

Dilemmaer, erfaringer, læring og inspirasjon fra andre sektorer

Normenkonferansen 2026

Et sårbart samfunn NOU 2000:24

- Åpnere verdenssamfunn
- Deregulering fører til mindre strenge krav
- Komplekse teknologiske systemer
- Effektiviseringspress
- Bemanningsreduksjon
- Privatisering og tjenesteutsetting



NOU 2015:13 Digital sårbarhet – sikkert samfunn

- Digitaliseringen er i stor grad fremmedgjort og ingen har lenger oversikt over sårbarhetsbildet slik vi en gang hadde (avs. 6.1)
- IKT-kriminaliteten er i ferd med å bli et reelt samfunnsproblem der oppdagelsesrisikoen er lav og fortjenestepotensialet høyt
- Snowden-lekkasjene



....teknologibrukere i det brede laget av folket

«Medisinskteknisk utstyr er i en rivende utvikling. Utstyr er også på vei inn i private hjem og påliteligheten til utstyret kan være variabel. Hjemmet vil i større grad være behandlingstedet fremover, men er også sårbart. Infrastrukturen her er privat – kanskje delt, kanskje er andre private og offentlige aktører i bildet: helsetjenester, vaktselskap, strømleverandør m.fl.»

(Omerovic A og 2015-rapport Gjære E A, Digitale sårbarheter i helsesektoren – en oppsummering av funn fra workshop holdt i mai 2025 i regi av Lysneutvalget)



Smarthuset deres ble hacket: - Dummere hus får man ikke

De bygget smarthus for et enklere liv. Så sluttet huset å fungere. Ta disse syv forholdsreglene om du har smartutstyr.

