

Informasjonssikkerhet som bidrag til *resiliens* i helsesektoren?

***Keiserens nye klær eller veien til trygge
informasjonssystemer ?***

HelsIT Prekonferanse, 26-09-2006

Tor Olav Grøtan, NTNU/SINTEF

”Alt henger sammen med alt” (GHB)

Trygge informasjonssystemer i helsesektoren ?

Resiliens (*resilience*)

*Information Technology in
Resilient Global Logistics*

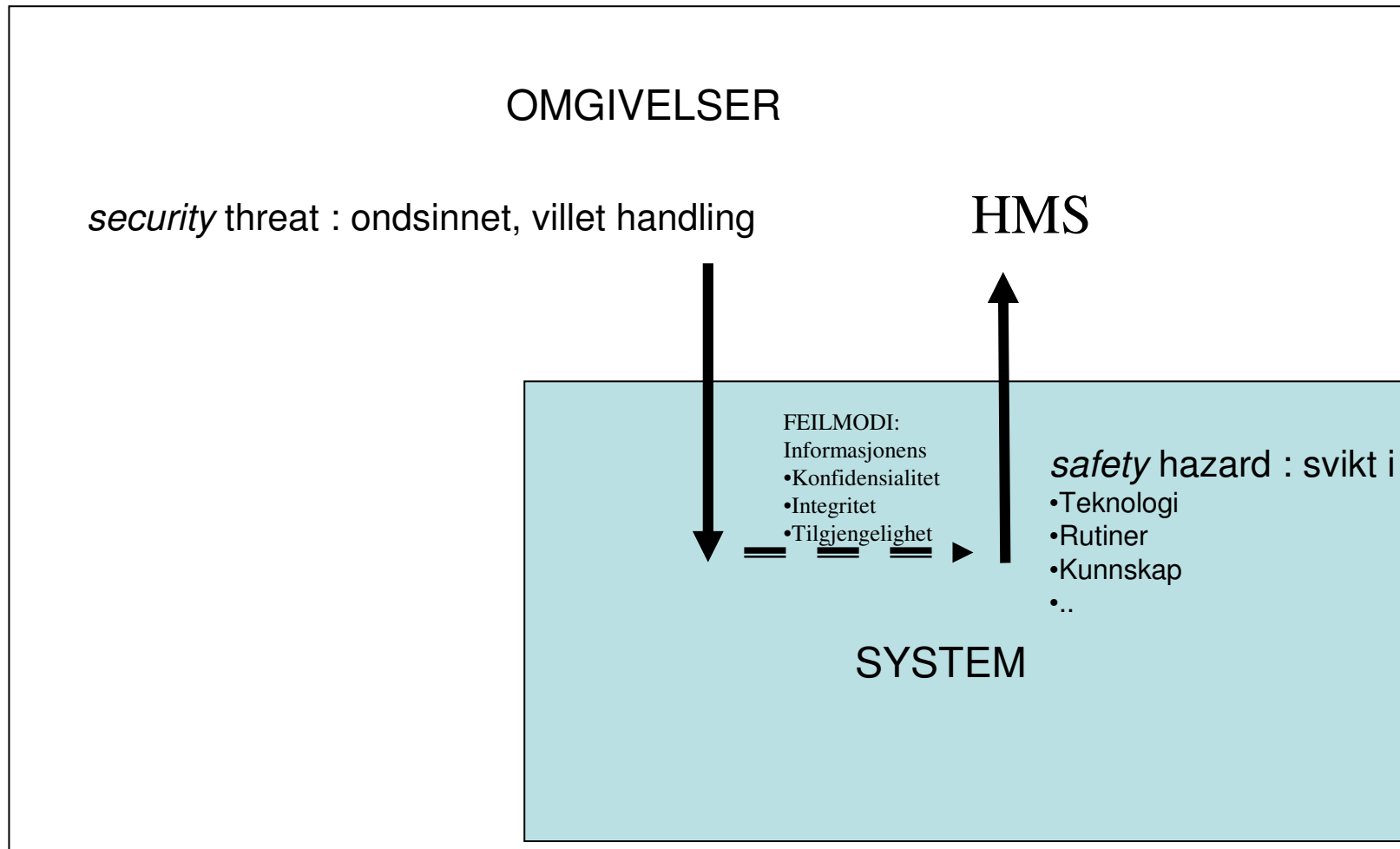
IT-/informasjons-sikkerhet

safety

security

industriell sikkerhet

Sikkerhet som begrep: *safety* og *security*



Informasjonssikkerhet = information *security* (?)

Sikkerhet: metoder

- Safety: Risikoanalyse og –håndtering: et bredt spekter av teknikker og metoder
 - Sjekklistor
 - Risikomatriser
 - Risiko = Sannsynlighet x Konsekvens
 - Risikomodeller med ulike detaljeringsgrader, e.g.
 - Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA), Failure Mode Effect and Criticality Analysis (FMECA), +++
 - Risikoindikatorer
 - Fokus på *sikkerhetsbarrierer* : tiltak som demmer opp for årsaker/konsekvenser
 - Beregninger/simuleringer med implikasjoner for dimensjonering, vedlikehold etc
 - Betyggende for den som "bor på en bombe"
- Safety management : (Teknisk) styring, oppfølging, kvalitetssystem
- Informasjonssikkerhet : kopierer safety, men uten å overdrive innsatsen....
 - E.g. risikomatriser i ulike formater
 - Barrierer (e.g. "brannmur" : metaforikken viser forbindelsen tilbake til *safety*)
 - Security Management: ISO17799, Personopplysningsforskriften
 - By default: maskinbyråkratisk organisasjonsforståelse
 - Organisatoriske effekter av IKT "finnes ikke", teller ikke. !!!

Retrospektiv sikkerhet

- Sikkerhetsarbeid har ofte (alltid?) vært preget av etterpåklokskap
