

Del 6: Avslutning

... a long, strange trip

“*What a Long Strange Trip It's Been*” var tittelen på samlealbumet Grateful Dead ga ut i 1977 da de oppsummerte sitt liv og virke de første ti årene.

Det kunne like gjerne vært tittelen på beretningen om vår fire tiår lange reise med Internett og Forskningsnett. Reisen har vært uforutsigbar, oppløftende og nedslående, spennende og kjedelig, innholdsrik og overfladisk, kort sagt det meste av det en reise kan innebære og litt til.

Framfor alt har det vært en *forunderlig* reise.

Vi er langt fra ved reisens slutt, den er bare så vidt i gang. Ett spørsmål er hvor denne reisen vil føre forskning og utdanning, institusjonene, universitets- og høyskolene, IT-organisasjonene og IT-virksomheten ved institusjonene og UNINETT i årene som kommer. Ett annet er hva den vil bringe for hver enkelt av oss, for våre relasjoner til andre, for privat- og arbeidsliv, for sosial, kulturell, politisk og økonomisk utvikling lokalt, regionalt og globalt?

En mer brukernær og strategisk IT-virksomhet

En hverdag uten IT og Internett er i dag utenkelig for våre studenter, undervisere, forskere, administratorer og ledere. IT og Internett er vedvært tett inn i alle deler av virksomheten ved våre institusjoner, det gjør at institusjonene og de som befolker dem kan tikke og gå. IT er blitt en innsatsfaktor av vesentlig betydning i alle produksjonsprosessene ved institusjonene og i sektoren, – i studiearbeidet, i undervisningen, i forskningen og formidlingen og i administrasjonen og styringen av virksomheten. IT er en ‘enabler’, en faktor som tilrettelegger for virksomhet og som setter den enkelte, institusjonene og sektoren i stand til å gjøre sine oppgaver og nå sine mål. Uten IT blir lite gjort. Med IT kan svært mye gjøres, IT er fortsatt generativ, en teknologi som tilrettelegger for og fremmer eksperimentering, utforskning og utvikling, den åpner muligheter og gir nye evner.

IT har en egenskap som skiller faget fra de fleste andre fagområder. På den ene siden er det et fag i seg selv. På den andre siden er det et fag som inngår i de fleste andre fagområder. Dette gir IT en spesiell posisjon ved at de ser sammenhenger på tvers av fagområdene, ser gjenbruksverdi av tilnærminger, metodikk og løsninger på tvers av virksomheter og områder og ser hvordan ressurser kan utnyttes best mulig gjennom samordning og samvirke. Dette gjelder i offentlig og privat virksomhet og det gjelder både vitenskapelig og administrativ virksomhet i vår sektor og ved våre institusjoner.

Utvikling av virksomheten i tråd med ITs rolle og potensiale, er en vesentlig utfordring for IT-organisasjonene ved institusjonene og for den faglige og administrative virksomheten ved institusjonene og sektoren i dag og i de nærmeste årene.

Operativ og strategisk IT

IT er på samme tid både operativ og strategisk, en leverandør og en medspiller, en driftsutgift og en investering. For å løse sine oppgaver må IT i framtida levere godt på det operative nivået, samtidig som de strekker seg i strategisk retning.



På den ene siden vil IT møte stadig sterkere krav og forventninger fra brukerne og institusjonene til stabilitet, tilgjengelighet og sikkerhet, tilstrekkelig kapasitet og bruks- og kosteffektive løsninger. Infrastruktur og tjenester med tilstrekkelig kapasitet og høy tjenestekvalitet forutsettes å være tilgjengelig 24 timer i døgnet, 365 dager i året.

På den andre siden kommer IT mer og mer på innsiden av stort sett alle arbeids- og produksjonsprosessene ved institusjonene. Dette krever at IT-organisasjonene må bygge kompetanse og utvikle arbeids- og samarbeidsformer som gjør at de kan bidra med kompetanse, løsninger og ressurser for å utvikle forsknings- og utdanningsvirksomheten og den administrative virksomheten. For å lykkes med dette må IT-organisasjonen skjønne hva fagmiljøene driver med, ha kompetanse på gjenstandsområde, metodikk, praksis og hva som er ITs bidrag til at fagområdet tikker og går. IT må være med og ta medansvar for resultatene som skal skapes.

Figur 6-1: ITs rolle på institusjonene har tradisjonelt vært å levere tjenester og stille ressurser til disposisjon for virksomheten. Etter hvert som IT veves tettere og tettere inn i produksjons- og arbeidsprosessene vil ITs suksess være avhengig av at IT bidrar til å utvikle og forbedre disse og til å utvikle nye evner i virksomheten og ta tak i nye oppgaver.



Det er slik institusjonene kan og må satse strategisk på IT, – satse på den IT som gir bedre og flere resultater av forsknings- og utdanningsvirksomheten og som forbedrer, forenkler og effektiviserer den administrative. Dette er en investering på linje med andre investeringer, den skal sette virksomheten bedre i stand til å løse sine oppgaver og betale seg ved at institusjonen leverer flere og bedre resultater.

Her finnes det ingen enkle svar eller ferdigsnekrete løsninger som kan kjøpes i butikken eller hos konsulentbyrået. Det er imidlertid ett vesentlig grep som må tas først av alt, – IT må så fort som mulig flyttes ut av den administrative virksomhetens domene og få sin primære forankring i den faglige virksomheten. Ved de aller fleste av våre institusjoner er IT i dag organisert som en del av den administrative virksomheten og på altfor mange steder er IT en del av organisasjons- og personalavdelingen eller økonomiavdelingen. Dette gir lang vei til institusjonsledelsen og enda lengre vei til primærvirksomheten ved institusjonene. IT må løftes opp på både den faglige og den administrative ledelsens dagsorden og IT må stå ansvarlig overfor den faglig og administrative ledelsen *samlet*, ikke kun den administrative.