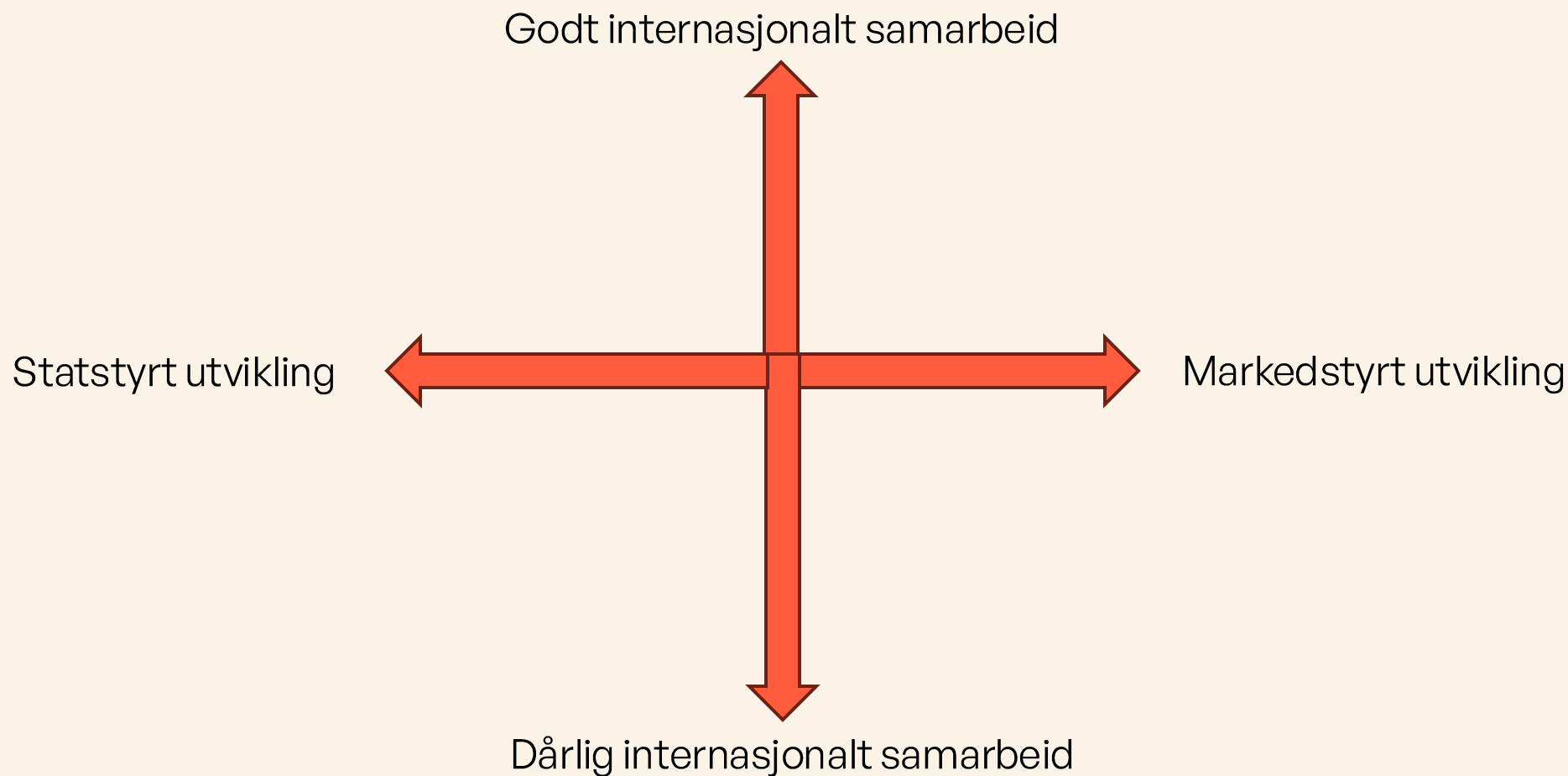


Tanken var å lage et smarthus med velferdsteknologi. Det har fungert bra siden 2013, men i november begynte det å skje ting i huset. Foto: Morten Uglum

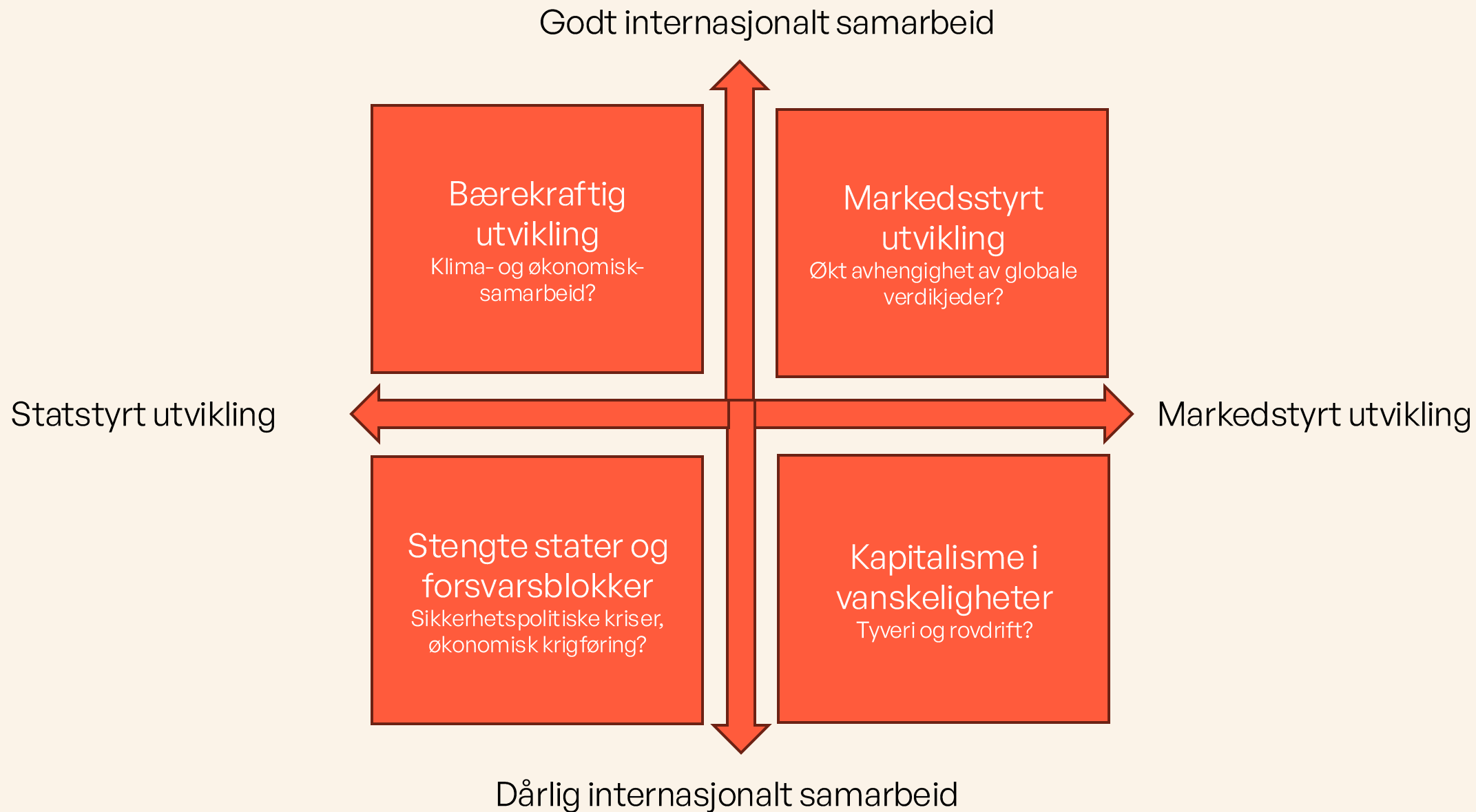
Smarthuset ble et dumt
hus, dummere hus
finnes ikke

