*ESRA SEMINAR, OSLO, 2018-09-16*

# SAMFUNNETS DIGITALE SÅRBARHET OG BÆREKRAFT - ER DET FARTEN ELLER BRÅSTOPPENE SOM ER FARLIG?

**Tor Olav Grøtan, PhD,**

**Seniorforsker, SINTEF Digital**

***tor.o.grotan@sintef.no***

Last update: 2018-09-25

Kilde: Dr. Hans-Peter Güllich, www.dydon.net, at https://paranoia.watchcom.no/paranoia18-presentations

# The Cyber Playground


**Cyber Risk Crisis**

**Shopping Center for Hackers**

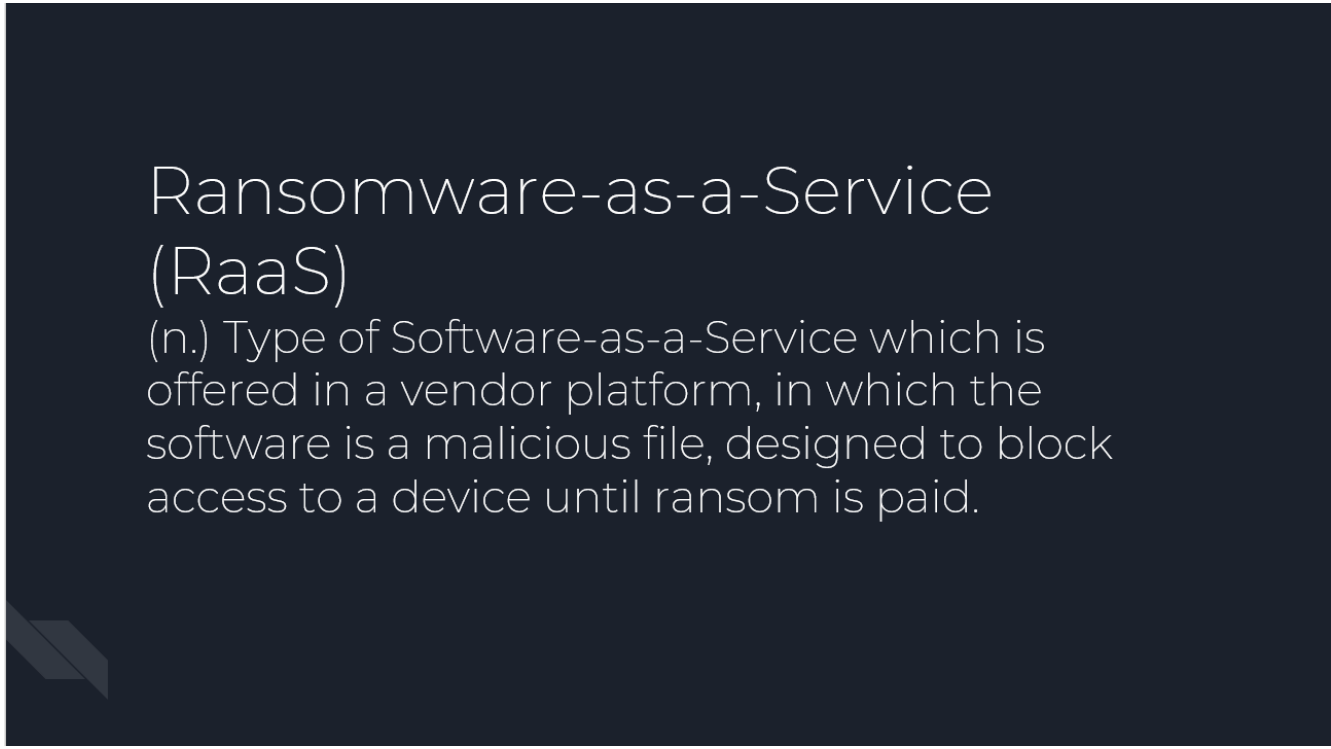
For ansvarlige borgere, seriøst næringsliv og samfunnets kritiske infrastrukturer?



SINTEF

Source: Yara Bayoumi, at
https://paranoia.watchcom.no/paranoia18-presentations

# Beyond Saas, Paas, Saas …




SINTEF

# Den rasistiske chatboten

MICROSOFT \ WEB \ TL;DR

## Twitter taught Microsoft's AI chatbot to be a racist asshole in less than a day

68

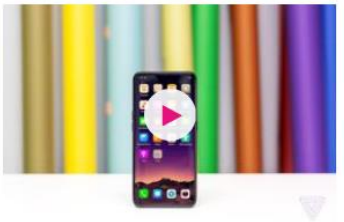
By James Vincent | @jjvincent | Mar 24, 2016, 6:43am EDT

SHARE


It took less than 24 hours for Twitter to corrupt an innocent AI chatbot. Yesterday, Microsoft unveiled Tay — a Twitter bot that the company described as an experiment in "conversational understanding." The more you chat with Tay, said Microsoft, the smarter it gets, learning to engage people through "casual and playful conversation."

Unfortunately, the conversations didn't stay playful for long. Pretty soon after Tay launched, people starting tweeting the bot with all sorts of misogynistic, racist, and Donald Trumpist remarks. And Tay — being essentially a robot parrot with an internet connection — started repeating these sentiments back to users, proving correct that old programming adage: flaming garbage pile in, flaming garbage pile out.


MOST READ



Oppo's Find X ditches the notch for pop-up cameras

Elon Musk emailed all of Tesla about attempted 'sabotage' by an employee

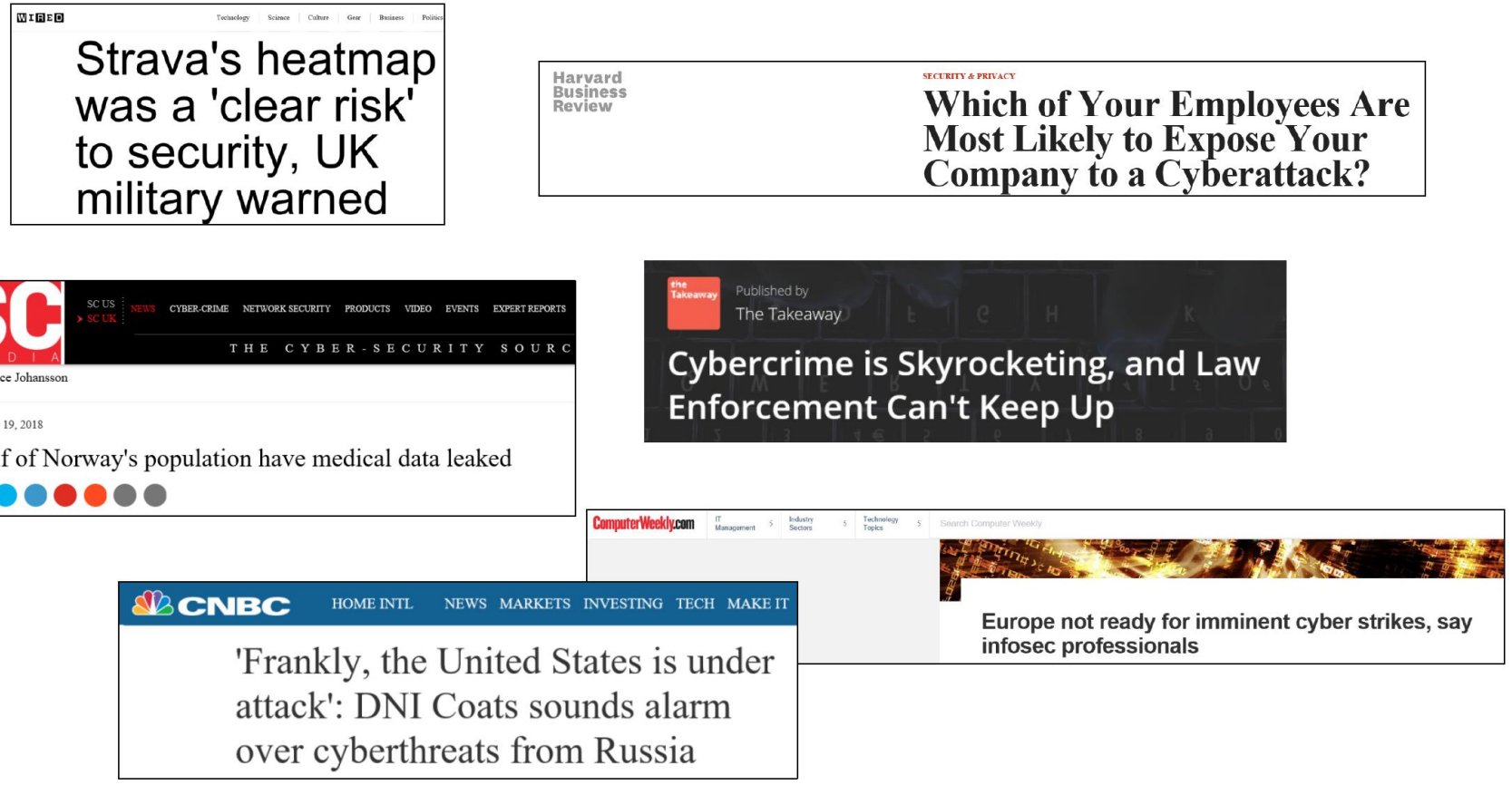
Android Messages will let you send texts from your computer starting today