 - Drives fram av uønskede hendelser.
 - Den naturlige motivasjonen er å hindre at det skjer igjen
 - Den økonomiske horisonten er imidlertid (for) kort
 - Vi vil finne ut hva som har skjedd, forsøke å gjøre verden forståelig (igjen)
 - Vi føler oss ”dømt” til å se på framtiden i lys av fortiden
 - Men glemmer Kierkegaard: ”*livet må leves forlengs men forstås baklengs*”
- Forhistorien preger antakelser og forberedelser mht fremtidige feil
 - Undertrykker den nødvendige ”imageringen” av nye muligheter
- Tradisjonelle tilnærminger til sikkerhet og risikoprediksjon er *inkrementelle*
 - De velprøvde løsningene endres først når noe feiler, og da vanligvis med å legge til én ny faktor i årsaksrekken som forklarer det (hittil) uforklarte
 - Lett å peke på menneskelig svikt, organisatorisk svikt, ”sikkerhetskultur”, selvtilfredshet etc
 - Vanlig prinsipp: Vi legger til eller endrer *akkurat så mye* at vi kan forklare hendelser som til da ikke kunne forklares av det fundamentale rammeverket

Hvorfor *Resilience Engineering* ?

- *Resiliens* er en betegnelse på ulike måter for å overkomme begrensninger i eksisterende tilnærminger til risiko og systemsikkerhet
- Innsikt etter mange år med ulykkesgranskning: ulykker og uheldige hendelser skyldes ikke enkeltfaktorer og/eller lineære forløp, men uheldige *kombinasjoner*
- Ulykker er baksiden av suksesser, det trengs ingen spesielle mekanismer for å forklare ulykker (*forklares på samme grunnlag*)
- Suksess er ikke bare et resultat av god planlegging. *De fleste suksesser er ikke planlagt slik de faktisk blir gjennomført*
- *Resiliens* presenteres dermed som et "paradigmeskifte"(!) med et annet vokabular enn tradisjonell sikkerhets- og risikotenkning