Aftenposten 13. des.
2021

Lovkrav til risikovurdering; hva er din risikoaksept?







Cyberkriminalitet globalt er den fjerde største økonomien globalt 10,5 trillioner USD!

*Cyber Rica is the world's third largest economy Press
Release – David Braue, Cybercrime Magazine, 2025*

“Ransomware is also disproportionately affecting small organizations.

In larger organizations, Ransomware is a component of 39% of breaches, while SMBs experienced Ransomware-related breaches to the tune of 88% overall”

(Verizone Data breach Investigation Report, 2025)



Cyberkriminalitet

- Bruk av KI
- Kommersialisering
- Internasjonalt samarbeid
- Geopolitisk ustabilitet og krigføring
- Avansert kriminalitet utøves av et mindre antall individer med lengre erfaring og kompetanse
- Uerfarne kriminelle støttes av KI og kommersielt tilgjengelige verktøy

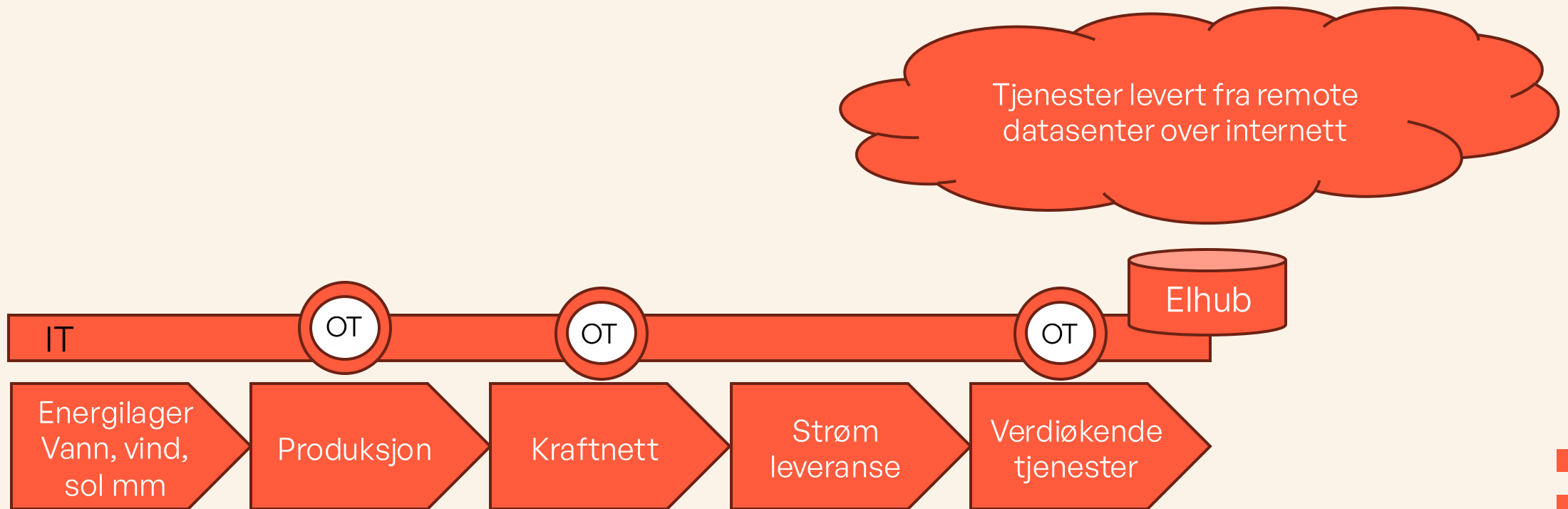


Trusselaktører og trusler

- Cyberoperasjoner som rammer operasjonell teknologi og industrielle styringssystemer kan sette sentrale produksjons prosesser ut av spill.
- I ytterste konsekvens kan slike angrep føre til alvorlige ulykker, driftsstans eller hindre leveranser som samfunnet er helt avhengig av.