SINTEF

Source: Paul Chaffey, KMD, at
https://paranoia.watchcom.no/paranoia18-presentations

# KMD:
# Uredd pådriver for digitalisering








SINTEF

# Allerede okkupert?


Saabs konsernsjef Håkan Buskhe er bekymret. Foto: Fredrik Sandberg/TT/NTB Scanpix

**Nyheter** Utenriks

## Saabs toppsjef: Sverige er okkupert av fremmed makt

Dagens Næringsliv

Publisert: 31.05.2018 – 08:21 Oppdatert: 31.05.2018 – 09:44



SINTEF

# Tar vi faresignalene på alvor?


Cyber-hendelser som "fun-facts" eller "horror-underholdning" ?

Adresseavisen

8.2.2018

## Redd noen skal «slå av Norge» fra utlandet

*Professor Olav Lysne roper varsko om hvor sårbar Norge og sentral norsk infrastruktur er.*

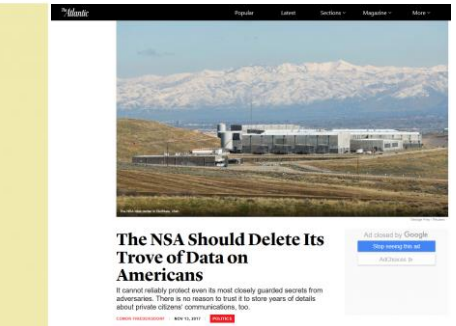

Advarer mot svakheter. Professor Olav Lysne sier det er fullt mulig å lamme hele Norge i en hybridkrig. Kunnskapsmangel, for svak sikkerhet og kritisk infrastruktur som alle er avhengig av, er de største problemene. FOTO: FRANK CADAMARTERI

SINTEF

# Are we prepared? or plainly

- C++ programming prevails
- Notorious Web (in)security: do we care?
- …….





Hva skjedde med demokratisk kapitalisme?

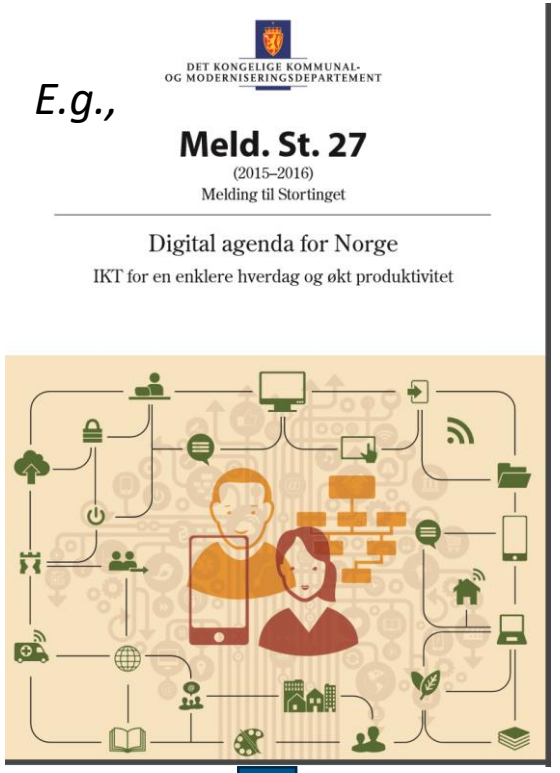
SINTEF

# Samfunnets digitale sårbarhet vs digitale ambisjoner


Eksponering


Muliggjøring

*E.g.,*





Tradisjonelle premisser om kontroll og ansvar utfordres.
Risiko på vandring.
Utydelige og komplekse eierskap.

? ? ?

M T O

**(E.g.) ISO2700,**
**Internkontroll**

"God informasjonssikkerhet"
"Godt personvern"
"Risikobasert"
(= mer enn formalismer?)

SINTEF

# Cyber/IKT sikkerhet: "Sette CIA-halen på grisen"?

## På norsk: konfidensialitet, integritet, tilgjengelighet

Norsk krypto sikret hotline mellom
Det hvite hus og Kreml

**Kryptografi har alltid vært et av hovedarbeidsfeltene til NSM (og tidligere FO/S). Et utslag av satsningen på kryptografi har vært at norsk industri i flere tiår har vært en ledende leverandør av kryptografisk utstyr til NATO. Under den kalde krigen sikret et norsk kryptoapparat en egen hotline mellom Washington og Kreml.**

En forklaring på denne suksessen har vært et tett og målrettet samarbeid mellom industrien, sikkerhetsmyndighetene og Forsvaret.

Gjennombruddet for industrien kom på 50-tallet. Bedriften Standard Telefon og Kabelfabrikk (STK) startet i 1955 utviklingen av en kryptomaskin, som kom til å revolusjonere koding av sikkerhetsgradert informasjon. Maskinen ble kalt Electronic Teleprint Cryptografic Regenerative Repeater Machine (ETCRRM), og var andre systemer overlegen når det gjaldt både kapasitet og sikkerhet.

**Norsk idémaker**

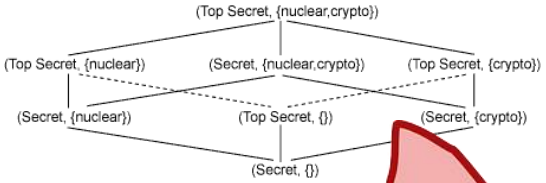
Sjefen for Hærens Samband, oberst, sivilingeniør og krigsveteran Bjørn Rørholdt var idémakeren bak ETCRRM. Et samarbeid mellom Rørholdt og Kåre Meisingset ved STK resulterte i at det i 1952 ble tatt ut patent på den nye kryptografimaskinen.