Hva er nytt med *Resilience Engineering* ? (1)

- Sikkerhetsforskning: måter å kompensere for utilstrekkelig eller feilaktig menneskelig atferd som ellers degraderte et "sikkert" system.
 - Pålitelighetsteori og management science → "demonstrably safe systems"
- Jens Rasmussen og andre snudde det hele og viste at operatørene ga et positivt bidrag, ved å dekke opp hullene i designet
 - Analysene viste gap mellom formelle arbeidsbeskrivelser og faktisk arbeidspraksis
- "Second stories" viste at feil handlet om *sammenbrudd i tilpasningene til kompleksitet*
 - En suksess er ofte implementert annerledes enn den er planlagt !
- Tidspresset er en fiende
 - Effektivitet uten grundighet skaper betingelser for ekstrem sensitivitet for små avvik
 - NASAs *FasterBetterCheaper* (FBC) og søken etter "Silver Bullets" ("best practice") viste seg å være fatal

Hva er nytt med *Resilience Engineering* ? (2)

- Sikkerheten er ikke en vare som kan bli tabulert og ”dokumentert”
 - Ikke nok å innføre tiltak som reduserer ”antallet” feil
- Sikkerhet er en ”dynamisk ikke-hendelse” (Karl Weick)
- Sikkerhet skapes gjennom resiliente, proaktive prosesser i stedet for gjennom reaktive barrierer og forsvarsverk
 - Studér fuglene på fuglebrettet!
- En resilient organisasjon behandler sikkerhet som en kjerneverdi, ikke som en eiendel eller et telleverk
- En resilient organisasjon bruker ikke gårsdagens suksess til å redusere morgendagens bestrebelser ift sikkerhet!

Emergens og resiliens (1)

- Etiologier om ulykker
 - Dominomodell (enkel lineær)
 - Sveitserostmodell (kompleks lineær)
 - I et resiliens-perspektiv er *concurrency* en temporær tilstand der flere ting skjer samtidig (jfr Perrowske normalulykker)
 - **Funksjonell resonans**
 - Endogen/eksogen variabilitet
- Variabilitet i ytelse/funksjon er *nødvendig* fordi
 - Både feil og normalitet er *emergente* (fremvoksende) fenomener
 - **Normal** ytelse er forskjellig fra **normativ** ytelse
 - Normal ytelse representerer en **likevekt** som avspeiler en regularitet
 - Ikke-intenderte effekter av handling skyldes variasjoner i kontekst
 - Menneskelig tilpasning og fleksibilitet er *forklaringen* på ”normalitet”
 - Feil oppstår når man *løser feil problem* på ”normal” måte
- Hvordan overvåke variabilitet i beslutninger for å avdekke at ”feil” problem løses?