Utfordringer i kø

For drifts- og utviklingstjenestene og tjenesteleveransene møter IT-organisasjonene konkurranse fra sterke aktører og trender. To av disse er vel verdt å nevne, – våre framtidige brukeres bruksmønstre og framveksten av skytjenester.

Digitale innfødte

Våre studenter har allerede før de kommer til våre institusjoner, etablert en omfattende digital tilværelse og praksis. De overlot for lang tid siden e-posten sin til Hotmail (eller hva det enn heter i

dag), Gmail og tilsvarende Webmail-tjenester. De snakker og utveksler meldinger med venner og familie på MSN, Skype, Facebook og andre tilsvarende medier. De hører på musikk med Spotify og kjøper den på iTunes og WiMP. De lagrer og deler informasjon, bilder og annet i Dropbox, Instagram, Facebook, YouTube og på stadig nye steder. De surfer like gjerne på smarttelefonen og nettbrettet som på PC-en, og de leser nyheter og bøker og ser TV-programmer og filmer heller der enn i tradisjonelle medier.

Dette er våre framtidige brukere, de vi skal levere nyttige tjenester og løsninger til i årene som kommer.

Det er en stor utfordring for institusjonene, sektoren og IT-organisasjonene å møte disse studentene med produktive læringsomgivelser og tjenester. Det ser ikke ut til at noen foreløpig har gitt noe fullgodt svar på dette. Én innfallsvinkel har vært å etablere læringsomgivelser og tjenester på institusjonenes premisser, med ordinære IT-tjenester og -verktøy i kombinasjon med systemer for læringsstøtte (LMS-er) som Fronter og It's Learning bygd rundt tradisjonell undervisning. En annen innfallsvinkel er å bygge læringsomgivelser som kan inngå som en mer eller mindre sømløs del av de digitale omgivelsene studentene allerede lever når de starter studiene, noe blant annet den siste tids interesse for *Massive Online Open Courses (MOOC)* er ett av mange uttrykk for. På ingen av disse områdene er juryen klar til å komme ut og avgi en kjennelse. Det eneste som er sikkert, er at svaret på utfordringen krever hardt planmessig og langsiktig arbeid på både operativt og strategisk nivå med testing, utforskning og eksperimentering.

Skytjenester som leveransemodell

I det større bildet er dette utfordringer for den eksisterende leveransemodellen for IT-tjenester ved institusjonene. Hittil har mesteparten av ITs tjenesteleveranser vært lokale. Ved hver institusjon har IT levert e-posttjenester, Web-tjenester, lagringstjenester og andre basis IT-tjenester i egen regi. På noen områder, spesielt det administrative, er det utviklet fellesløsninger for sektoren. Erfaringene fra dette arbeidet tilsier at det burde tenkes fellesløsninger på langt flere områder. Med dagens infrastruktur er det fullt mulig og høyst sannsynlig regningssvarende, og det ville ganske sikkert gitt ett kvalitetsmessig løft for mange brukere.

Figur 6-2: 'Sky'-tjenestene lover gjennomsliktig og enkel tilgang til data, tjenester og applikasjoner fra hva som helst av brukerutstyr fra hvor som helst over Internett.



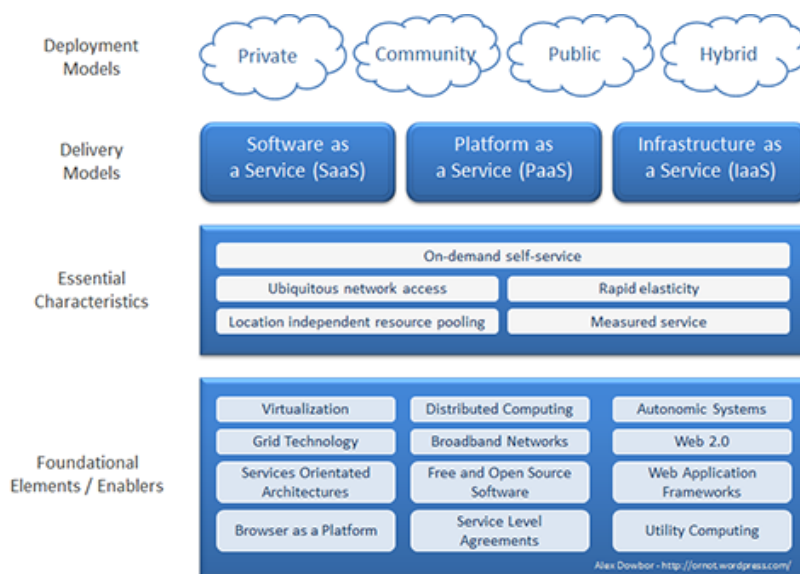
Inn fra sidelinja kommer så 'sky'-tjenestene som en ny leveransemodell for IT-tjenester og -ressurser. Denne modellen bygger på en formodning om at IT er blitt hyllevare som like gjerne kan kjøpes i et marked når den trengs av den som kan levere. Det utvikles et marked der små og store, lokale og nasjonale foretak leverer basis IT-tjenester og -ressurser bygd på denne modellen.

