viten om at overvåk-ning skjer	Lav	Høy	Lav	Lav	Middels
Spesifikk sammen-heng med Internet-teknologi	Lav	Middels	Middels	Høy	Høy

Noen internasjonale perspektiver

Interception	Filtrering	Trafikkdata	Adferdsdata	Sikkerhets-tiltak
Sterk opptrapping i USA etter 2001, *NSA* Rykket ubeha-gelig nær? Svenske "FRA-loven" i 2008 Kripos deltar i internasjonalt samarbeid	Kritikk mot Google™ for å gi etter for krav fra Kina om å filtrere ut innhold *Europa*; påvirke ISP-er, samarb. offentlige mynd. *USA*; påvirke sluttbrukerledd, filtreringsbehov tolket av private	Del av debatten om *lagrings-direktivet*: Trenger vi virkelig å la det bli "EØS-relevant"?	Enighet om at *teknologien* bør støtte valgfrihet Lite samspill internasjonalt på politisk og rettslig nivå	Internasjonale *standarder*, nasjonale eller private *løsninger* I noen sjeldne tilfeller vil sikkerhets-løsninger og -behov kunne *begrense* internasjonal kommunikasjon