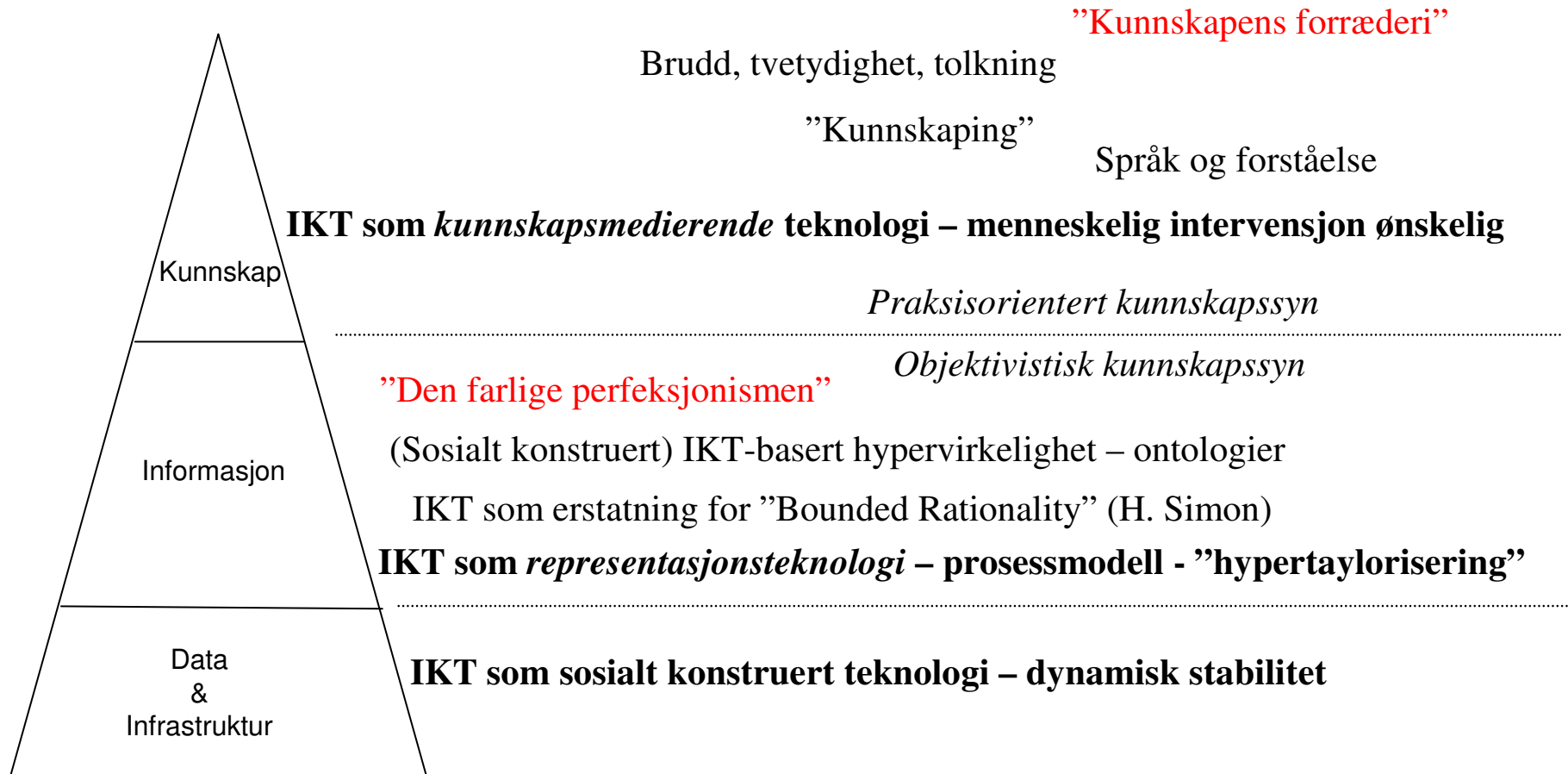
Emergens og resiliens (2)

- Dynamisk stabilitet er suksessfaktoren
- Den virkelige utfordringen er å innse at dynamisk stabilitet noen ganger kan endres til dynamisk *instabilitet*
 - Plutselig eller gradvis (emergent)
 - Endring/tilpasning må ikke komme ut av kontroll
 - Et mer nyansert syn på endring er nødvendig
 - Tekniske artefakter er aldri "nøytrale", kan ikke substitueres uten videre
- **Resiliens: Keiserens nye klær ?**