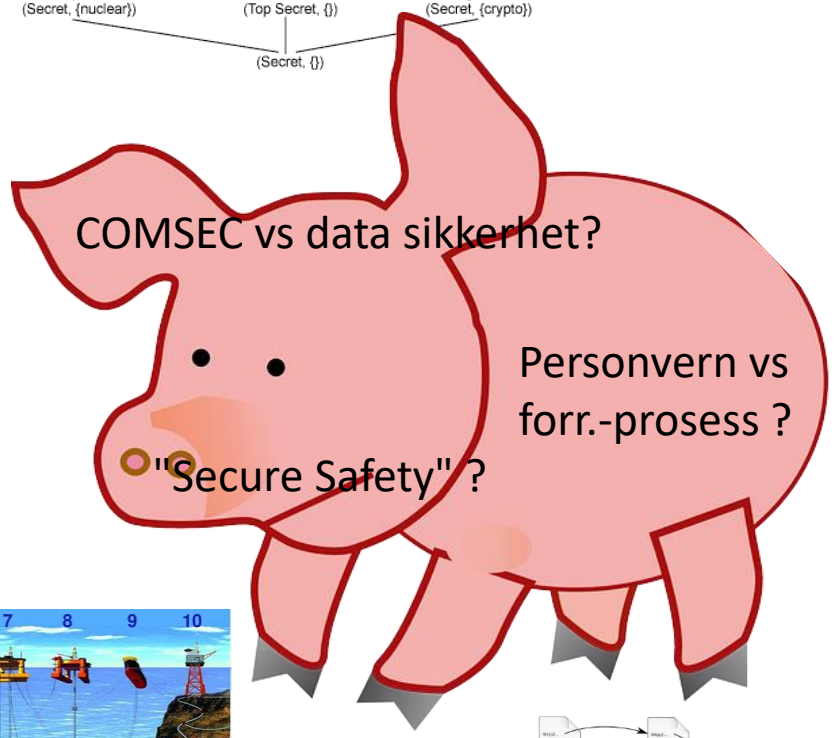
NATO-landene ble raskt begeistret for den norsk nyvinningen. I løpet av få år oppnådde ETCRRM å bli standard kryptografimaskin i NATO.

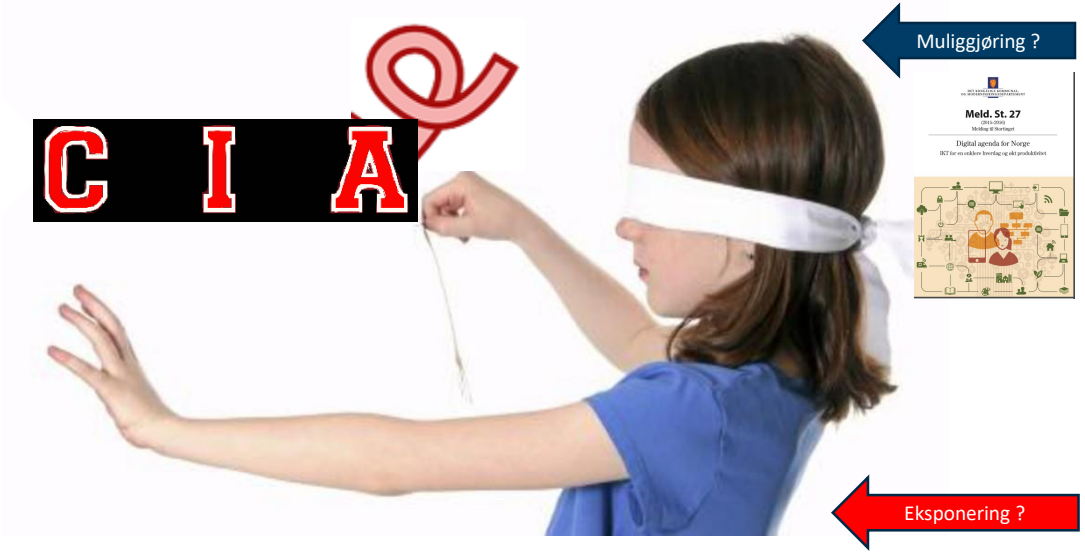
ETCRRM kom også til å spille en rolle i rivaliseringen mellom øst og vest under den kalde krigen. I kjølvannet av Cuba-krisen ble ETCRRM brukt for å etablere en sikker telekslinje mellom Kreml og Det hvite hus.

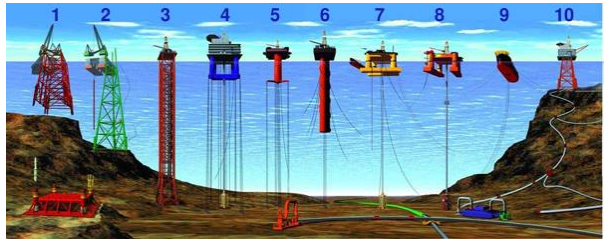
*Foto: Kryptomaskinen ETCRRM*

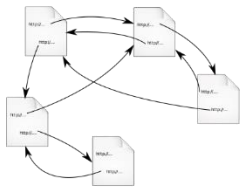




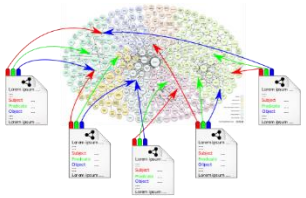



The traditional web -
*A web of documents*



The semantic web -
*A web of human and machine readable content employing linked data*



SINTEF

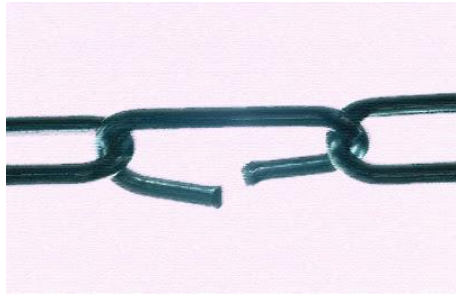
# Forstår vi dagens situasjon godt nok?
(fra gårsdagens bilder?)

- …➔ (5G, NaaS, IaaS, PaaS)
- Kritisk infrastruktur?
- Digital økonomi?
- Digital makt?
- Digital nasjon?
- …
- Fantasien trenger støtte!
- Ulike (for-)forståelser er verken ulempe eller garanti


*Gareth Morgan*

# SAMRISK prosjekt: New Strains of Society

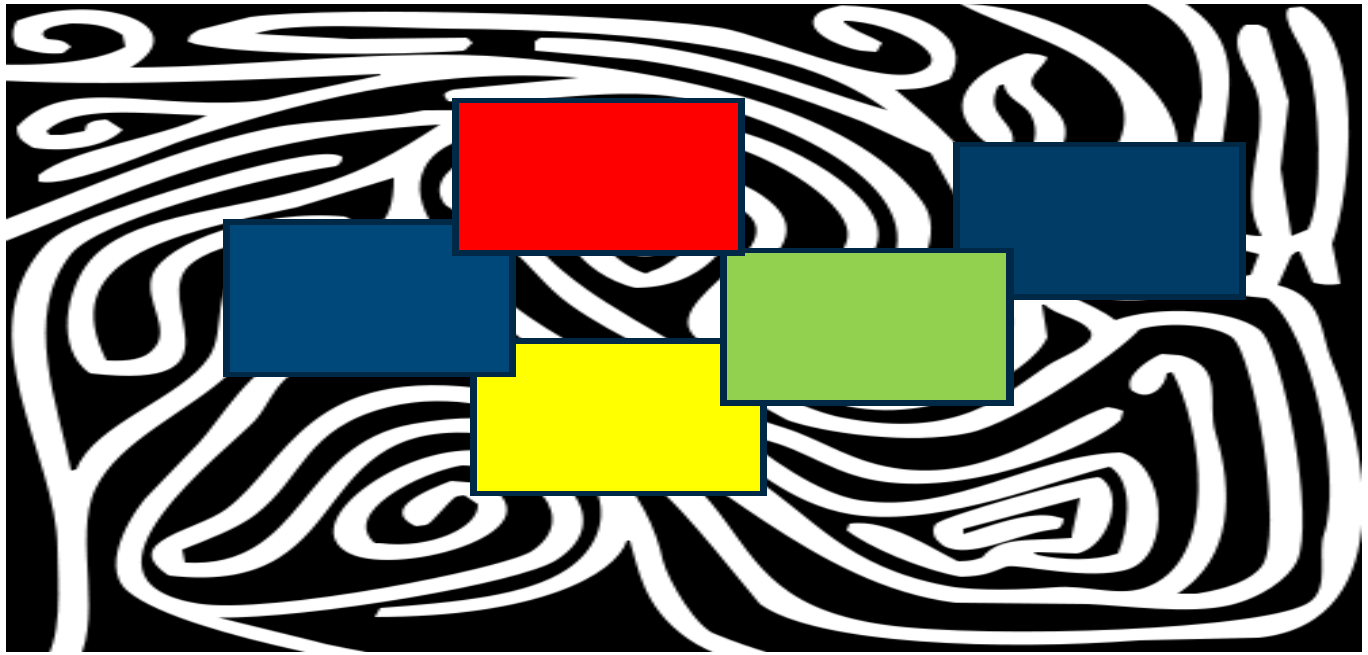
## "Oppdrag: sette på spissen"



