

Når krisen kradser!

Søren Bank Greenfield

It og digitalisering

Cyber- og informationssikkerhedsafdeling.

Digital Sundhed Danmark





Digital Sundhed Danmark - Helt kort

Digital Sundhed Danmark er sat i verden for at understøtte sundhedsreformen gennem data, digitale løsninger og fælles infrastruktur.



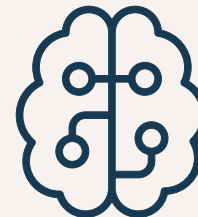
Understøtte
omstilling til det
nære
sundhedsvæsen



Understøtte
sammen-
hængende
patientforløb



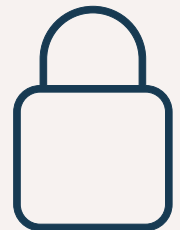
Udvikle og udbrede
brugervenlige
digitale løsninger og
infrastruktur



Styrke det
innovative
sundhedsvæsen



Sikre
sundhedsdata i
verdensklasse



Sikre et robust
beredskab
indenfor
cybersikkerhed

Data er ikke et mål i sig selv. Data skal skabe nærhed, sammenhæng og bedre behandling.

Sikre og bevare borgernes tillid!



Når krisen kradser!

Er vi så klar?

En multifacetteret tilgang til:

- digital suverænitet
- robusthed
- handlefrihed



Bevare tilliden



Når cybertruslerne står for døren, sårbarhederne er "uendelige" og de geopolitiske vinde blæser kraftigere og kraftigere

– hvordan skaber vi så et robust og cybersikkert sundhedsvæsen som borgerne kan stole på??