For brukeren er data, tjenester og applikasjoner tilgjengelig fra hva som helst av utstyr via Internett. Hvis bare en brøkdel av potensialet som tilskrives denne modellen blir realisert, vil det snu opp ned på de fleste forestillingene vi har om IT-drift. Å utnytte denne leveransemodellen for institusjonenes og sektorens formål, vil bli en like krevende oppgave som å møte utfordringene knyttet til tilpassingen av virksomheten til studentenes digitale liv. Og på sett vis er det en og samme sak, – de fleste komponentene i studentenes digitale tilværelse og praksis er allerede i skyen.

Forskningsnettet og UNINETT

Det er åpenbart at leveransemodellen basert på lokal drift ikke er bærekraftig for store deler av sektoren og for vesentlige deler av tjenestetilbudet. Skytjenester som leveransemodell er kommet for å bli med Internett som infrastruktur og virtualisering av alt fra infrastruktur til tjenester og arbeidsomgivelser. At dette er mulig, innebærer ikke automatisk at det er ønskelig eller hensiktsmessig. Kardinalspørsmålet er det samme her som ved enhver annen anledning, – hvordan kan dette best inngå i institusjonenes og sektorens operative og strategiske IT-virksomhet?

Figur 6-3: En vanlig brukt beskrivelse av skybaserte tjenester er den amerikanske standardiseringsorganisasjonen NIST sin “The NIST Definition of Cloud Computing”. Den deler skyen i fire, – privatsky for en brukergruppe, bransje-/sektor-sky for et avgrenset virksomhetsområde, offentlig sky med tjenester tilgjengelig for alle og hybridsky med en blanding av disse. For alle finnes det et sett av leveransemodeller og de deler de samme egenskapene og bygger på de samme teknologiene.



Dette åpner noen nye muligheter for forskningsnettene, og det er av vesentlig betydning å komme på offensiven her. Det pågår for tiden mye arbeid og tenking i IT-organisasjonene lokalt ved institusjonene, i UNINETT, i NORDUNET og i andre sammenhenger. Det er satt i gang arbeid med mange av de spørsmålene som må avklares: forholdet til lov- og regelverk, hvilke tjenester vil komme i hvilken skykonfigurasjon, driftsløsninger, betalingsmodeller, koplinger til andre skyer med mere.

Skyen og det den fører med seg, er den ene av de store omstillingene forskningsnettets virksomheten står overfor. Den andre er knyttet til den tette koplingen mellom IT og den faglige virksomheten ved institusjonene og i sektoren, det IT-strategiske aspektet nevnt ovenfor. Denne delen krever tett interaksjon og samhandling mellom fagmiljøene og IT-virksomheten. Dette er blant annet et tema i Terenas EARNest-studie fra 2008, og noe ligger også i *UNINETT strategi 2009–14* og andre plandokumenter. På dette området har forskningsnettene, inkludert UNINETT, fortsatt en vei å gå, og de vil være mer avhengig av tettere kontakt med institusjonenes IT-virksomhet enn de ellers har hatt.

Gjennom GigaCampus- og eCampus-programmene har UNINETT tatt steget ut til institusjonene og gjort campusnettet og campustjenester til et satsingsområde. Dette arbeidet har primært vært rettet mot institusjonene i høgskolesektoren og gitt institusjonenes IT-virksomhet et betydelig løft som de fleste av dem neppe hadde klart på egen hånd. I videreføringen av dette arbeidet må Forskningsnettet også finne sin rolle som støttespiller for den fagnære IT-virksomheten som drives ved de største institusjonene og spesielt universitetene. Det er her utviklingen har kommet lengst, det er i stor grad her løsninger utvikles og prøves og det er her det høstes lærdom og erfaringer som resten kan dra nytte av. Det vil være en stor oppgave for forskningsnettene å fange opp dette,

bearbeide og videreformidle det.

De to viktigste lærdommene

Etter snart 40 år med Forskningsnettet og arbeid med tjenester og ressurser for forskningen og utdanningen i landet og på lærestedene og institusjonene, har vi høstet to grunnleggende lærdommer.

Den ene lærdommen er at knapphet på goder gir feil fokus. Mangel på kapasitet, tilgang og funksjonalitet medfører at (grupper av) brukere leter etter muligheter for å gå rundt manglene og søke løsninger andre steder. Dette er den største trusselen mot det fellesskapet som er en forutsetning for formålstjenlig og hensiktsmessig bruk av IT i sektoren og på lærestedene og det første skrittet på en vei som leder til balkanisering av IT-virksomheten og framveksten av suboptimale løsninger. Det er ingen vei utenom å sørge for at brukerne får den kapasiteten som friksjonsfri bruk forutsetter og at de har enkel tilgang til de tjenestene og ressurser de trenger for å løse sine kort- og langsiktige oppgaver. Dette krever at IT-organisasjonene er tett på sine brukere og i stand til å fange opp behov helst før de manifesterer seg.

Den andre lærdommen er at IT-virksomhet er arbeidskraftkrevende. Umiddelbart ser dette ut som en selvmotsigelse, men ved nærmere ettertanke er det selvsagt. Alle oppgavene i arbeidet med IT-løsninger krever folk, – anskaffelser, installasjon, drift, vedlikehold, spesifikasjon, utvikling, testing, tilrettelegging, feilretting, dokumentasjon, informasjon, veiledning, opplæring, styring, planlegging og så videre. Og det krever folk med kompetanse og kunnskap. Uten folk og kompetanse oppstår rask en situasjon preget av knapphet, feil og utilgjengelighet, den tilstanden den første lærdommen sier at vi må unngå.

Utfordrende, men uansett går vi inn i interessante og krevende tider ...

Kan Internett redde verden?