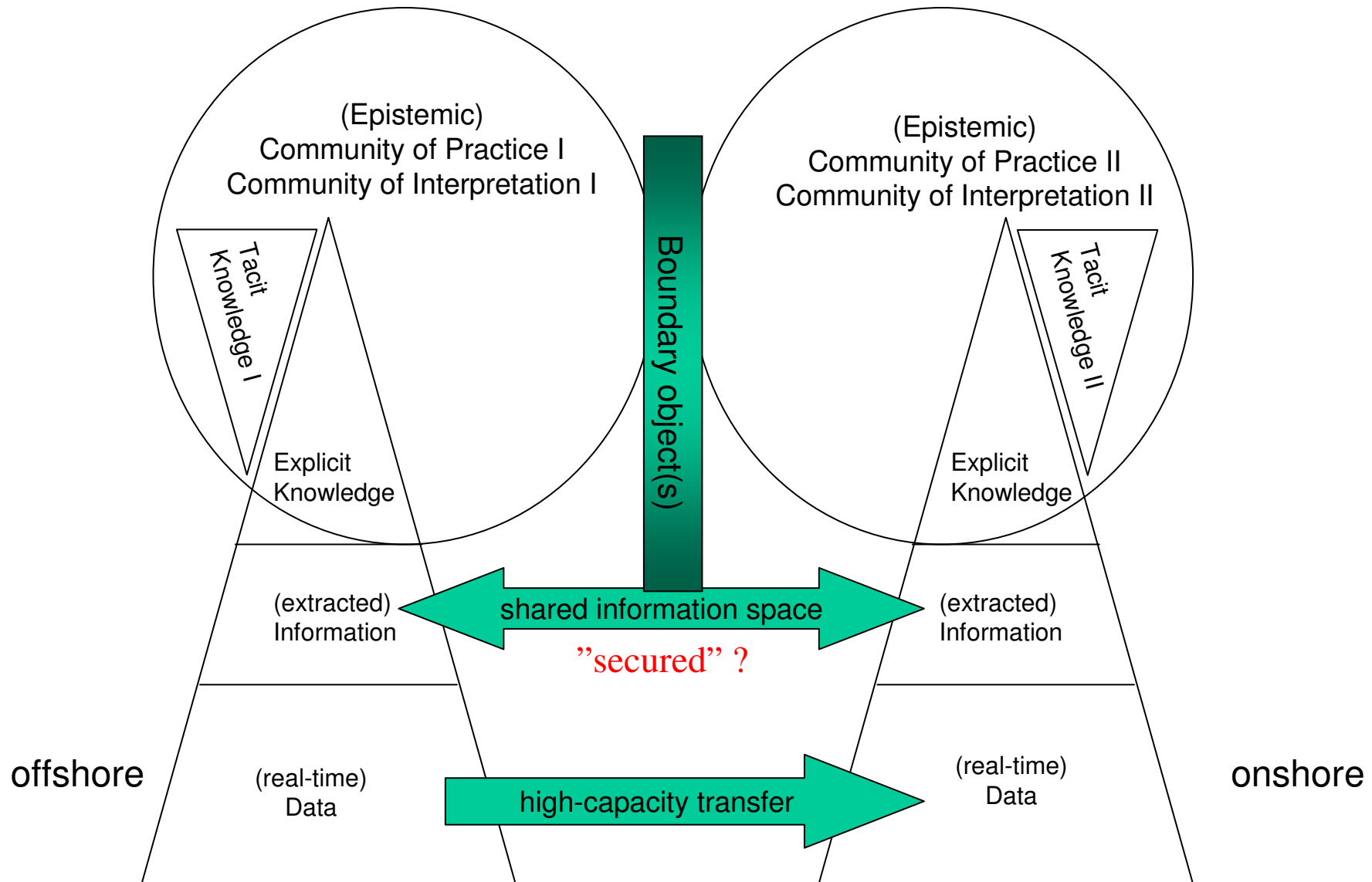
Eksempel på resiliens i aksjon

- Snorre A hendelsen i Nordsjøen – november 2004
 - 80.000 dødvekt-tonn
 - Produserte gass for 200.000.000 NOK per dag
 - Kunne blitt den alvorligste hendelsen på norsk sokkel
 - Årsaken var at sikkerheten hadde forvitret på "alle" plan
 - Granskning ved NTNU Samfunnsforskning
 - Ekstrem "*resiliens*" berget situasjonen i siste øyeblikk!
- Sikkerhet og resiliens bør helst kunne eksistere sammen!
- Hypotetisk spørsmål:
 - Kunne resiliens berget St.Olavs IP-situasjon ?
 - Hva er mest komplekst: En ukontrollert gassbrønn under beina, eller IP-nettet i en helseregion ?

