Beskyttelse av digital infrastruktur i en skjerpet trusselsituasjon

Christian Bull, CISO
Telenor Norge

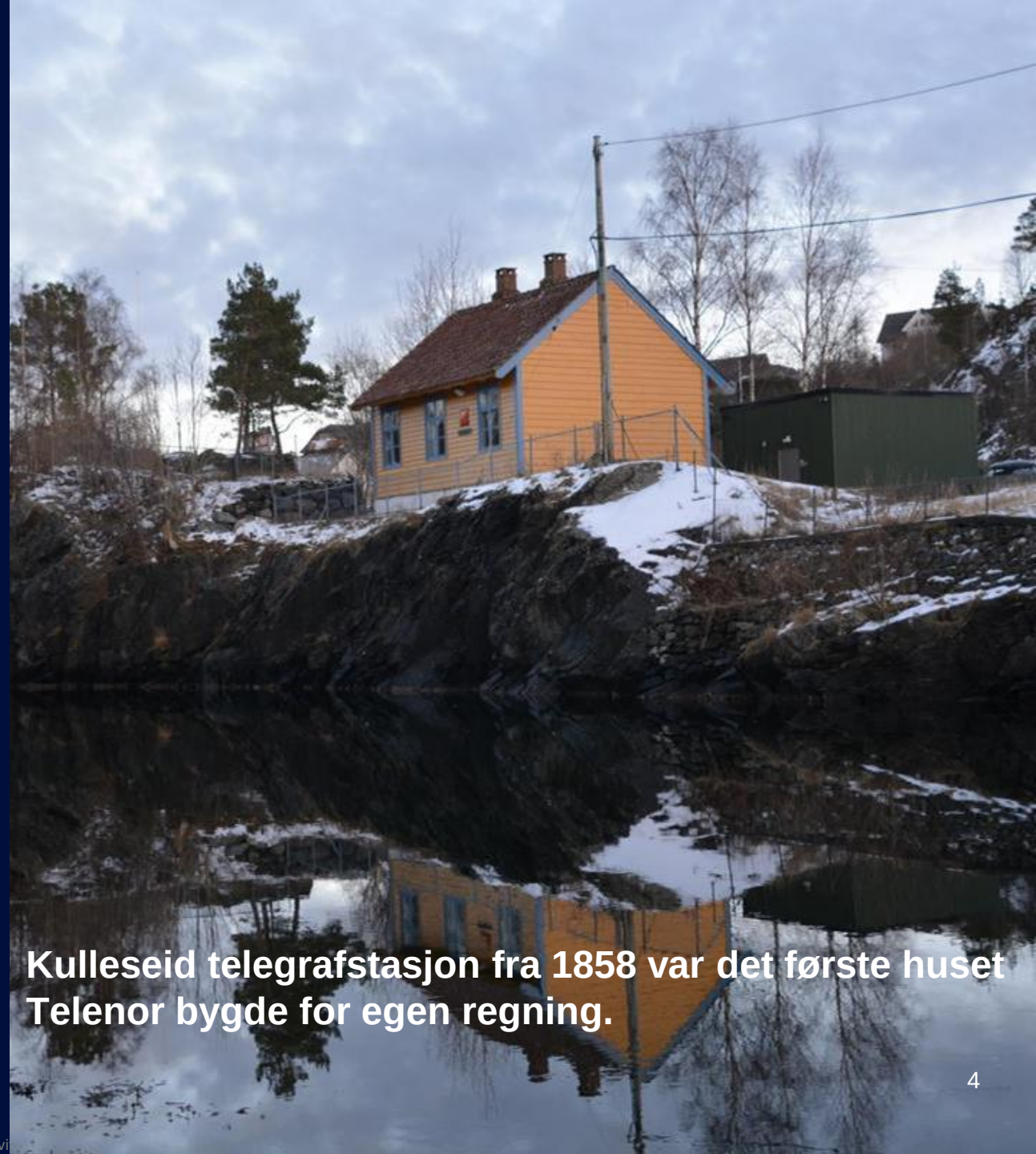
- Intro
- Trusselsituasjonen slik vi ser den
- Hvordan forholder vi oss til den?