Rammer og termer



Sikkerhed vs Robust vs Resiliens

Sikkerhed



Robusthed

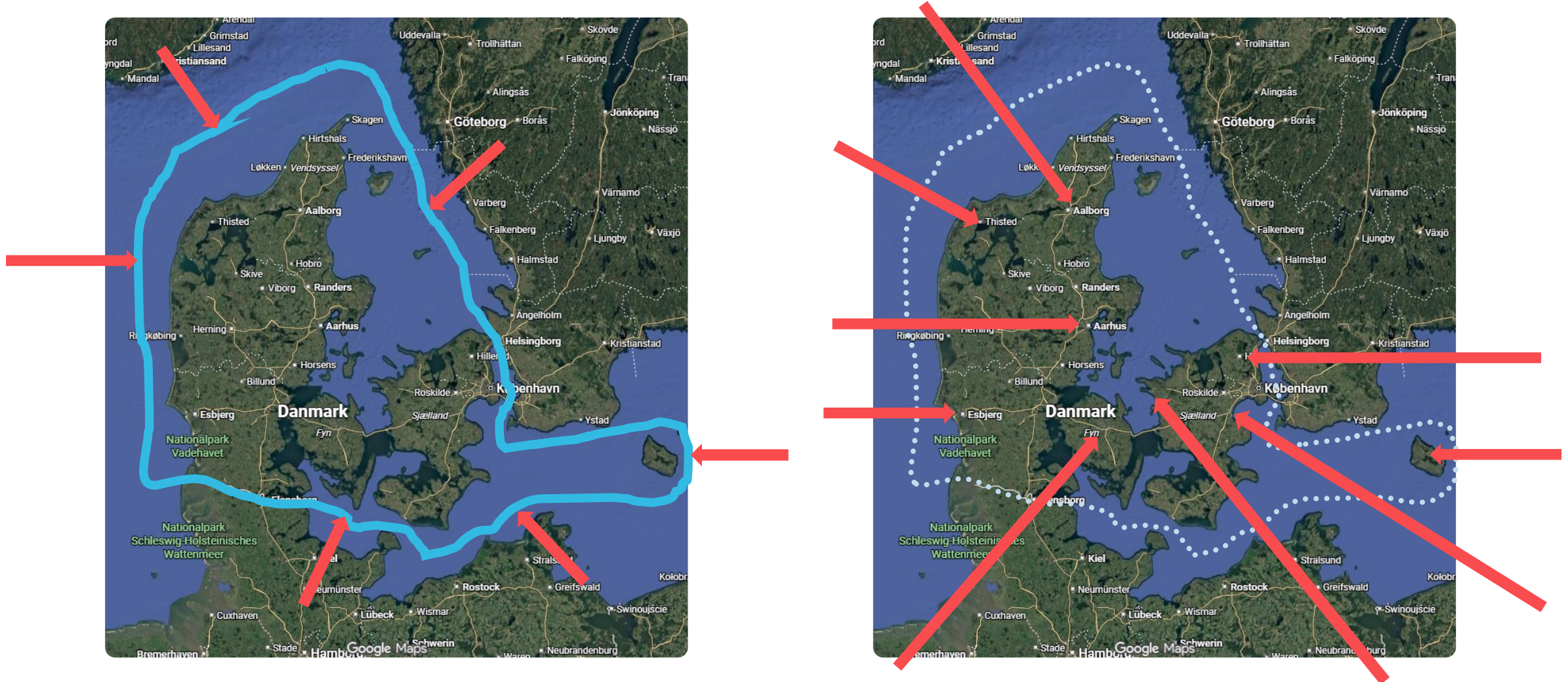


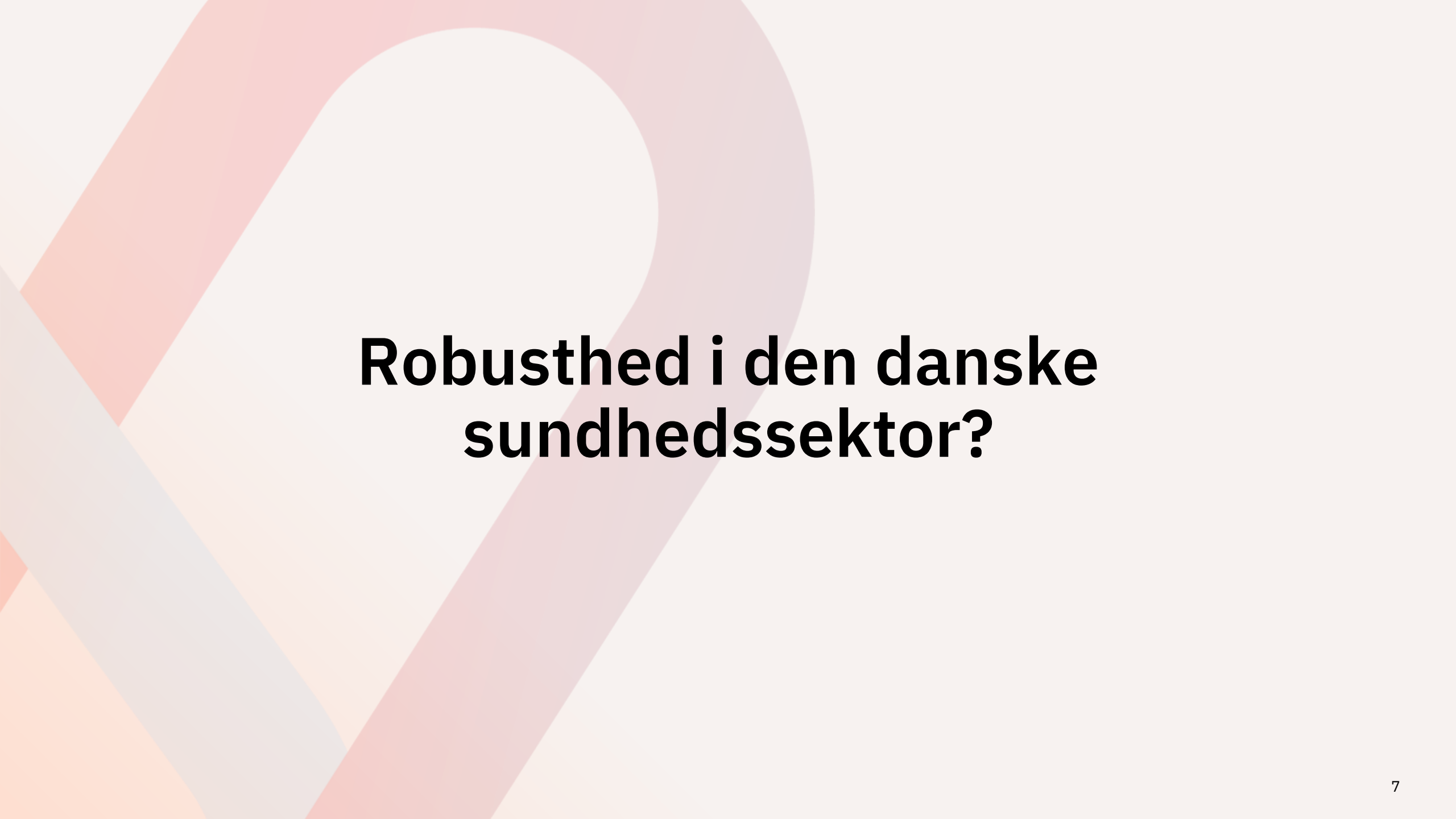
Resiliens





Suverænitet vs digital suverænitet (illustration)





Robusthed i den danske sundhedssektor?



”

Den sikkerhedspolitiske situation er yderligere forværret. Rusland har intensiveret sin anvendelse af sabotage, destruktive cyberangreb og angriber mål i Europa med droner.

Hybridkrigen eskalerer.

Forsvarets Efterretningstjeneste, Vurdering af truslen fra Rusland, 24. september 2026, s. 1



NATO 2026 Resilience Baseline Requirements

- Baseline Requirement 1: Assured Continuity of Government and Critical Government Services
- Baseline Requirement 2: Resilient Energy Supply
- Baseline requirement 3: Ability to Manage Controlled and Uncontrolled Movement of People
- Baseline Requirement 4: Resilient Food and Water Resources
- **Baseline Requirement 5: Resilience To Deal With Mass Casualties And Disruptive Health Crises**
- Baseline Requirement 6: Resilient Civil Communications Systems