IKT i *Resilient Global Logistics*. Epistemiske skiller, analytiske modeller



Boundary objects provide *sufficient* coherence (bridging epistemic differences)
RISK scenario: from dynamic stability to dynamic instability in cooperation



Er informasjonssikkerhet et bidrag til resiliens i helsesektoren i dag ?

- I utgangspunktet: NEI
- Er definert gjennom tradisjonell *safety*. Fokuserer primært på data/infrastruktur
- Sviktende infrastruktur f.eks "IP-ulykker" = "**common-cause failure by design**" ?
 - Hvem forsikret seg om at denne enkelt-komponenten var/er høypålitelig, feiltolerant og robust ?
- Er f.eks patche-regimer et uttrykk for resiliens ?
- Tilgang til pasientinformasjon *kunne* åpenbart bidratt til resiliens ift pasientbehandling!
 - Men kan også være en sovepute ("systemet gir meg det som er viktig")
- Pasientjournalen som *hypervirkelighet* : ingen vesentlige motforestillinger ?
 - Omnipotente informasjonssystemer bidrar til den "farlige perfektionismen"
- *Kunnskapens forræderi* er et sosialt konstruert selvbedrag
 - "Flytende akseptkriterier"
 - Resiliens må tuftes på tvetydighet, imaginering av andre muligheter, kritisk sans og dissens
- "**Knowledge can only appear as manageable if one actively maintains ignorance of this diversity and its history**" (Lilley/Lightfoot/Amaral, 2004. *Representing Organizations. Knowledge, Management and the Information Age*)
 - Et valg som gjør at informasjonssikkerheten forblir reaktiv, og ikke bidrar til resiliens
 - Perspektivet kan også anvendes på IP-problematikken
 - den tekniske infrastrukturen som "pasient"
- "Resilient" informasjonssikkerhet må understøtte (de sosiale) kunnskapsprosessene, ikke bidra til forsøket på å låse kunnskapen inne i datamodellene

Personvernets rolle og vilkår ?

- Et lite forbehold: 3 års "pause" fra helsevesenet
- Datatilsynet: Pådriver for "safety" -tilnærming, men lar mange spørsmål stå åpne
 - Hvordan operasjonalisere pasientsikkerhet vs personvern
 - Hvor er (var) Helsetilsynet ?
- Er lite kunnskap(ing)s-orientert : stopper ved "opplysninger" (informasjon)
 - Kan tolkes som tilslutning til "objektivistisk" kunnskapssyn
 - Preger selve definisjonen av personvernet (juridisk)
 - Preger premisene for beskyttelse av informasjon : informasjonssikkerheten forblir reaktiv
 - Stenger for innsikt ! (bokstavlig og overført !)
- Ignorerer viktige aspekter ved kunnskaps-produksjon og samhandling
 - Har ikke kontakt med viktige deler av den sosiale virkeligheten i helsevesenet
 - Kanal for "FBC-frustrasjoner" (en av få!)
 - Men har ikke noe annet svar enn
 - å drive "oppholdende strid" ???
 - Helsepersonellets personvern i en tid med "empowered self-control" ?
- Vil en vending mot resiliens være interessant for Datatilsynet ?
 - Formodentlig ikke noe problem på "Infrastruktur" ...verre på kunnskap
 - Aksepterer medisinsk/juridisk legitimering av "hypervirkelig" journal ?
 - Vil utfordre skillet mellom "nød-" og "normal-situasjon"

Takk for oppmerksomheten