- *Verden blir stadig mindre. Teknologi og infrastruktur blir stadig mer sammenflettet, nasjoner knyttes tettere sammen gjennom transport, kommunikasjon og økonomi. Men denne utviklingen fører også med seg nye belastninger for samfunnet. Avhengigheten av datasystemer gjør oss sårbare, og det oppstår nye former for kriminalitet. Hvordan kan vi møte slike utfordringer?*
- *Tradisjonene for sikkerhetsstyring og risikovurdering hviler på forestillinger om kontroll og ansvar. Det vil si, risiko må oversettes til kontrollerbare størrelser, og noen må eie problemet. Hva om truslene er grenseløse? Hva om ingen eier dem?*
- *Vår oppmerksomhet rettes mot det vi kaller skjulte, dynamiske og emergente (oppkommende) sårbarheter. Det er sårbarheter som kan være ukjente i enhver betydning: ignorert, glemt, aldri tenkt på, umulig å identifisere, feiloppfattet eller underestimert. Vårt mål er å utvikle et analytisk rammeverk for å forstå, identifisere og håndtere denne typen nye samfunnsmessige belastninger.*
- *For å anerkjenne nye utfordringer må vi godta at nåværende risikotilnærminger kan komme til kort. Nye belastninger krever ny tenkning og nye tilnærminger til risiko og sårbarhet. Oppmerksomheten vendes dermed mot komplekse landskap av risiko, som involverer flere systemer som kan generere, overføre og omplassere risiko. Vi kaller disse større bildene for "trussellandskap" - landskap som involverer flere systemer i samspill. Vi åpner dermed for at flere scenarier griper inn i hverandre – med muligheter for overføring og eskalering.*
- *New Strains of Society går inn for å stress-teste (belastningsteste) samfunnets evne til å møte nye trusler og sårbarheter. Vi retter også stress-testen mot oss selv ved å spørre krevende spørsmål: Hvordan evner eksisterende risikotilnærminger å forklare samfunnets nye belastninger? Kan eksisterende metodikk noen gang kunne imøtekomme de nye utfordringene? Hvor ligger metodenes begrensninger?*

# New Strains of society;

## *hidden, dynamic and emergent (h/d/e) threats and vulnerabilities* *(SAMRISK-II, 2014-17)*



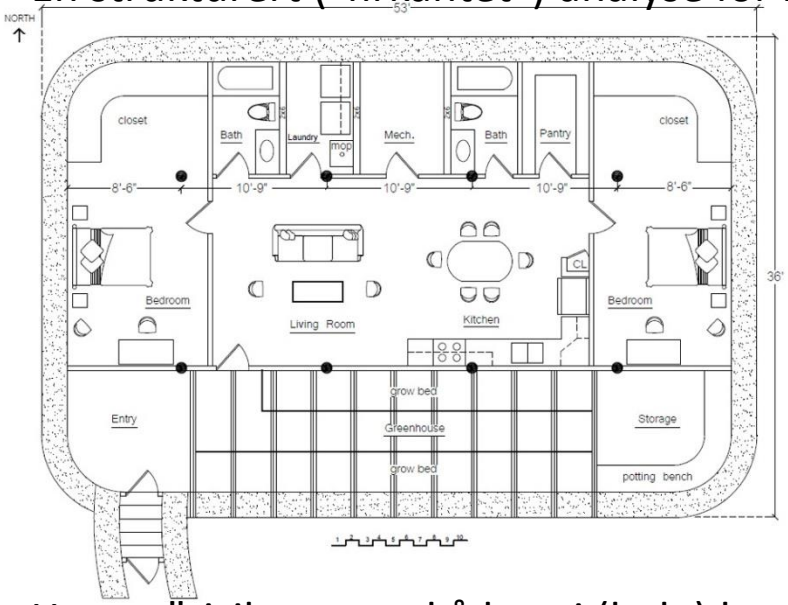
- Tradisjonelle forutsetninger om kontroll og ansvar utfordres med IKT
- Avgrensede/definerte trusselbilder vanskelig å opprettholde. Uklare/komplekse "eierskap" til risiko
- **Trussel-landskap** forstått som overlappende trusselbilder
- Ukjent/dynamisk bakgrunnslandskap ("labyrintisk")

SINTEF

# Bygge *trussel-landskap*; utfordre etablerte rammer for kunnskap og erfaring

- Hvert "rom" representerer en pragmatisk risiko-horisont og forståelsesramme
  - Innside vs utside, e.g.,
    - industriell sikkerhet, HMS, energi, personvern, helsetjeneste, transport, kommune, blålys/SAR,,,,,
  - Treghet, motsetter seg utvidelse
- Hva blir  det "større bildet" av kombinerte trusler og gjensidige ("h/d/e") sårbarheter ?

**Analogi: "Sikkerhet rom-for-rom"**
En "avgrensning" for hver trussel/område
En strukturert ("firkantet") analyse for hver



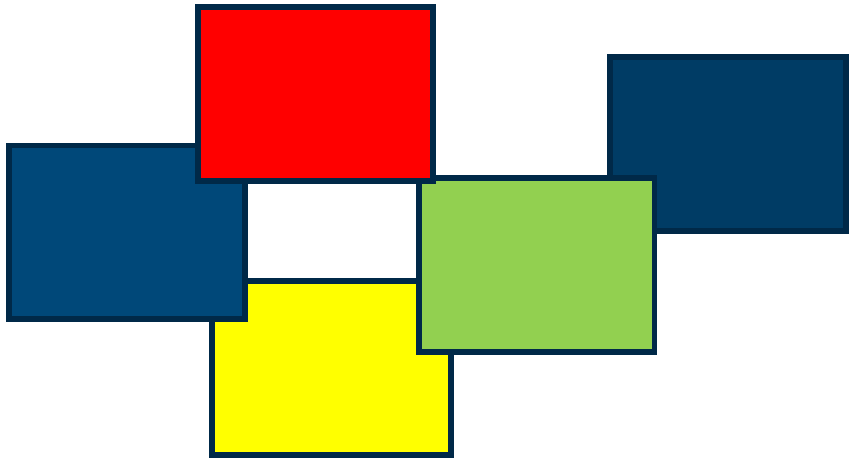

Hva er "risikoen med å leve i (hele) huset" ?
Hva er virkningen av ny teknologi?

SINTEF

# "Microscopic" (MTO) cyber-threat landscape: Industrial Control Systems (ICS/"SCADA")

Inspired by: enisa European Union Agency for Network and Information Security

- Aging and mix of old and new hardware/software
- User competence and awareness
- Internet of Things
- Complex web of actors (complex value chains)
- Intentional acts (sabotage and criminal intent)