Kort om meg

- Leder Avdeling for informasjonssikkerhet og arkitektur.
  - 9 år i Telenor. 7 av dem som IT-sikkerhetsarkitekt.
- Tidligere Seniorrådgiver i Kommunal- og regionaldepartementet.
  - Valgavdelingen. Sikkerhetsansvarlig i E-valg prosjektet som moderniserte støttesystemene for valggjennomføring.
- Startet mitt yrkesliv som rådgiver innenfor informasjonssikkerhet og personvern i NAV og Arbeids- og velferdsdirektoratet, hvor jeg en kort periode var CSO.
- Formelt er jeg samfunnsviter, men livslang datanerd…

Kort om Telenor Norge

- Norges største og eldste infrastrukturselskap.
  - Siden 1855.
  - Ca. 2.75M mobilabonnementer i Norge. Ingen fasttelefonkunder.
  - De fleste husstander er på en eller annen måte bruker av våre tjenester.
  - Vårt landsdekkende transportnett «BRUT» flytter noe over 50% av alle IP-pakker på internett i Norge. Ned fra over 80% for 10 år siden.
- En av svært få bedrifter i Norge som driver egen etterretningsinnsamling.



Kulleseid telegrafstasjon fra 1858 var det første huset Telenor bygde for egen regning.

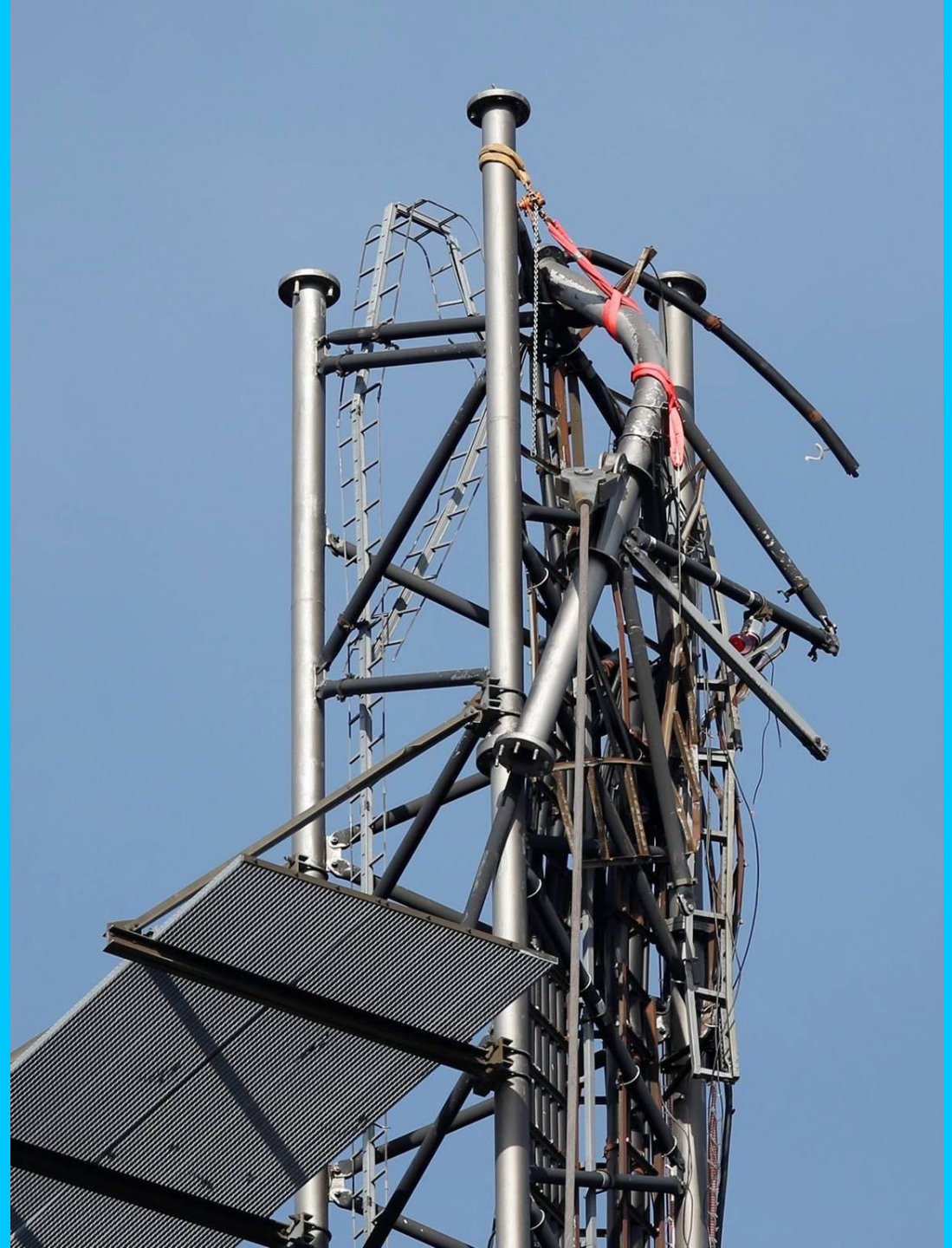
Trusselforståelse er grunnleggende for styring av sikkerhets- og operasjonell risiko

