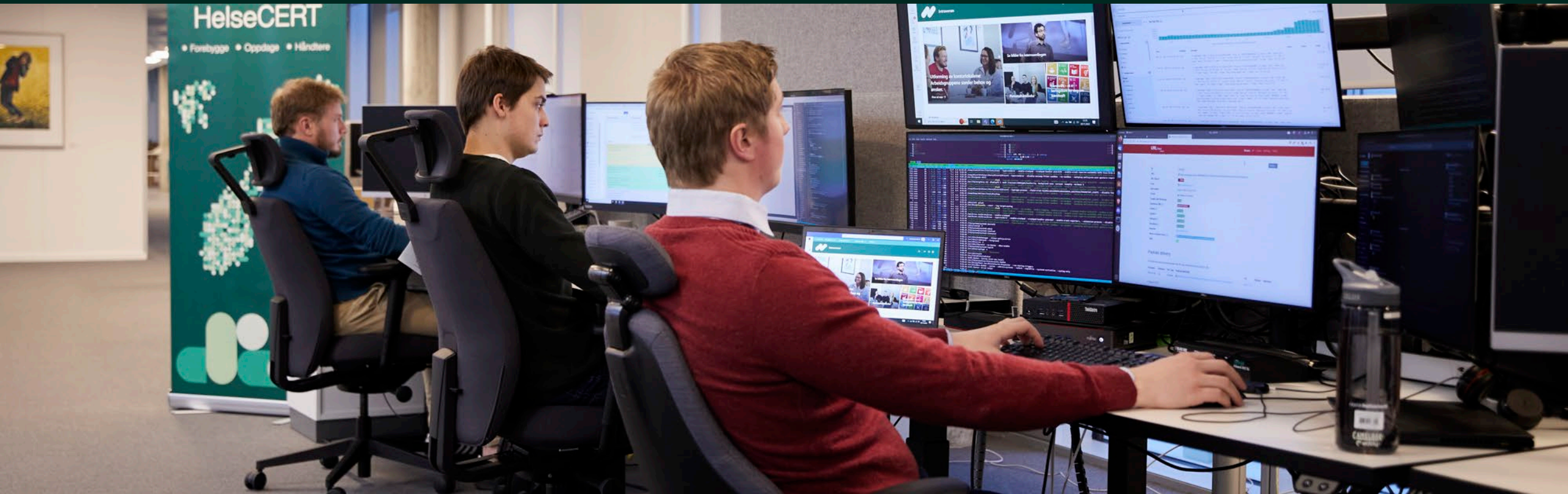
Norsk helsenett

Cybertrusler og tilstand

Dimensjonerende og statlige

Hans Kristian Strømme
Helse- og KommuneCERT

NOKIOS
23. oktober 2025

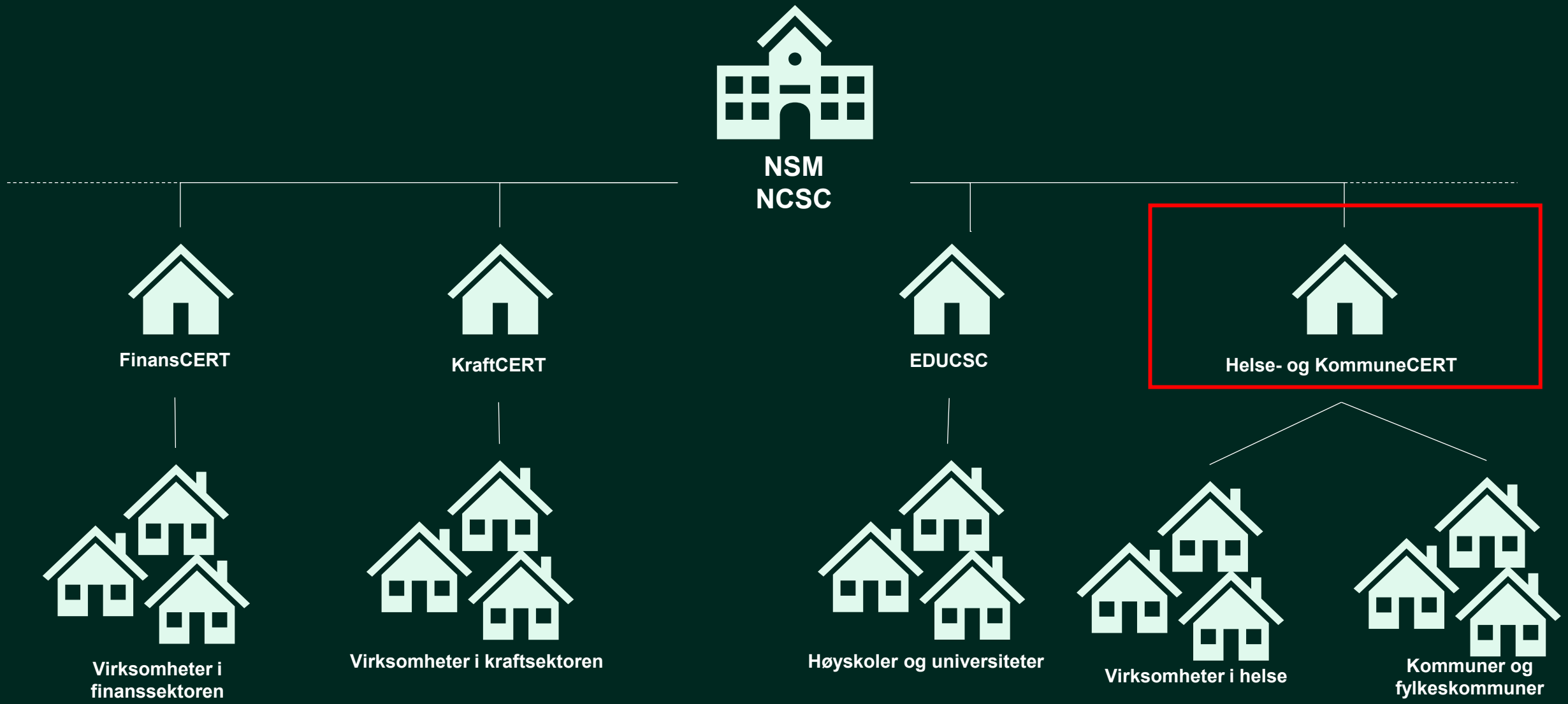


Agenda

- Hvem er jeg og vi
- Trusselbildet i cyberdomenet
  - Dimensjonerende – ransomware
  - Statlige – Kina, Russland
- Tilstanden "der ute"
- Anbefalinger