- Baseline Requirement 7: Resilient Civil Transportation Systems

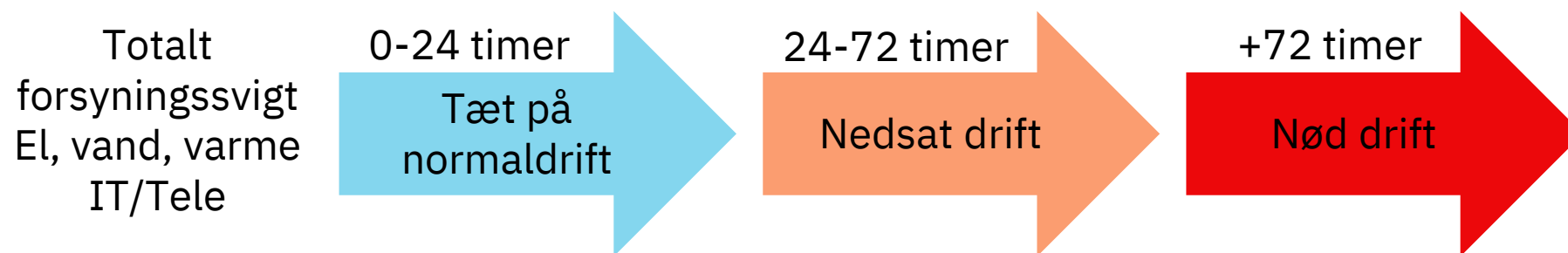


Ny vejledning til regionerne om opretholdelse af sygehusdrift i tilfælde af forsyningssvigt



Målsætninger for sygehusenes drift

Det er målsætningen, at sygehusene, i stedet for at imødegå forsyningssvigt med en umiddelbar nedskalering af driften, sigter efter at kunne opretholde *tæt på normal drift* med mindre påvirkninger i minimum 24 timer, og at der først herefter vil være behov for at gå på *nedsat drift* samt *nøddrift* efter 3 dage i forbindelse med totalt forsyningssvigt. Definitionerne af de tre driftsniveauer samt hvordan de håndteres fremgår af bilaget.





Hvor afhængig er vi?

**Der er vand til –
”Et tryk i
toiletterne”**

**”Vi begynder at
sende patienterne
hjem efter 15
minutter uden
internet”**

**Bil og enheder
indeholder samlet
over 20 simkort!**

**Fra en
leverandør...
På grund af
udbudsregler**

**Husker man
nødstrøm til
funktioner der
udføres af
robotter?**

**F.eks. på
apoteker?**



Hvordan løser man det??