…og vår infrastruktur.

- Mer enn 15.000 «siter» i Norge.
  - Omfatter alt fra «hytter» i skogen til fortifikatoriske anlegg dypt inne i fjell.
  - Satellitter…
  - Tusenvis av lokasjoner i transportnettet.
  - Redundante føringsveier på langs og på tvers i Norge fra Lindesnes til Longyearbyen, og gjennom Sverige.
- Alt er klassifisert og beskyttet ihht. behov…

Trusselbildet

- Telenor er en del av det norske totalforsvaret. Vår samfunnsoppgave er å bygge en robust nasjonal infrastruktur, som kan levere grunnleggende kommunikasjonstjenester i krise og krig.
- Det siste tiåret har det vært en jevnt økende aktivitet mot norske interesser fra utenlandske trusselaktører med ulike motivasjoner.
- Stater, som Kina, Iran, Pakistan og Nord Korea driver betydelig aktivitet mot og i Norge.
- Vi har over lang tid sett russisk vilje til å ta stadig økende risiko i operasjoner utenfor egne grenser i en verdenssituasjon vi betgner som “hybrid ufred”.



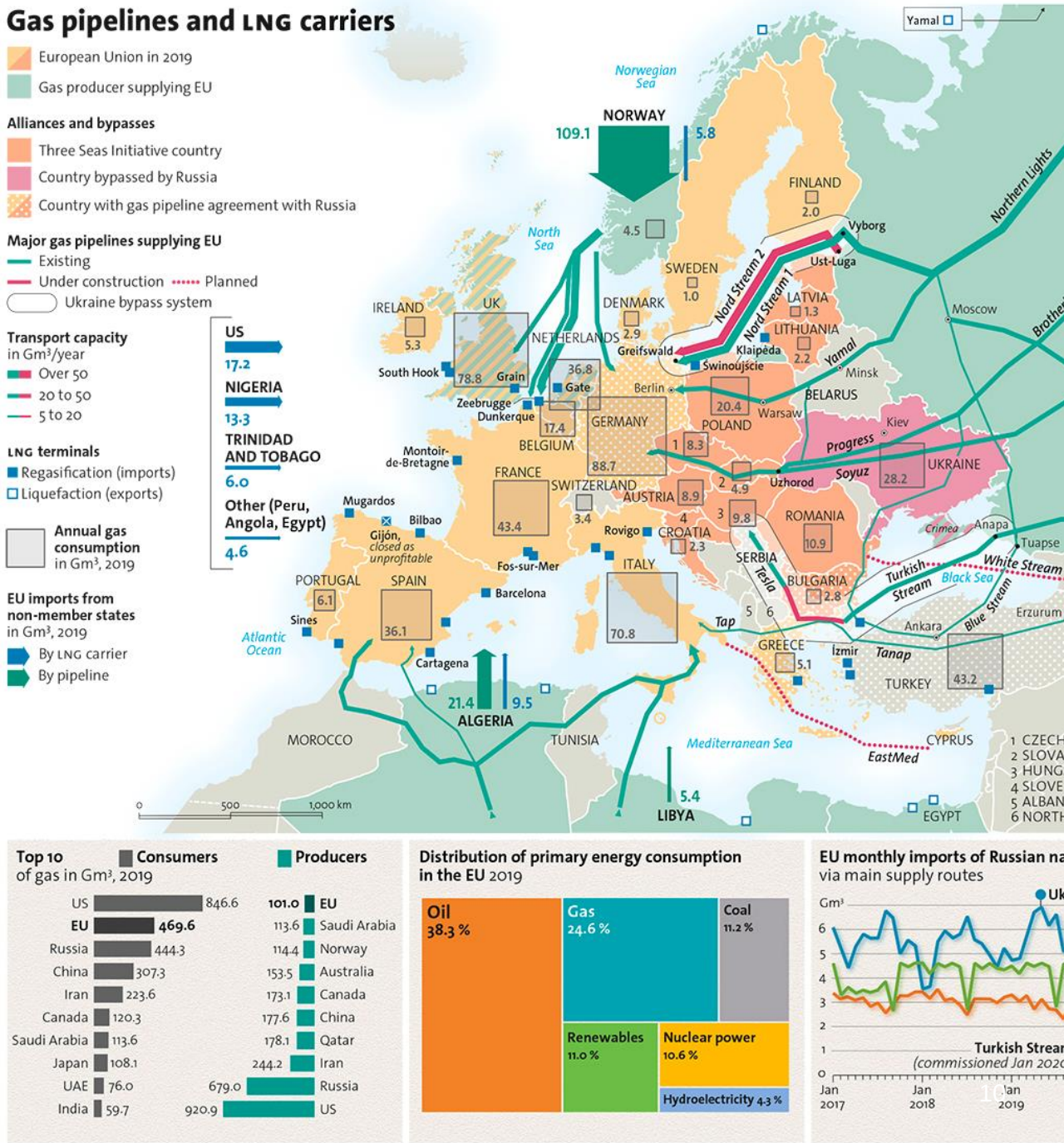
Overfallet på Ukraina

- Overfallet på Ukraina ble innledet med cyberangrep på Ukrainas kommunikasjonsinfrastruktur.
  - Angrepene hadde vidtrekkende konsekvenser også utenfor Ukraina, og slo bla. ut 1500 vindmøller i Tyskland.
  - Målet var primært å slå ut millitær kommunikasjon.
- Imidlertid har den sivile kommunikasjonsinfrastrukturen i Ukraina for det meste holdt stand.
  - Både mobilnett og internett er i stor grad oppe.
- Ingen observert endring i trusselaktørers aktivitet mot våre systemer.
  - Det er tydelig kommunisert at angrep på et NATO-medlems kritiske nasjonale infrastruktur kan bli betraktet som et angrep og kunne utløse NATO-paktens artikkel 5.

https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K

Hva er har endret seg det siste året?

- Krigen går (svært) dårlig for Russland. Mye av grunnen til dette er at Russland mislyktes med sin langsiktige strategi:
  - Vesten har stått samlet i sin støtte til Ukraina, og støtten har bred folkelig støtte.
  - Den «gjensidige avhengigheten» i energisektoren viste seg å være svakere enn antatt.
- Selv om man har klart å frigjøre seg fra russisk gass er Europas energisituasjon fortsatt sårbar.