Vi var entusiaster på Internettets vegne på 90-tallet. Det var lett å omfavne fenomenet og gi det tilnærmet guddommelig kraft. På et tidspunkt erklærte vi til og med uavhengighet fra den gamle verden i "*Declaration of the Independence of Cyberspace*" skrevet av John Perry Barlow (som en periode også var poet for Grateful Dead) og publisert av Electronic Frontier Foundation i 1996:

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

Ut av 90-tallet

Erklæringen kan på mange måter stå som minnesmerket over uskyldens tiår i Internettets historie. Vi var full av entusiasme og hadde stor tro på tiden som skulle komme. Vi forlot tiåret noe forvirret, noe urolig, lett omtåket og kunne ikke helt begripe hva det var som hadde truffet oss. Etter dot.com-bobla var det mye som ikke var helt i vater, og vi tok fatt på det nye tusenåret lett desillusjonerte.

Egentlig hadde vi ikke noen grunn til det. Rundt årtusenskiftet var det ryddet kraftig opp, – Internett rådde alene grunnen, standardene regjerte i større grad enn før, Moores lov produserte stadig vakrere tekniske løsninger på utstyrssiden og Linux og åpen programvare var på offensiven.

IT, IT-tjenester og Internett vokste ikke bare i omfang, de ble stadig viktigere og inntok en mer og mer sentral plass i alle deler av samfunnet utenfor universitetene og høyskolene. At KONTUR, tidsskriftet for lærerutdanningen, ga ut et dobbeltnummer om Internett og UNINETT i 1993 var unntaket, ikke mange utenom universitetene omtalte dette på den tiden. At Aftenposten, NRK og andre medier omtalte Internett i en eller annen sammenheng bortimot daglig, var normalen i 1999.

Fram mot år 2000 ble opplevelsen av at Internett ikke lenger var en fredelig og vennskapelig samling av stammen rundt leirbålet, påtrengende. Livet på nettet lignet mer og mer på det virkelige liv, fortiden var i ferd med å innhente framtiden og vise at den hadde innflytelse, myndighet og

makt. Gleder og sorger, oppturer og nedture, oppbygging og ødeleggelse, lovlidighet og kriminalitet, respekt og forakt gikk hånd i hånd også på Internett. Vi trodde vi etablerte Internett og Cyberspace i ubebodd område. Det viste seg at det var bebodd allerede, av de samme sosiale, kulturelle, politiske og økonomiske interessene, maktkonstellasjonene og konfliktene som ellers former vår hverdag, våre relasjoner og det lokale og globale samfunnet vi er del av.

Spam og annen uønsket oppmerksomhet ble noe vi ble tvunget til å leve med. Den første tiden kunne vi ikke gjøre så mye annet enn å observere at spammere og kverulanter oversvømte innboksen og raserte menings- og informasjonsutvekslingen i USENET Network News. Vi måtte også lære oss å leve med trusselen fra virus, ormer og annen ondsinnet programvare. Vi innså etter hvert at vi måtte beskytte oss og vår interaksjon på nettet. Dette ble spesielt åpenbart da de første nettbankene kom og det viste seg at de i sin tidlige versjon eksponerte både personinformasjon og kontoopplysninger for all verden. Sårbarheten i tjenester og løsninger åpnet også et 'marked' for halv- og helkriminelle handlinger. Nettet var plutselig et risikabelt sted å være.

Så var det sensuren og overvåkingen. De som i alle sammenhenger ønsker å kvele alle ytringer som kan provosere den alminnelige konsensus og bluferdighet, kom tidlig også på denne banen. Fra tid til annen kunne en ha lyst til å gi dem rett, nettet eksponerte uttrykk for noen av de mørkeste og nedrigste sidene av virkeligheten. Myndighetene og maktapparatet ønsket imidlertid ikke bare å overvåke oss, de ønsket å kunne kikke oss i kortene til enhver tid, og overvåkerne mislikte sterkt utviklingen av krypteringsløsninger og andre tiltak som vanskeliggjorde deres virksomhet. Og Napster, fildeling, MP3 og framveksten av P2P-nett brakte krefter med stor makt og betydelige økonomiske muskler på banen.

Vi så det kanskje ikke godt nok den gang, men den smule korreksjon og realitetsorientering dette medførte var nyttig. Vi innså at vi kunne ikke melde oss ut av verden, vi var allerede dratt rett inn i sentrum av vesentlige samfunnsmessige prosesser og vi måtte begynne å handle deretter.

Teknologi er verken god eller ond, og er heller ikke nøytral

I de siste 10-15 årene har Internett vært allemannseie. Det har vært en velsignelse og en sann fryd og gitt oss tjenester og løsninger som på mange måter har gjort livet enklere og morsommere for de aller fleste av oss. Samtidig er det viktig å huske at vi *også* har gjort livet enklere for dem som er ute etter bombardere oss med reklame, tjene penger på oss, svindle oss, stjele våre verdier, overvåke oss, utnytte oss, skaffe seg urettmessig tilgang til ressurser vi disponerer og mange andre handlinger som vil ramme oss på måter vi ikke ønsker og knapt er i stand til å overskue. Det er ikke alltid denne siden av Internett og IT kommer fram i medias og bransjens omtale. Det er heller ikke alltid slik at vi reflekterer over dette når vi gjør våre overveielser og valg om hva vi bruker nettet til, hvordan vi opptrer der og hva vi legger igjen etter oss av informasjon og spor.

Siden det i Internettets historie har vært entusiastenes fortellinger som har preget offentligheten, passer det bra å avslutte denne fortellingen med å trekke fram noen forfattere og analyser som balanserer dette bildet. Ved å gi et lite innblikk i noen av disse, er håpet å pirre interessen for å undersøke dette nærmere og fremme refleksjon om de utfordringene vi står overfor som daglige og avhengige brukere av IT og Internett. Tiden er nå inne for å tenke gjennom også disse sidene ved vår virksomhet, den praksisen vi utvikler, de valgene vi gjør, og de konsekvensene det har for dagligliv, arbeidsliv og samfunnsliv.