Risiko og dilemma knyttet til digitalisering av OT



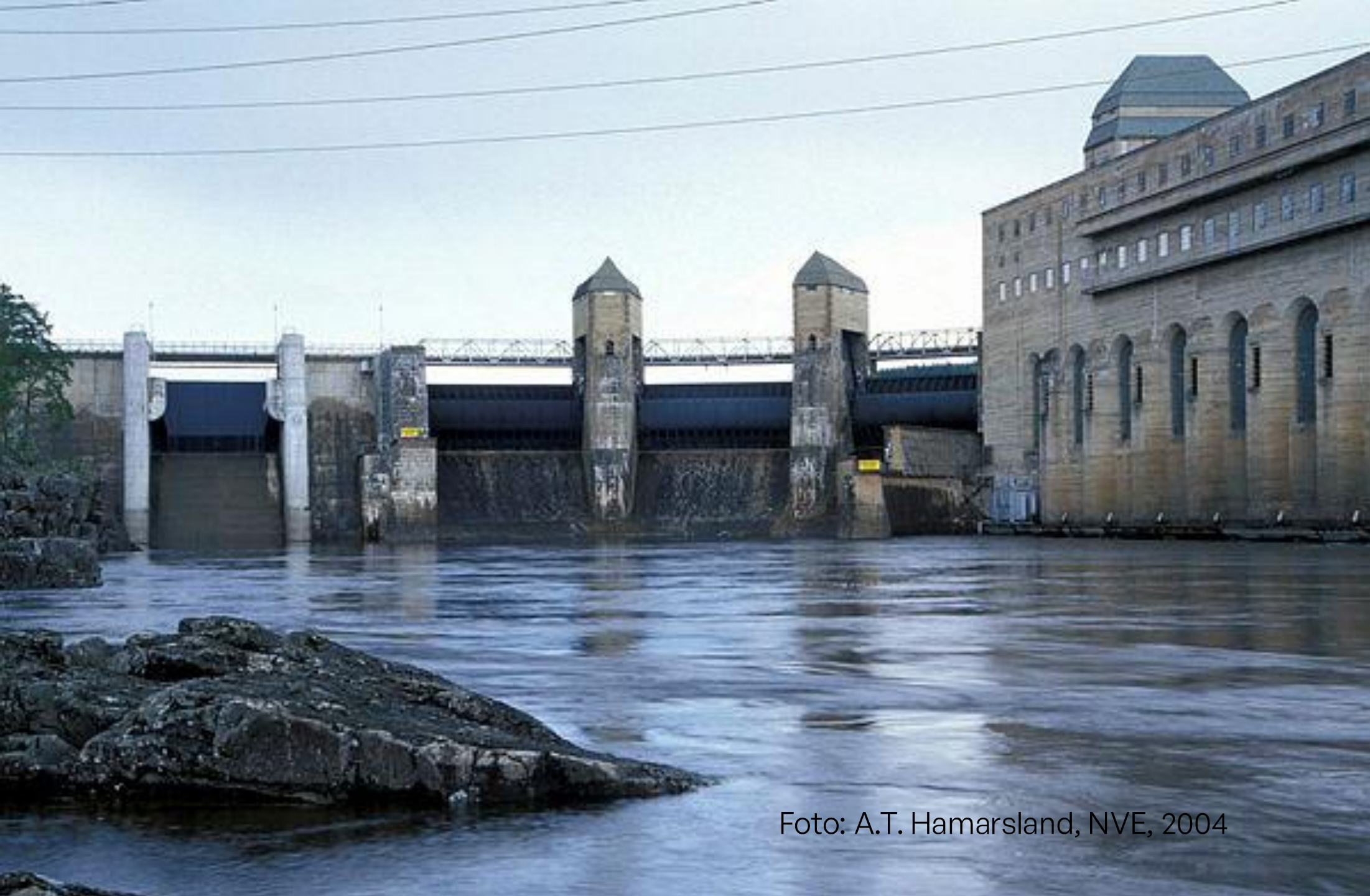


Foto: A.T. Hamarsland, NVE, 2004



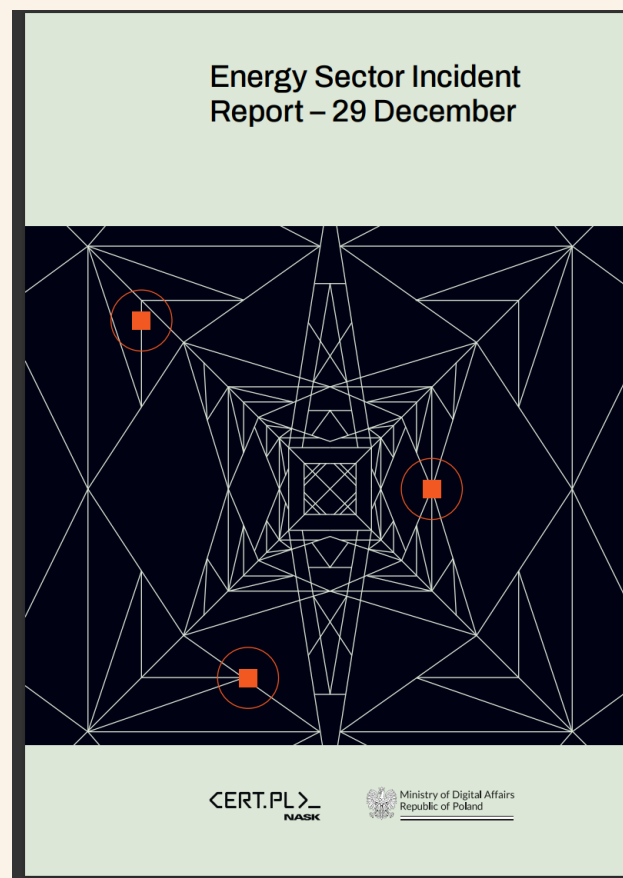
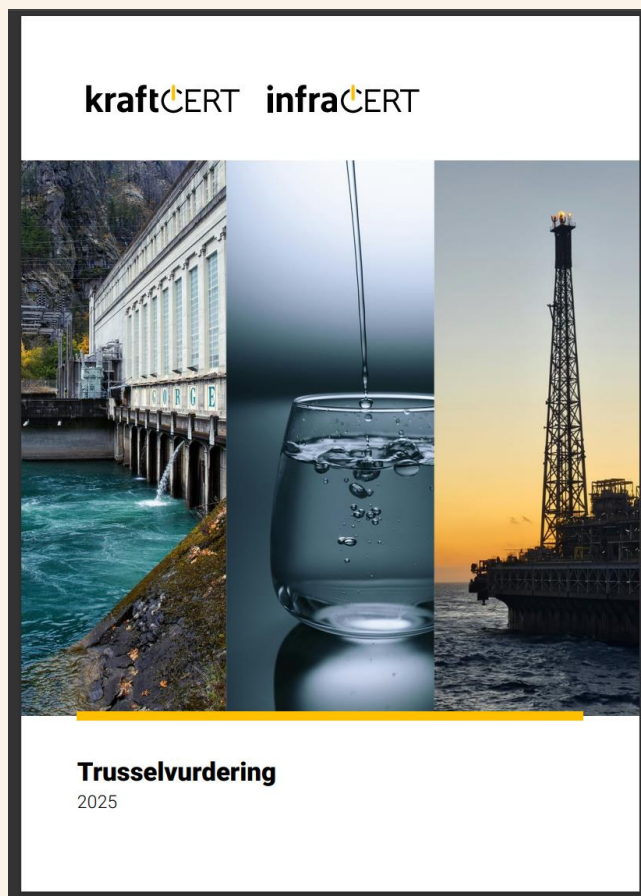
An aerial photograph of the Lista Wind Farm in Norway. The image shows a vast landscape of rolling green hills and rocky terrain dotted with numerous white wind turbines. A prominent road or path winds through the foreground, leading towards the turbines. The sky is filled with large, grey clouds, and the overall scene conveys a sense of a large-scale renewable energy project in a natural setting.