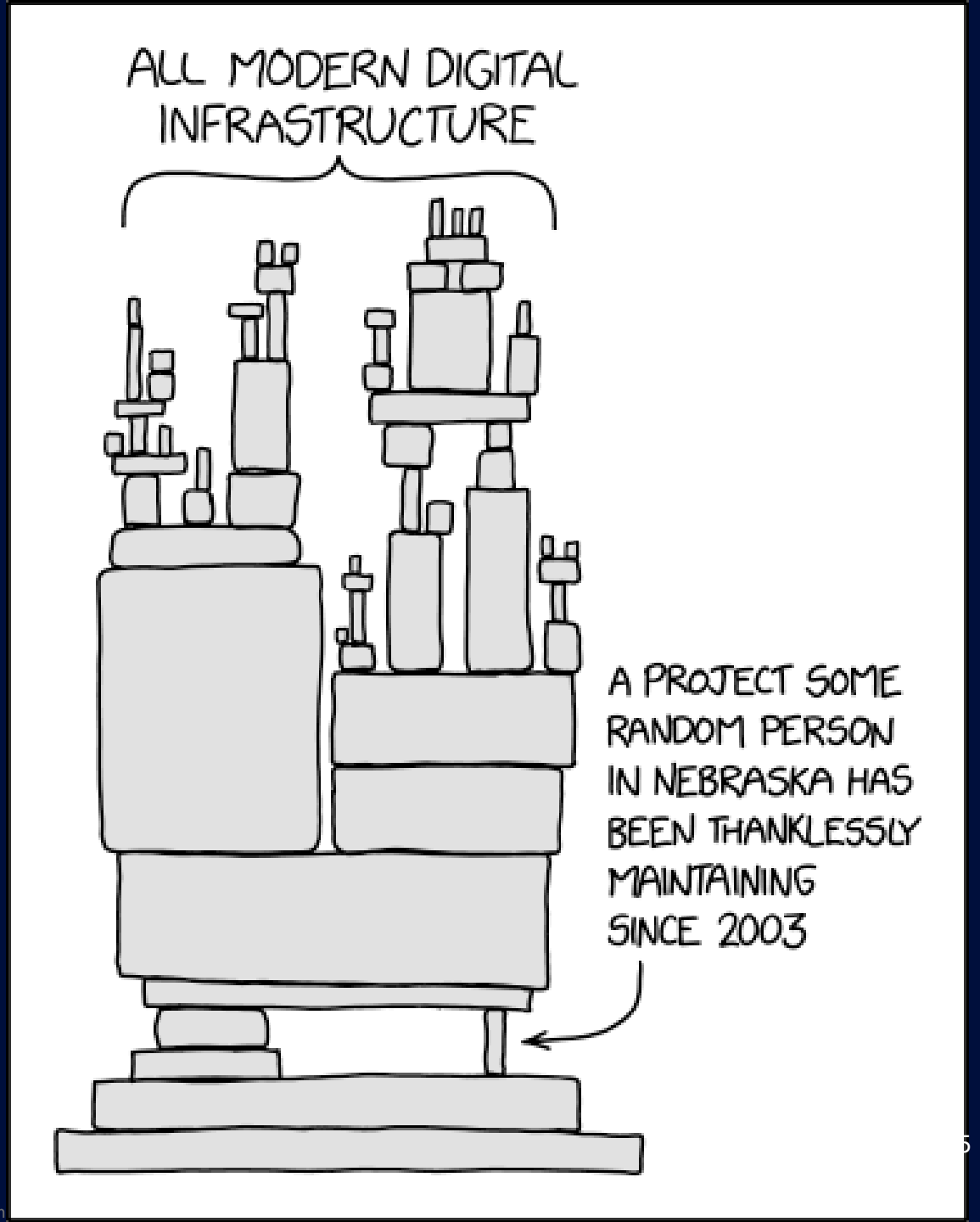
Vår vurdering av trusselsituasjonen akkurat nå.

- Høsten 2022 varslet PST om “forhøyet sabotasjetrussel mot Norge”.
- Vi tror ikke det er noen umiddelbar fare for større aksjoner som kan bringe Russland i åpen konflikt med NATO.
- Imidlertid er det forhøyet risiko for aksjoner ment for signalering.
  - Vil være av mindre omfang og “plausibly deniable”.
- Slike aksjoner kan imidlertid få uforutsette virkninger som medfører større skade enn tiltenkt.
- Energisektoren mest utsatt, men stor fare for at eventuelle aksjoner også vil treffe kommunikasjonssektoren.

Beskyttelse av digital infrastruktur i en skjerpet trusselsituasjon: Hva gjør vi nå?

Visibilitet, visibilitet, visibilitet!

Digital hygiene: vulnerability management



Analog hygiene: hvor vi henter folk

Pentesting av alt! Hele tiden!

Ha en plan for hva du skal gjøre når det går skikkelig galt!

Oppsummert:

- Vi har en skjerpet trusselsituasjon, med økt sannsynlighet for sabotasje. Sannsynligheten er imidlertid ikke *veldig* høy.
- Situasjonen tilsier ikke at vi trenger å gjøre noe radikalt nytt. Vi har hatt god tid på å forberede oss.
- Ting kan imidlertid skje raskere enn tidligere, og situasjonen kan endre seg raskt.