Kommunikasjonslinjer

Sektorvis responsmiljøer



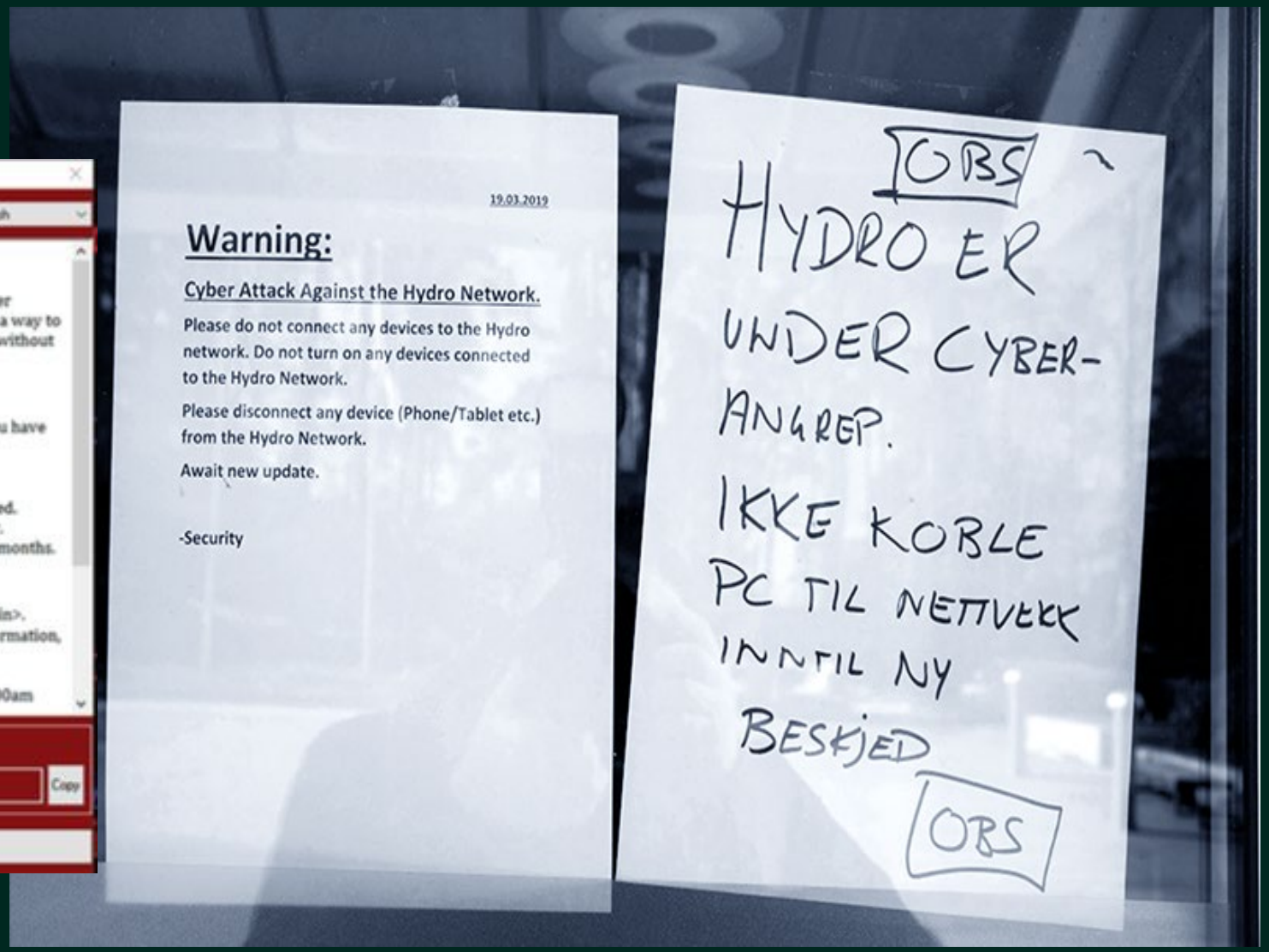
Helse- og KommuneCERT

- Sektorvis responsmiljø (SRM) for helse- og kommunesektoren
- HelseCERT etablert i 2011