Lawrence Lessig

For mange av oss var Lawrence Lessigs bøker *"Code and other Laws of Cyberspace"* fra 1999 og *"The Future of Ideas – The Fate of the Commons in a Connected World"* fra 2002 den første åpenbaringen. Lessig var av de første som utfordret den utbredte forestillingen om Internett som 'frihetens eldorado', som et sted hverken myndigheter eller andre kunne kontrollere eller regulere:

I believe that these first thoughts about Internet and cyberspace are just as misguided as the first thoughts about government after communism. Liberty in cyberspace will not come from the absence of the state. Liberty there, as anywhere, come from a state of a certain kind. We build a world where freedom can flourish not by removing from society any self-conscious control; we build a world where freedom can flourish by

setting it in a place where a particular kind of self-conscious control survives. We build liberty, that is, as our founders did, by setting society upon a certain constitution.

But by “constitution” I don’t mean a legal text. [...] I mean an architecture – not a legal text but a way of life – that structures and constrains social and legal power, to the end of protecting fundamental values – principles and ideals that reach beyond the compromises of ordinary politics.

Constitutions in this sense are built, they are not found, Foundations get laid, they don’t magically appear.

Mangelen på sentral kontroll og regulering var et arkitekturmessig karaktertrekk ved Internett nedfelt i prinsippene for ‘*end-to-end networking*’ og ‘*stupid networks*’. For Lessig var ikke dette en grunnleggende, uforanderlig egenskap ved Internett, men et valg som ble gjort. En uheldig allianse mellom et nærings- og forretningsliv som ønsket å bruke Internett som markedsførings- og salgskanal og en stat som ønsket mer oversikt over hva borgerne tillater seg å gjøre, var ifølge ham i ferd med å gjøre om denne arkitekturen til en arkitektur som kunne muliggjøre perfekt kontroll og regulering:

Not necessarily control by government, and not necessarily control to some evil, fascist end. But the argument of this book is that the invisible hand of cyberspace is building an architecture that is quite opposite of what was at cyberspace’s birth. The invisible hand, through commerce, is constructing an architecture that perfects control – an architecture that makes possible highly efficient regulatory control.

[...]The regulator is the obscurity in the book’s title – Code. In real space we recognize how laws regulate – through constitutions, statutes, and other legal code. In cyberspace we must understand how code regulates – how the software and hardware that make cyberspace what it is, regulate cyberspace as it is.

Lessig er jurist med spesiell interesse for opphavsrett til åndsverk og brukte dette som lærestykke. På den tiden bøkene kom, var kontroversene om Napster, fildeling og tilgrensende fenomener og reaksjonene på dette fra mediebransjen og spesielt plateselskapene på sitt mest intense. I beskrivelsene av de tekniske løsningene som ble lansert i kjølvannet av dette, illustrerte han sine poenger ved å vise hvordan disse forrykket balansen ved å styrke rettighetshavernes interesser og makt på bekostning av allmennhetens.

Lessig var forøvrig en viktig bidragsyter til utviklingen av Creative Commons, en formulering av opphavsretten som, under gitte betingelser, gir andre lov til å dele og bygge videre på et åndsverk. Dette er en lisens Lessig har lagt på sine bøker, noe som innebærer at bøkene er tilgjengelig for nedlasting.

Bruce Schneier

Allerede før utgivelsen av bøkene “*Secrets and Lies – Digital Security in a Networked World*” (2000), “*Beyond Fear – Thinking Sensibly About Security in an Uncertain World*” (2003), hadde vi erfart at Internett og cyberspace ikke var ufarlige steder å bevege seg. Bøkene kom på et tidspunkt da mange slet med å forstå hva sikkerhet i Cyberspace og på Internett innebar:

The goal of this book is to demystify security, to help you move beyond fear, and give you the tools to start making sensible security trade-offs. When you’re living in fear, it’s easy to let others make security decisions for you. You might passively accept any security offered to you. This isn’t because you’re somewhat incapable of making security trade-offs, but because you don’t understand the rules of the game.

When it comes to security, fear is the barrier between ignorance and understanding. To get beyond fear, you have to start thinking intellectually about the trade-offs you make. You have to start evaluating the risks you face, and the security options you have for dealing with those risks. There’s a lot of lousy security for purchase and a lot of lousy security being imposed on us. Once you move beyond fear and start thinking sensibly about trade-offs, you will be able to recognize bad or overpriced security when you see it. You will also be able to spot inefficient security – and explain why it’s ineffectual. (fra “Beyond Fear”)

Det Schneier først og fremst lærte oss, var at sikkerhet i den digitale verden hadde akkurat de samme problemstillingene og utfordringene som sikkerhet i den virkelige verden. For det *første* at sikkerhet forutsetter en avveining der sikkerhet veies mot brukervennlighet og kostnader. For det *andre* er sikkerhet blitt mer krevende siden kompleksiteten i våre systemer øker, systemene koples i

større grad sammen og samvirker, systemene brukes til andre ting og har konsekvenser som ikke var forutsatt ved etableringen, og systemene er lagd av mennesker og har med nødvendighet feil. For det *tredje* dreier sikkerhet seg om tre ting som alle må inngå i sikkerhetstiltakene vi iverksetter, – beskyttelse og sikring, kontroll og overvåking, og reaksjon og oppfølging. For det *fjerde* teller konteksten – det som skal sikres, og hva som er relevante trusler mot det – mer enn teknologi.