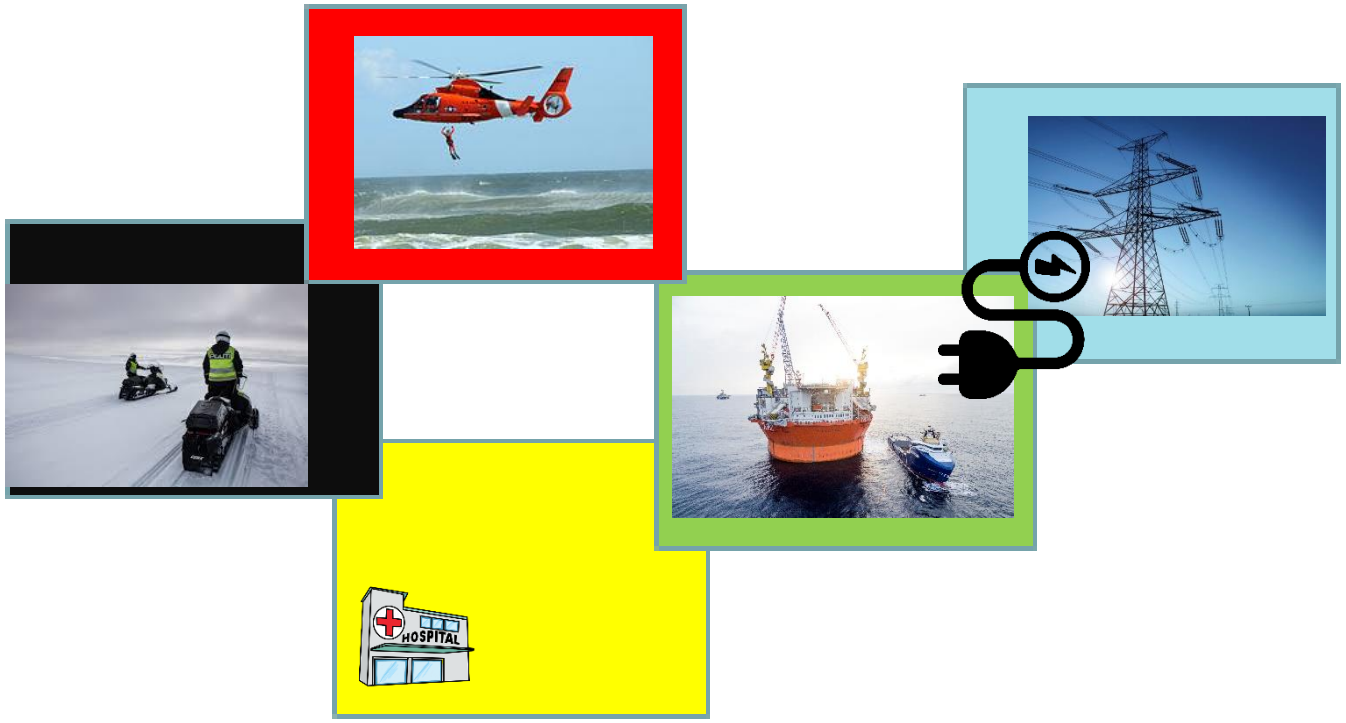


*WORKSHOP June '16 ("Cyber Safety, Security and Resilience of Critical Energy Infrastructures"): deeper overlaps than expected!*