LISTA Vindkraftverk

Foto: S. Oldani, NVE 2020

Hva er risikoen hvis du ikke gjør noe?

Utsatt for kriminalitet, økonomisk tap, omdømmetap



Problem A: Minimer forventet risiko ($\mathbb{E}[L]$)

Mål:

$$\min_x \sum_{s \in S} p_s L_s(x) = \sum_{s \in S} p_s (L_s^{(0)} - \sum_{i \in I} b_{si} x_i)$$

Begrensninger:

1. Budsjett (økonomi):

$$\sum_{i \in I} c_i x_i \leq B$$

2. Regelverk (compliance):

(a) Dekningskrav pr. regel r :

$$\sum_{i \in I} a_{ri} x_i \geq \theta_r \quad \forall r \in R$$

(b) Eventuelle "must-have"-tiltak $M \subseteq I$:

$$x_i = 1 \quad \forall i \in M$$

3. Praktiske muligheter:

(a) Ressurs-/kapasitetsbegrensning (én samlet):

$$\sum_{i \in I} h_i x_i \leq H$$

(b) Avhengigheter (rekkefølge/forutsetning):

$$x_j \leq x_i \quad \forall (j, i) \in \mathcal{P}$$

(c) Begrensning på antall parallelle tiltak (enkelt, hvis du vil begrense kompleksitet):

$$\sum_{i \in I} x_i \leq K$$

(velg K for en gitt periode/prosjektportefølje).

Variabeldomene:

$$x_i \in \{0, 1\} \text{ (eller } [0, 1]) \quad \forall i \in I$$

Kommentar: Dette gir en miks-heltallig lineær modell som de fleste standardlødere (CBC, Gurobi, CPLEX, SCIP) håndterer effektivt.

4) Problem B: Minimer hale-risiko (CVaR) osv

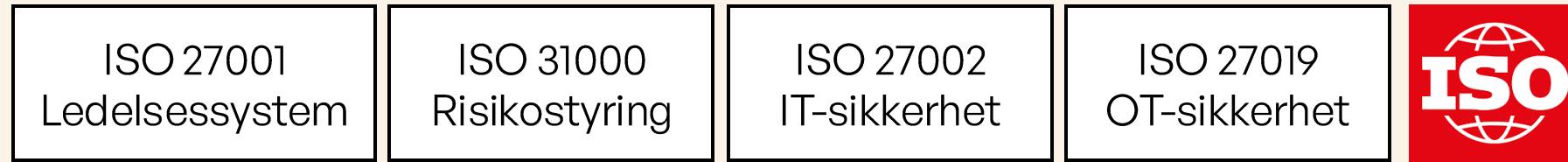
Hvor ligger balansen?

- Lovverk setter begrensninger og gir pålegg!
- Risikoapetitten til styre- og ledelse
- Reell betalingsvilje- og mulighet
- Beslutningstakeres og rådgiveres risikoforståelse
- Beredskap

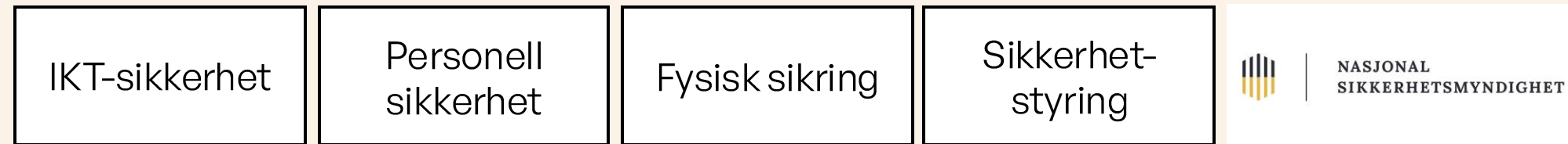


Slik kan du styre risiko og hente verdi mellom IT og OT

Har du mye ressurser og er en stor virksomhet:



Har du lite ressurser og er en liten virksomhet, NSMs Grunnprinsipper for:



Lovkrav gjelder – husk å sjekk disse!





Griter



Wikimedia Commons

- Takk for tiden din og for at du lyttet
- Kontakt meg gjerne på LinkedIn eller epost janne.hagen@griter.no



Janne Hagen

Director and Head of OT-Security

+4790529180

Griter.no



UNIVERSITETET
I OSLO