Technology alone cannot save us. Products have problems, and they are getting worse. The only thing reasonable to do is to create processes that accept this reality, and allow us to go about our lives as best as we can. It's no different from any other aspect of society.

[...]Security is not a product; it's a process. You can't just add it to a system after the fact. It is vital to understand the real treats of a system, design a security policy commensurate with those treats, and build in appropriate security measurements from the beginning.

Og han lærte oss å stille de riktige spørsmålene:

- Hvilke verdier er det som skal beskyttes?
- Hva er truslene mot disse verdiene?
- Hvor godt vil sikringstiltak beskytte mot disse truslene?
- Introduserer sikringstiltakene andre risikoer og trusler?
- Hva er kostnadene ved tiltakene og hvilke konsekvenser har de?

Jonathan Zittrain

I boka *“The Future of the Internet, and How to Stop It”* viderefører Jonathan Zittrain deler av tankegodset fra Lessig. For Zittrain er Internett og PC-en som *generativ* teknologi det sentrale. De arkitekturvalgene som ble lagt til grunn for utviklingen av både PC-en og Internett, fremmet løsninger som tilrettela for og oppfordret til å bli plukket på av brukeren:

Both platforms were released unfinished, relying on their users to figure out what to do with them, – and to deal with problems as the arose.

For Zittrain var denne uferdigheten årsaken til begges suksess og forutsetningen for den innovasjonen som ga mange av de gode løsningene som er utviklet på disse plattformene. Samtidig er denne åpne arkitekturen også mottakelig for trusler mot den selvsamme arkitekturen, spesielt truslene knyttet til sikkerhet. Etter hvert som truslene økte og sikkerhetsproblemene eskalerte, ble brukerne mer villige til å gi fra seg den friheten generativiteten ga dem i bytte mot bedre sikkerhet:

The first reaction to abuses of openness is to try to lock things down. One model for lockdown can be drawn from our familiar appliances, which are sealed when they leave the factory (...), and we've seen glimpses of that model in communications platforms like iPods, most video game consoles, e-book readers like the Amazon Kindle, and cable company set-up boxes. Such lockdown was the direction a visionary Steve Jobs – the guy who gave us the first open PC, the Apple II – first took with the iPhone, with which he bet the future of Apple.

[...] But there's another model for lockdown that's more subtle, and that takes, well, a book to unpack. This new model exploits near-ubiquitous network connectivity to let vendors change and monitor their technologies long after they've left the factory – or to let them bring us, the users to them, as more and more of our activities shift away from our own devices and into the Internet 'cloud'.

Eli Pariser

I et større oppslag i Dagens Næringsliv i januar 2013 ble det vist hvordan Google svarer forskjellig avhengig av hvem som spør. Grunnen til dette er at Google, på linje med Facebook, Apple, Yahoo, Microsoft og en rekke andre tjenester vi bruker, vet mye om oss, vår bakgrunn, vårt virke, våre vaner og interesser og bruker denne kunnskapen til å filtrere informasjonen og tilpasse svarene de gir oss. Dette er tema i Eli Parisers bok om *“The Filter Bubble – What the Internet Is Hiding from You”* fra 2011:

[...] the rise of pervasive, embedded filtering is changing the way we experience the Internet and ultimately the world. At the center of this transformation is the fact that for the first time it's possible for a medium to

figure out who you are, what you like, and what you want. Even if the personalizing code isn't always spot-on, it's accurate enough to be profitable, not just by delivering better ads, but also by adjusting the substance of what we read, see and hear.

As a result, while the Internet offers access to a dazzling array of sources and options, in the filter bubble we'll miss many of them. While the Internet can give us new opportunities to grow and experiment with our identities, the economics of personalization push towards a static conception of personhood. While the Internet has the potential to decentralize knowledge and control, in practice it's concentrating control over what we see and what opportunities we're offered in the hands of fewer people than ever before.

Resultatet er at vi blir presentert for en boble vi kan trives i. I denne bobla er vi alene, bobla er usynlig for oss og vi velger ikke selv å gå inn i den, men det er få veier utenom i vår jakt på informasjon og opplevelser på Internett. I følge Google-direktør Eric Schmidt er drømmen å bygge et Google som ikke bare kan “*guess what I'm trying to type*”, men også “*tell what I should be doing next*”. Hva dette vil gjøre med våre oppfatninger og kunnskaper, vår evne til å lære, forstå og reflektere og vår evne til å gjøre gode valg og velbegrunnede beslutninger, er ikke vanskelig å forestille seg.

På vår ferd gjennom Internett blir våre bevegelser og vår atferd registrert sammen med informasjon vi bevisst eller mest sannsynlig ubevisst legger igjen. Facebook har drevet dette enda lenger og vet snart mer om hver enkelt av oss og våre relasjoner enn vi vet selv. Denne informasjonen benyttes av algoritmer til å forutse hva som vil behage oss og imøtekomme våre behov og interesser best mulig. Det startet med systemer for å personalisere annonser og endte opp med systemer som presenterer for oss tilpasset informasjon og et tilpasset verdensbilde:

We're never bored. We're never annoyed. Our media is a perfect reflection of our interests and desires.