- KommuneCERT fra 1.12.2023
- 32 ansatte

- Helse- og KommuneCERT er en felles enhet.

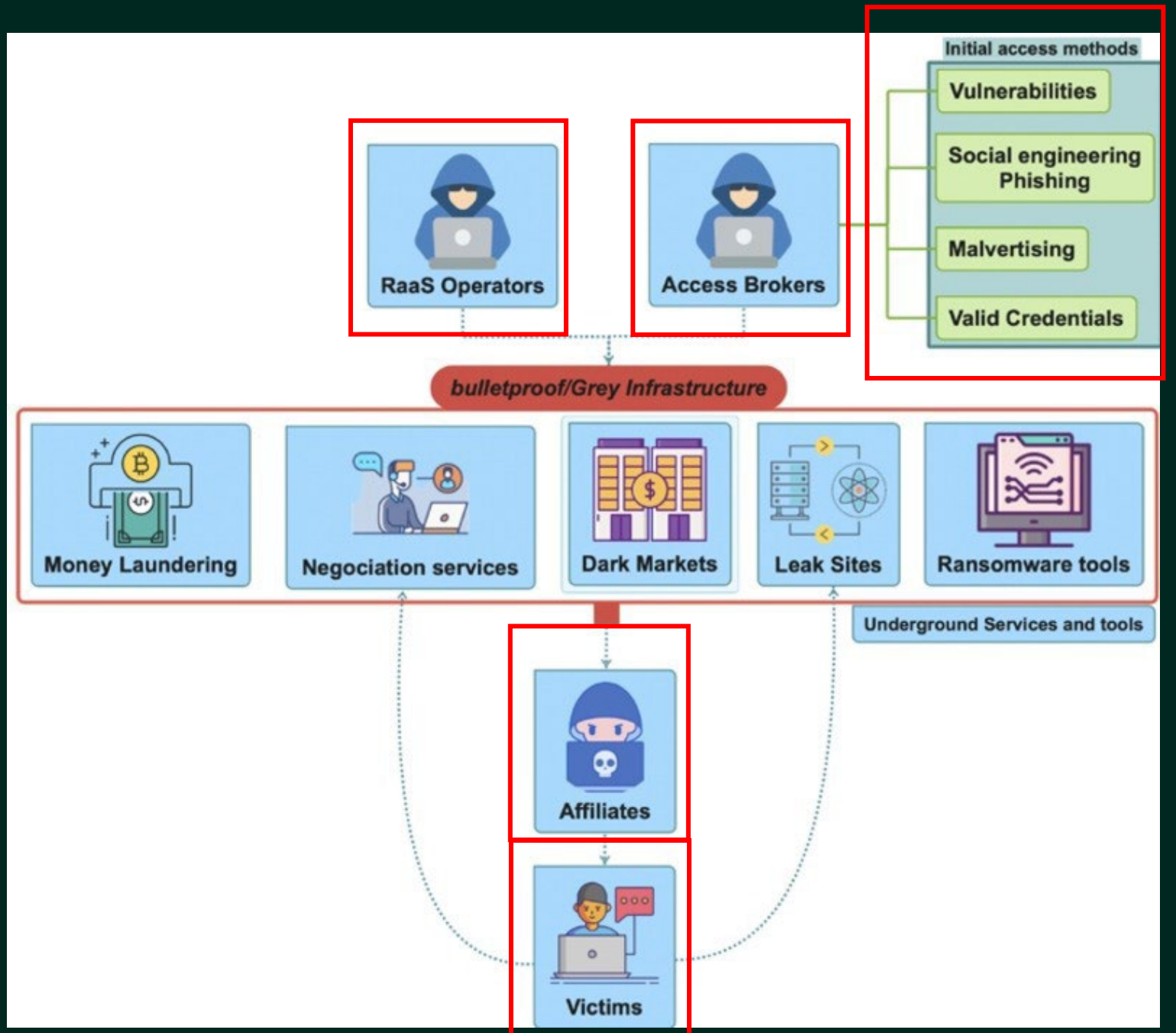
- Forebygge, oppdage, håndtere tilsiktede cyberhendelser
- Helse- og Kommunesektor sikrere