SINTEF

# Cyber-threat landscapes in New Strains: examples



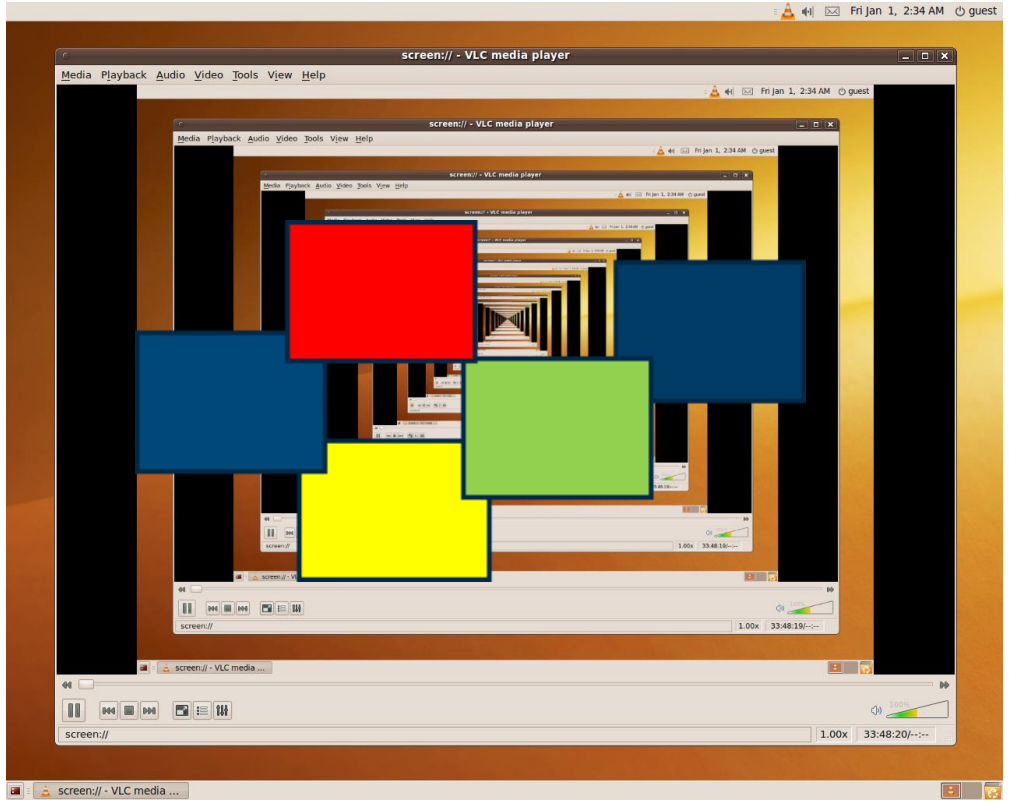

**Oil in High North (OiHN)**

**Cyber Safety, Security and Resilience of Energy Infrastructures (electricity, oil&gas)**

**SCADA**

SINTEF

# Trussel-landskap og skalering

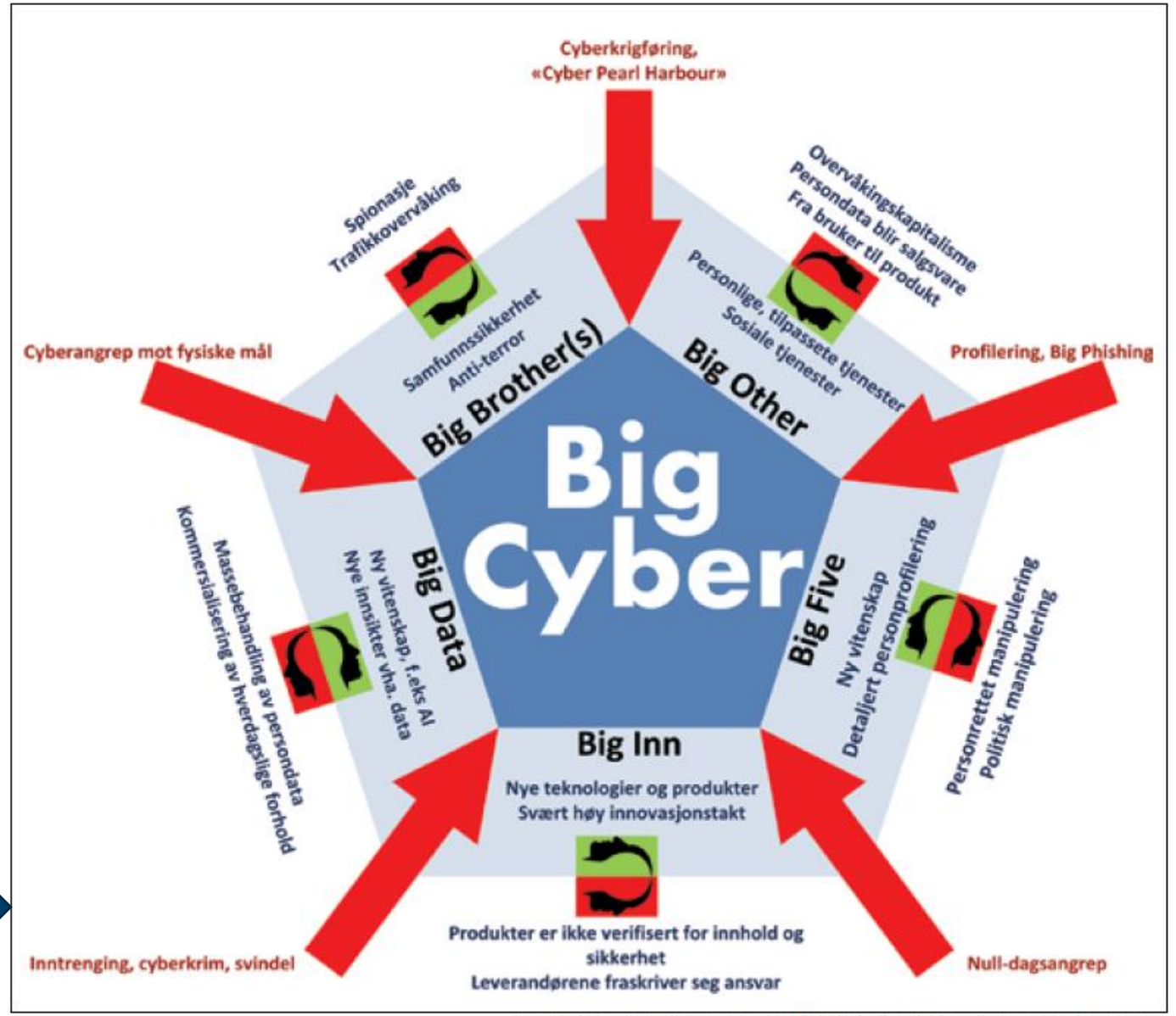



| SCADA | SCADA in energy infrastructure | Smart metering (AMS) | Oil in High North (OiHN) | "What-if" ??? |
|---|---|---|---|---|
| As a composite technology | Awareness of (high) vulnerability for "critical" infrastructures | A re-engineering of the energy system<br>Disruptive business models<br>New, unanticipated vulnerabilities involving end-users<br>Hard to separate inside/outside of CI | Cyber vulnerabilities everywhere<br>Saturation potentials<br>Hard to separate the Unclassified from the Classified |  <br>  |



SINTEF


*Sensiteringsmodell* for "h/d/e"
trusler, sårbarheter, koplinger




ILLUSTRASJON: STIG ØYVANN, ETTER PRESENTASJON AV TOR OLAV GRØTAN, SINTEF

**FORLOKKENDE OG FORRÆDERSK:** Moderne teknologi fremstår med et «Janus-ansikt», med både attraktive og uønskete sider og egenskaper. Det åpner for nye risikoer og sårbarheter, med tilhørende angrepsvektorer.

Nr. 23 • uke 37 - 2017 COMPUTERWORLD 7

SINTEF


Cyber Pearl Harbor
Cyber conflict

*surveillance capitalism*
*commodification of personal data/behavior*
*from client to product*

*Espionage, surveillance everywhere (e.g. traffic, crowds, individuals)*

*Societal security, anti--terror*

*Personalization, Customization Social Media*

Cyber-physical impact

Profiling, BigPhishing

Big Brother(s)

Big Other

Big Cyber

Big Data

Big Five

BigInn

*Robotic dialogue?*

*AI/DL, New insights, patterns, Predictions, capacities*

*Massive computations based on "trivia", "Internet of Things", "Internet of Everything"; nothing escapes attention and scrutiny*

*("New") Science of Profiling and purposed targeting*

*Individual/groupwise targeting and (commercial/political) communication*

*Intelligent defense*

*Intelligent offense*

*High(er) rate of innovations*

*Vulnerable designs (ForeverDays)*

*Vulnerable OE*

*lack of assurances*
*lack of liability*

Intrusion, cyber crime/fraud

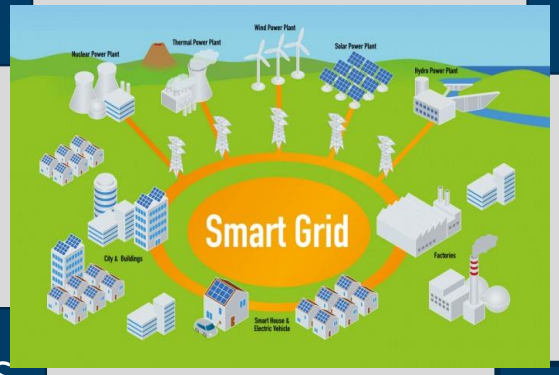
Zero Days

SINTEF

(SMART) ENERGY SYSTEM IN TRANSFORMATION, INCREASINGLY DEPENDENT ON SCADA/ICS

SCADA/ICS

SCADA/ICS

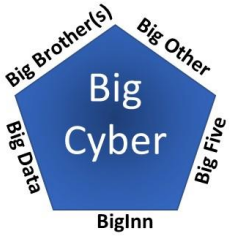



SCADA/ICS

SCADA/ICS

**SMART METER**

Home Area Network (HAN) port

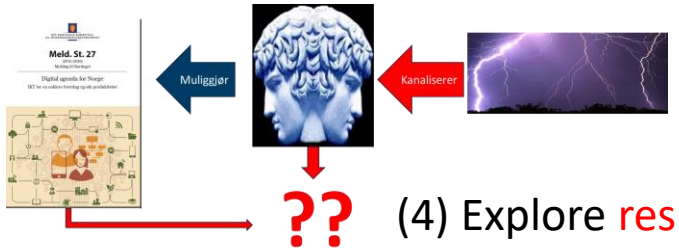





"Smart Metering Paranoia":
*T.O. Grøtan (ESREL 2018,)*
*Building cyber resilience through a discursive approach to "Big Cyber" threat landscapes*

SINTEF

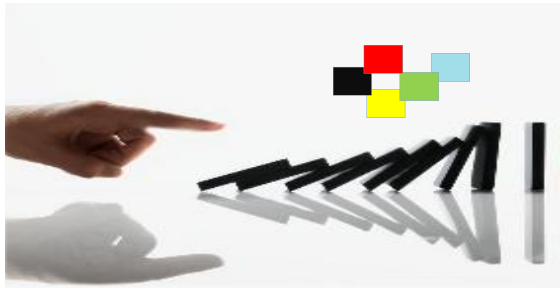
# *Fra "kontroll" til "tåleevne"*



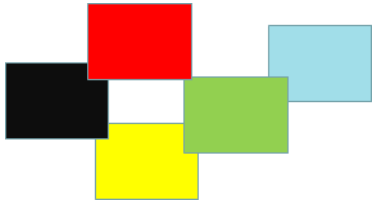

(4) Explore responsive capacities

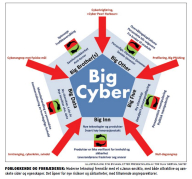


(3) Stress-test



(2) Threat Landscape (TL) generation/saturation






(1) Threat Pictures (TP) elaboration

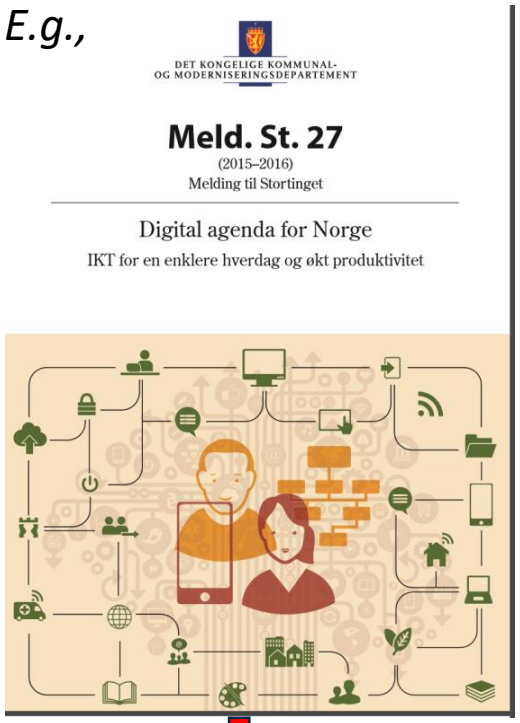
**(MTO)**

SINTEF

# Veien til

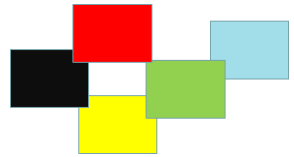

?