Tim Wu

Tim Wu bretter ut det store lerretet i “*The Master Switch: The Rise and Fall of Information Empires*” fra 2012. Her gir han en framstilling av den historiske utviklingen av massemediene, – telegraf og telefon, radio, fjernsyn, film. Gjennom dette mener han å ha avdekket et mønster i utviklingen, et mønster han kaller “*The Cycle*”:

History shows a typical progression of information technologies from someone's hobby to someone's industry; from jury-rigged contraption to slick production marvel; from a freely accessible channel to one strictly controlled by a single corporation or cartel – from open to closed system. It is a progression so common as to seem inevitable, though it would hardly have seem so at the dawn of any of the past century's transformative technologies, whether telephony, radio, television, or film. History also shows that whatever has been closed too long is ripe for ingenuity's assault; in time a closed industry can be opened anew, giving way to all sorts of technical possibilities and expressive uses for the medium before the effort to close the system likewise begins again.

Det store spørsmålet han reiser, er om Internett er i stand til å bryte denne syklusen og stå imot presset som går i retning av monopolisering og lukkede systemer og løsninger:

Our future is almost certain to be an intensification of our present reality; greater and greater information dependence in every matter of life and work, and all that needed information increasingly travelling a single network we call the Internet. If the Internet, whose present openness has become a way of life, should prove as much subject to the Cycle as every other information network before it, the practical consequences will be staggering. And already there are signs that the good old days of a completely open network are ending. To understand the forces threatening the Internet as we know it, we must understand how information technologies give rise to industries and industries to empires.

Evgeny Morozov

Evgeny Morozov er hviterusser og bosatt i USA. Han er en både fargerik og kontroversiell skribent og en spissformulert forfatter som nok litt for ofte gjør potensielt nære venner og allierte til sine største fiender. I boka “*The Net Delusion – How Not to Liberate the World*” fra 2011 går han til krig mot alt som smaker av det han omtaler som ‘cyber-utopisme’ og ‘Internett-sentrisme’ og all tro på at Internett kan redde verden, fremme demokrati og rettsstat og frigjøre folk fra undertrykkende

regimer av alle slag.

Morozov går til krig mot framstillingene av opprørene i Iran og Midt-Østen som 'Twitter Revolution' og 'Facebook Revolution' med spissformuleringer som:

All by itself, the Internet provides nothing. In fact, as has become obvious in too many contexts, it empowers the strong and disempowers the weak.

Twitter don't topple governments, people do.

After all, modern technologies abet all revolutions, not just those that are decidedly pro-western in character.

American pundits goes to talk shows, Iranian bloggers goes to prison.

For Morozov er det viktig å fortelle at å klikke "Like" på en Facebook-side ikke endrer verden. Et annet og viktigere poeng er at autoritære regimer og ledere er ikke dummere enn deres motstandere. De har vist at de i forbausende grad er i stand til å bruke teknologi for egne formål, og de har betydelige ressurser å sette inn for å bruke teknologien til propaganda, sensur og overvåking. Ikke nok med det, Internett og informasjonsteknologien har gjort denne virksomheten langt enklere og billigere, og det er nok av store foretak og organisasjoner som hjelper de autoritære regimene i dette arbeidet. For Stasi og andre apparat for undertrykking ville Internett og sosiale medier vært en gullgrube. Å undervurdere autoritære regimers og lederes evne til å utnytte den samme teknologien som fremmer opposisjonen og opprøret, fører med nødvendighet til katastrofer for dem som står i frontlinja. Det vet de opposisjonelle i Iran, som iransk politi identifiserte ved hjelp av opptak og meldinger som ble publisert på YouTube, Facebook, Twitter og andre medier under den "den grønne revolusjonen" i 2009.

Et hovedpoeng for Morozov er at teknologi bidrar til endring, men disse endringene er ikke bestemt av teknologien selv, men av de politiske, sosiale, kulturelle og økonomiske omgivelser teknologien utfoldes innenfor:

Information does not flow in a vacuum, but in a political space that is already occupied.

Panopticon – Internett overvåket

Lessig og andre argumenterer sterkt for at arkitekturen Internett bygger på, gradvis endres i retning av å bli et system for perfekt regulering og kontroll. Pariser redegjør for hvordan ulike aktører samler inn massive mengder informasjon om oss for å kunne presentere oss for en virkelighet tilpasset våre interesser og behov til enhver tid. Morozov beretter om en virkelighet der Internett og teknologi like gjerne kan brukes til undertrykking som til frigjøring, og der Internett brukes i varierende grad og til tider med stort hell av makthavere overalt på kloden til propaganda, sensur og overvåking.

Helt på slutten av arbeidet med denne fortellingen, kom avsløringene av at amerikanske etterretnings- og overvåkingsorganer hadde sikret seg tilgang til trafikkdata hos den største mobiloperatøren i USA (Verizon) og til all trafikk hos store tjenesteleverandører som Google, Facebook, Microsoft, Apple og Yahoo. Overvåkingsprogrammet *PRISM* viste seg å ha pågått siden 2007 med hjemmel i *Patriot Act*, lovgivingen som i kjølvannet av terroranslaget 11. september 2001 ga overvåkings- og etterretningsmyndighetene svært utvidete fullmakter.

En motivasjon for massiv overvåking av befolkning og virksomheter finnes hos myndigheter, politi, overvåkings- og etterretningstjenester i de aller fleste land. At det har skjedd og skjer i autoritære regimer, er velkjent. Utallige avsløringer viser imidlertid at sikkerhetstjenester også i vestlige demokratier er villig til å gå svært langt i denne retningen, langt utover hva lovverk og offisiell politikk tilsier. Overvåking og kontroll med kommunikasjon er en viktig, om ikke den viktigste delen av overvåkings- og etterretningsvirksomheten. Begrunnet i behovet for å bekjempe alt fra barnepornografi og narkotikatrafikk via økonomisk kriminalitet til terror, er grensene for hva disse virksomhetene kan drive med av overvåking og etterretning, utvidet betydelig det siste tiåret. Hvor mye vet vi ikke sikkert, for informasjonen om dette er hemmeligstempelt, – naturligvis.