Handlefrihed

Der er **ingen** "Silver bullet"

Alt "ikke EU" er farligt!

- Hvad er definitionen af "ikke EU"?
- Hvor langt går man ned i komponenterne?
- Hvad så med alle data der flyder gennem core routere?
- Hvor der deres CPU'er produceret?
- Igennem hvilke lande er de blevet fragtet?
- Af hvem?

Open source svaret!

- Har du overblik over alle "open source libraries", der er brugt hos dig?
- Hvad så når det produkt bliver så godt at det bliver købt?
- Hvem har lavet den software?
- Hvad med al den software, der er lavet af AI?
- Hvor har den hentet sin kode fra?
- Har du set alt din kode igennem – selv?

Kun "danske" leverandører!

- Hvad er en dansk leverandør?
- Hvem ejer dem som så ejer dem og hvem ejer dem...?
- Bruger de ingen "ikke dansk software"?
- Bruger de kun dansk udstyr?
- Hvad er dansk udstyr?
- Hvilken leverandør af PC har staten?
- Hvilke telefoner?

Alt skal være on prem!

- Fin start men hvad så med opdateringer, sker de online direkte til hver server?
- Er du virkelig en "ø"?
- Hvad med dine hardware komponenter – firewallen?
- Hvem er din internet udbyder?

Vi skal da bare gå "offline"!

- Urealistisk i en verden med de udfordringer og ønsker vi har.



PACE princippet i digital resiliens



P rimary
A lternative
C ontingency
E mergency

13. Cyber Defence and Digital Resilience

- Mission assurance shall be enhanced by embedding Zero Trust principles across all digital infrastructure to strengthen NATO's cyber defence and digital resilience, ensuring continuous verification, least privilege access, and secure handling of data, users, and systems.
- NATO shall accelerate the adoption of post-quantum cryptography to ensure long-term protection of sensitive data and communications, mitigating future threats posed by quantum computing and preserving strategic information superiority.
- Mission critical services shall be identified, prioritised, protected and continuously optimised to ascertain mission assurance and uninterrupted execution of core functions across static, mobile and dispersed warfighting Headquarters. The resilience and survivability of mission critical services shall be ensured through redundant and diversified technical solutions, based on the PACE (Primary, Alternate, Contingency, Emergency) principle.

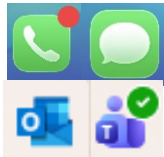


(illustration) Procesnedbrydning med PACE

Beredskabskommunikation

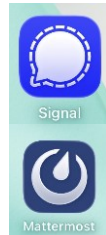
Primær (P)

- Telefoner
- Teams
- Outlook



Alternativ (A)

- SIGNAL app
- MatterMost



Krise (C)

- SINE radioer



Nød (E)

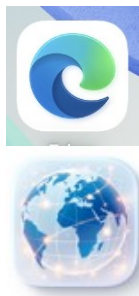
- Satellit telefoner



Dataudveksling

Primær (P)

- Internettet



Alternativ (A)

- SundhedsDataNettet



Krise (C)

- Nøddatanetværk



Nød (E)

- USB-nøgler personbåret



Gå fra binær til multifacetteret tilgang til digital suverænitet, robusthed og handlefrihed



Binær tilgang

- En løsning, der løser det hele
- Løsningen vil også være relevant i både fred, nedbrud, krise og krigstider!



Multifacetteret tilgang

- Tænkt ikke i kun sikkerhed - men **også robusthed og resiliens**.
- Fokuser på **den trussel man rent faktisk prøver at undgå**.
- **Handlefrihed kan** betyde flere leverandører
- Hav HELT styr på den software, der bliver brugt hos jer – **”managed open source”**.
- **Brug PACE** til at gennemgå leverance af samfundskritiske aktiviteter
- **Opbyg alternative løsninger** – enten tekniske eller alternative processer (ja man kan ikke det samme som i de primære).



Tak for ordet



Følg med på LinkedIn for seneste nyt

Vil I være med til at skabe resiliens i sundhedssektoren?
Sundcert@sundhedsdata.dk