*E.g.,*

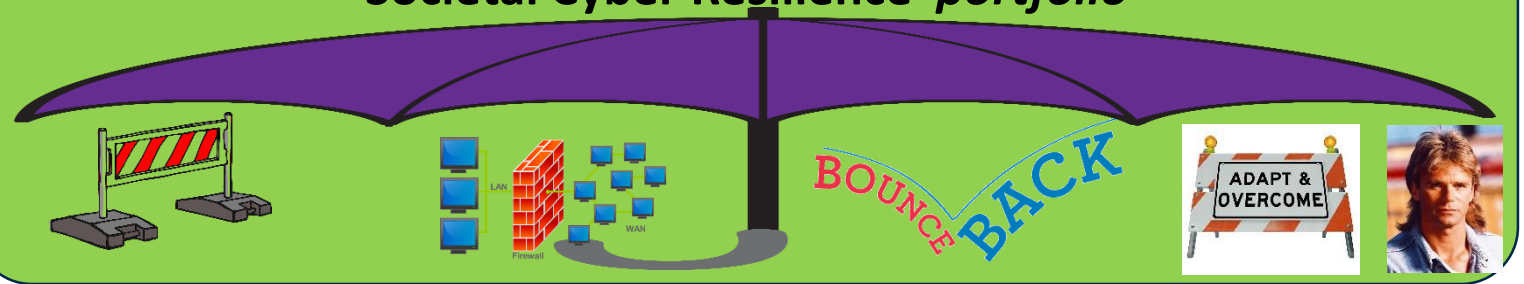



Muliggjøring


Eksponering

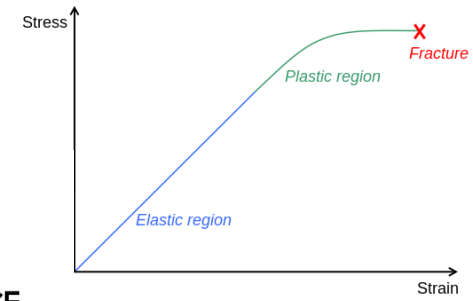



**Societal Cyber Resilience *portfolio***

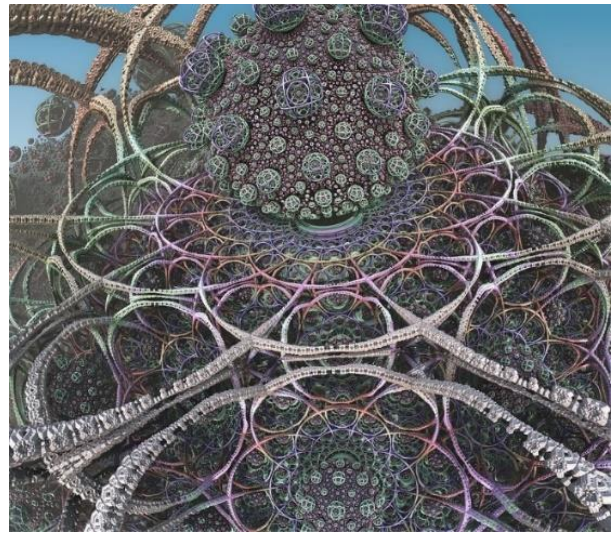


# "Forelska i  "?


E.g.,
Resilient forest >> Σ Resilient trees ?



- "Resiliens-**landskap**" av (forstående/handlende) **subjekter** med ulike forutsetninger og agendaer

- Hvem står i fare for å "ofres"? Pensjonisten i nettbanken? Strømkunden som åpner AMS/HAN-porten for ambisiøs tredjepart?
- Bidrar "resilience" rett og slett til en "forakt for svakhet"? (A.J. Vetlesen)

SINTEF

Big Brother(s) ?? Big Five Big Other(s) ?? Big Inn(ovation) Big Data

# Big Cyber trusler

Cyber-physical impact

"Cyber Pearl Harbour"

Operational vulnerabilities

Mass profiling (Big Phishing)

Zero Days

Forever Days

Crime/fraud

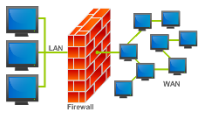
Orchestrated ? attacks

# "Societal Cyber Resilience" ?

M T O

Key Theme 1 | Key Theme 2 | Key Theme N-1 | Key Theme N

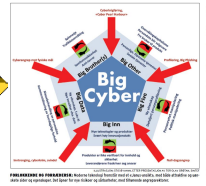
Tools & methods




stress Test

Threat landscape




Joint vulnerabilities

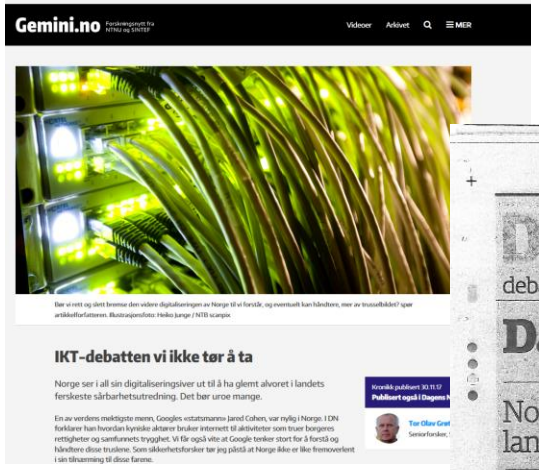

Potential for collaboration

Resilience-landscape ("poly-centric"?)

SINTEF

# Kronikk, DN, 28.11.17

- Digitaliseringsiver som "glemmer" sårbarhet
- Google eller Norge i (vårt) førersete?
- Tradisjonelle sikkehetstilnærminger ikke tilstrekkelige (premisser for ansvar, kontroll)
- (Alvorlig) etterslep på digital sikkerhetskompetanse
- I stedet for å presse marginer, bør vi "bremse" til vi forstår/kan mer?
- Uoversiktlig sårbarhet: fem Janus-ansikter ("Big Cyber" modellen)
- Nye angrepsflater, ukjente intensjoner og motiver
  - E.g., smarte energinett vs forsyningssikkerhet?
- Vi må øke vår digitale motstandskraft ("cyber resilience")


Gemini.no

IKT-debatten vi ikke tør å ta

Norge ser i all sin digitaliseringsiver ut til å ha glemt alvoret i landets ferskeste sårbarhetsutredning. Det bør uroe mange.


Tirsdag 28. november 2017 | Dagens Næringsliv

Debatt

debatt@dn.no

Datasikkerhet i dødvinkelen

Norge ser i all digitaliseringsiveren ut til å ha glemt alvoret i landets ferskeste sårbarhetsutredning. Det bør uroe mange.

Bør vi rett og slett bremse den videre digitaliseringen av Norge til vi forstår, og eventuelt kan håndtere, mer av trusselbildet

Innlegg Tor Olav Grotan

Sikkert nok for cyberspace?

Tor Olav Grotan, seniorforsker ved Sintef

# Replikk (DN 4.12) & (kort) tilsvar

ringene til å fatte beslutninger om for eksempel lønn og bonus, forfremmelser og trenings- og utviklingstiltak. Mange organisasjoner har også benyttet normalfordelte vurderinger, slik

dette ble kalt prestasjonsledelse 2.0 og hadde som mål å få til mer samarbeid og teamarbeid, mer utvikling og vekst gjennom å være «tettere på» sine medarbeidere og hvor tilbakemeldingene

brukte cirka 2 millioner timer årlig på sine evalueringer av noe over 65,000 medarbeidere. Nå anbefaler til og med konsulentskapene som tidligere anbefalte systemer slik Microsoft hadde å

## Ikke tid for digitalbrems

Tor Olav Grøtan stiller i DN 28. november spørsmål om vi skal sette digitaliseringen på pause. Digitalisering bringer med seg utfordringer innen personvern og datasikkerhet, men løsningen er ikke å sette digitaliseringen på vent.

Digitaliseringen drives ikke først og fremst av politikere, men av forbrukere, gründere og fagfolk som finner nye og bedre løsninger. Digitaliseringen gir oss uante muligheter. Det må også det offentlige utnytte for å tilby folk mer effektive tjenester og en enklere arbeidshverdag. Når vi digitaliserer tjenester frigjør vi ressurser som vi heller kan bruke på å gi gode tjenester til folk.