I utallige filmer og TV-serier ser vi agenter, hackere og andre representanter for både venner og fiender bruke nettet til å skaffe seg informasjon, overvåke og på andre måter utføre sine oppgaver

enten det er å begå eller bekjempe forbrytelser. Det meste er skrikende urealistisk. Samtidig trigger det spørsmål om noen har mulighet til å overvåke hele Internett og hvor realistisk og sannsynlig dette er. På Black Hat-konferansen i USA i 2009 ble det presentert en undersøkelse av hva som må til for å oppnå dette:

- Kapasitet og mulighet til å tappe trafikken
- Kapasitet til å overføre dette til et egnet sted
- Kapasitet til å lagre trafikken
- Kapasitet til å analysere innsamlete data og gjøre nytte av den

Bare det første punktet alene tilsier at det eneste landet som har mulighet til å overvåke hele Internett, er USA. Årsaken til dette er at de store Internett-tjenestene er hjemmehørende der, og at mesteparten av trafikken i Internett går innom dette landet. Ved å analysere trafikken slo foredragsholderne fast at for å tappe opptil 90 % av denne trafikken holder det med tilgang til et trettitalls av de undersjøiske fiberkablene som binder Internett på den vestlige og østlige halvkule sammen. Tilgang til å tappe trafikken som flyter gjennom mindre enn ti av de sentrale samtrafikkpunktene (IX-ene), gir ytterligere muligheter. Disse tilgangene vil overvåkerne lett få fra AT&T som er til stede på de fleste av disse punktene, og som i dag spiller en like sentral rolle i amerikansk etterretning som firmaet gjorde under den kalde krigen.

Den neste utfordringen er å lagre og overføre de enorme datamengdene som tappes. Med dagens tekniske løsninger for å filtrere og komprimere informasjon er det fullt mulig å redusere datamengden til et nivå som enkelt kan overføres til et sted for lagring og analyse. At National Security Agency (NSA) bygger et gigantisk anlegg i ødemarken i Utah i USA er velkjent. Dette anlegget skal ifølge ulike kilder være i stand til å lagre all innhentet kommunikasjon i hundre år. På det samme anlegget og på en rekke andre steder, finnes mer enn nok maskinkraft til å søke i og analysere denne informasjonen.

I presentasjonen på Black Hat-konferansen gjøres det overslag som viste at dette ville kostet 4.4 milliarder USD (+/-0.5 millioner USD) i 2009-priser, noe som er klart innenfor økonomisk rekkevidde for en organisasjon som NSA. En ukjent joker i dette er ressursene som kreves for å dekryptere kryptert kommunikasjon. Det antas at overvåkerne foreløpig ikke er i stand til å dekryptere denne, med mindre de har bakdører som kan avsløre krypteringsnøkler. Alene det faktum at kommunikasjonen er kryptert, er imidlertid nok til å vekke overvåkernes interesse.

Motivasjonen for massiv overvåking har vært til stede i lang tid. At det er innenfor økonomisk rekkevidde, gjør at det er ganske så naivt å tro at slik overvåking ikke skjer. Men det er kanskje ikke den internasjonale overvåkingen som er den viktigste. Vel så viktig er overvåkingen som skjer lokalt i det enkelte land. Makthaverne i land med mindre utbygd infrastruktur, færre operatører og sterkere kontroll med kommunikasjonstjenestene står overfor en mye enklere oppgave. I land som Russland, Kina, Iran, de tidligere Sovjet-republikkene, Pakistan, Saudi-Arabia og hele cocktailen av autoritære regimer kloden rundt skjer det en massiv overvåking og kontroll av Internett-trafikk, og dette brukes konsekvent og aktivt for å styrke regimenets grep om makta over eget land og folk. At tilsvarende ikke skulle være interessant også for myndigheter og etterretningsvirksomhet i våre vestlige demokratier, er like usannsynlig som at jorda skulle vise seg å være flat allikevel.

Benthams Panopticon var et fengsel der alle cellene kan overvåkes fra ett punkt, men ingen av de innsatte vet på noe tidspunkt om deres celle er under overvåking. På Internett lever vi i et gigantisk, desentralisert Panopticon, vi vet de er der, vi vet de er aktive, vi vet at de vil vite mest mulig om oss, men vi vet aldri hvem de er og om akkurat vi blir overvåket og kartlagt.

Dette er ikke slutten

Det er mange sider ved både Forskningsnettet og Internett i Norge og globalt som hadde fortjent en omtale, men på ett punkt må vi sette en sluttstrek for denne fortellingen. Det skjer i trygg forvisning om at både Forskningsnettet og Internett fortsatt vil være med oss og fortsatt vil prege vår hverdag, våre relasjoner og vår framtid. Det er en virkelig verden der ute, en verden der det er viktig å forstå

hva som skjer både i solskinnet og i tussmørket og der vi må opptre som helter for å kunne leve et alminnelig, anstendig liv. Derfor passer det å avslutte på samme måte som vi startet, – med meldingen fra Grateful Dead i “Truckin’” på LP’en “American Beauty”:

Truckin’**Sometimes the light's all shinin' on me****Other times I can barely see****Lately it occurs to me, what a long strange trip it's been****Truckin', I'm goin' home, back where I belong****Back home, sit down and patch my bones, and get back truckin' on**

Publisert 1. jan. 2014 13:32 - Sist endret 16. jul. 2014 12:10

Innhold:

[En mer brukernær og strategisk IT-virksomhet](#)

[Kan Internett redde verden?](#)