Grøtan har rett i at digitalisering medfører en del utfordringer knyttet til. Å ivareta personvern og datasikkerhet er en av flere forutsetninger for at folk skal bruke digitale tjenester. Personvernutfordringene er internasjonale og kan ikke løses av norske myndigheter alene. Offentlige ikt-systemer skal ivareta personvernet slik at vi i størst mulig grad råder over egne opplysninger - hvordan de kan rettes, slettes og glemmes. Det er viktig å bli med på EUs innsats for å innføre merkeordninger for godt personvern. Godt person- og forbrukervern vil i stadig større grad også bli et konkurransefortrinn.

Det er ikke tid for å sette på bremsen nå.

**Mari Holm Lønseth (H)**, stortingsrepresentant

## Maktens språkrasling

«Allerede på jusstudiet starter innlæringen av til dels tungt juridisk språk. Vi påvirkes av stammefrendene våre», skriver Torstein Frantzen i DN lørdag 18. november.

Juridisk fakultet i Oslo har startet et klarspråk-prosjekt.

Fra nyttår vil vi også utvide faget «rettslig metode» med en ny del som heter «rettslig argumentasjon». Vi har innledet et samarbeid med fagmiljøet ved Institutt for

## Politikerne må ta cyberansvar

Mari Holm Lønseth kommenterer 4. desember mitt DN-innlegg, der jeg spør om vi bør bremse digitaliseringen av Norge til vi forstår, og eventuelt kan håndtere, mer av sikkerhetstrusselen i cyberspace. Jeg er glad for responsen, men blir ikke særlig beroliget.

Lønseth ser det kommende europeiske personopplysningsregelverket (GDPR) som en bærebjelke for personvern. Men GDPR handler like mye om å legge til rette for en digital økonomi basert på persondata og gir ikke all verdens motstandskraft mot truslene som venter.

Politikere må gjerne promotere det positive som digitalisering åpner for. Men denne teknologien har et janusansikt som kan snu seg fort. Er politikerne også klar til å ta ansvar for et "Cyber Pearl Harbor" mot kritisk infrastruktur som USA frykter?

Politikerne kan ikke være Tante Sofie når det gjelder vanlig nettbruk. Men når befolkningens helseopplysninger sendes ut i verden, og kritisk infrastruktur utsettes for fare, må vi likevel kunne forvente mer av politiske aktører enn at de bare forutsetter at sikkerhetshull er tettet.

Lønseth setter sin lit til fagfolkene. Men da må disse pleies bedre enn det som kommer fram i DN 2. desember om mangelen på kryptokompetanse i Norge.

Mange sektorer må forberede seg på "eventualiteter" utover det en vanlig risiko- og sårbarhetsanalyse kan overskue. Ikke minst må vi som nasjon utvikle prinsipper for digital motstandskraft som også omfatter befolkningen – før vi innfører autonome transportsystemer eller bygger smarte byer.

**Tor Olav Grøtan,** seniorforsker, Sintef

# Hva er farligst ?

- NSM: Senke farten?
  - Paranoia '18 (Roar Thon)
  - Kronikk Finansavisen '18 (Bente Hoff)


DEBATT

Send innlegg til debatt@finansavisen.no

Bedrifter mister ofte oversikten over IKT-systemene i digitaliseringsprosessen. Svakt sikrede punkter kan utnyttes av de som ønsker det, skriver Bente Hoff i Nasjonal sikkerhetsmyndighet.

## Digitalisering over fartsgrensen

**De aller fleste** virksomheter vil i 2018 svare bekreftende på at digitalisering er et viktig satsingsområde. Digitalisering skaper nye måter å levere tjenester på, og er en viktig drivkraft for forenkling og forbedring av privat så vel som offentlig sektor.

Nasjonal sikkerhetsmyndighet (NSM) ser samtidig at trusselbildet i det digitale rom er forverret de siste årene. Trusselaktørene blir stadig flere og dyktigere, og verktøy og metoder som tidligere var forbeholdt nasjonale aktører er nå allemannseie. Samtidig blir IKT-systemene vanskeligere å beskytte. En av årsakene er at innføring av nye tjenester medfører økt kompleksitet. I løpet av det siste året har NSM koordinert håndtering av større og mer alvorlige digitale hendelser enn før. I lys av dette fremstår norske virksomheter som lite motstandsdyktige.

**Det er derfor naturlig** å stille spørsmålet om digitaliseringen må bremses. Har vi en hastighet som gjør at risikoen for den enkelte virksomhet og for samfunnet ikke ligger på et forsvarlig nivå? Dette er et komplekst spørsmål som det ikke kan være et entydig svar på. I mange tilfeller kan digitaliseringen gå raskere enn i dag med fullt akseptabel risiko. Det avhenger av om man har kontroll på hva man gjør, og at beslutninger tas på et tilstrekkelig informasjonsgrunnlag. Med bakgrunn i NSMs kunnskap om risiko og kjente sårbarheter i det digitale rom ser vi dessverre ofte at virksomhetene ikke har tilstrekkelig kontroll. Noen av årsakene til dette er mangel på sikkerhetskompetanse, utdaterte og komplekse IKT-systemer og manglende oversikt over avhengigheter.

**Digitalisering er en måte** å effektivisere, automatisere og forbedre det man gjør, og de valgene ledelsen tar er kjernen i sikkerhetsarbeidet.

Alt for ofte møter NSM overraskelse fra ledelsen etter et større datainnbrudd «Ups, jeg var ikke klar over at dette var tilstanden hos oss» eller «Ups, jeg var ikke klar over at dette var en risiko». Sikkerhetskompetanse er en viktig forutsetning for å digitalisere. Den samme kompetansen er en mangelvare i samfunnet, i mange virksomheter og ikke minst på ledernivå.

Ny funksjonalitet legges gjerne til på eksisterende IKT-systemer og muliggjøres gjennom sammenkoblinger av flere systemer. En tommelfingerregel er at nye og oppdaterte IKT-systemer gir best sikkerhet. En annen er at økt kompleksitet gir økt risiko. Digitaliseringen medfører derfor økt risiko og nye sårbarheter.

**Ofte mister virksomhetene** oversikten over IKT-systemene i digitaliseringsprosessen, og svakt sikrede punkter kan utnyttes av de som ønsker det. Det er ikke mulig å ha kontroll på hvem som har tilgang til hva med mindre man har kontroll på hvor data er lagret og på alle sammenkoblinger. En konsekvens er at før man beslutter å tjenesteutsette drift av enhver IKT-løsning må man ha kontroll på virksomhetsarkitekturen og tilgangsstyringen i IKT-systemene.

Det mest krevende er kanskje å ha oversikt over avhengigheter utenfor egen organisasjon. Med økende kompleksitet i sammenkoblede digitale verdikjeder er det utfordrende for virksomhet og leverandør å se konsekvenser av de beslutninger de gjør. Til en viss grad kan nasjonal regulering adressere dette, men det er også kritisk at den enkelte virksomhet prioriterer kartlegging av avhengigheter som en del av digitaliseringsarbeidet.

**Endring og videreutvikling av** organisasjoner og IKT-systemer vil alltid medføre risiko. Noe risiko må aksepteres for å få de nedvendige gevinstene, men hastigheten må tilpasses forholdene. NSM erfarer for ofte at farten medfører høyere risiko enn virksomheten selv er klar over, og vi ser alvorlige eksempler på manglende kontroll. Digitaliseringen krever både gass og bremser på riktig sted. Basert på det vi ser i NSM bør bremsepedalen brukes oftere enn i dag.



Bente Hoff.

**BENTE HOFF,**
Leder for strategisk IKT-sikkerhet hos Nasjonal sikkerhetsmyndighet

- Eller, tar vi en "Stutum",
  - "det er bråstoppene som er farlige"
- ?



SINTEF

SINTEF

Teknologi for et bedre samfunn