Trussel - dimensjonerende



Opportunistiske

- Økosystem
- Spesialisering

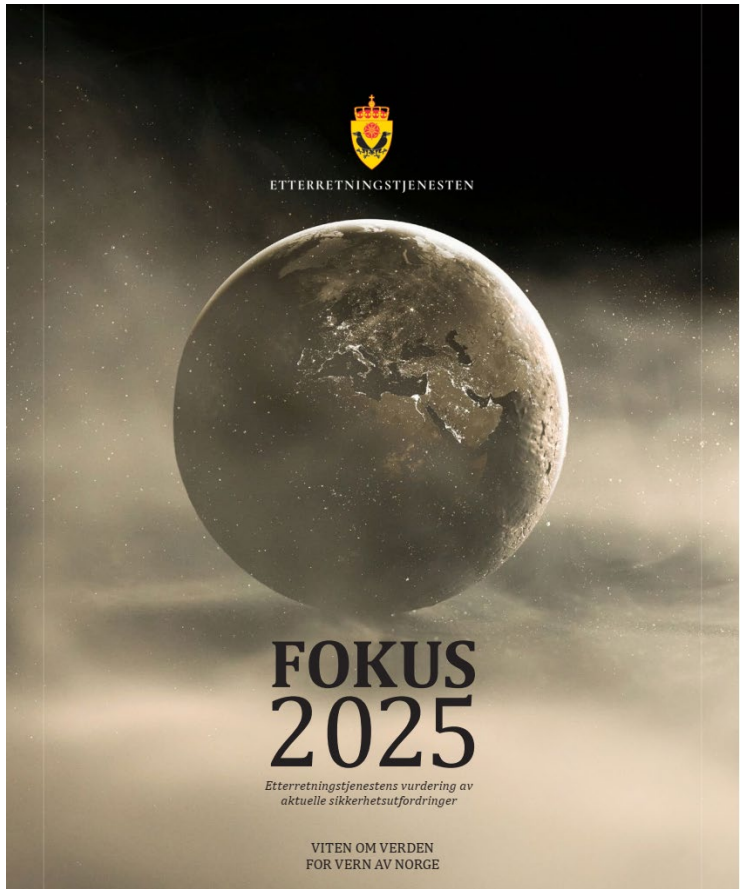


Opportunistiske

- Mål:
  - Mest mulig penger
    - For minst mulig arbeid
      - Og minst mulig (opplevd) risiko

Statlige

Trusselvurderinger

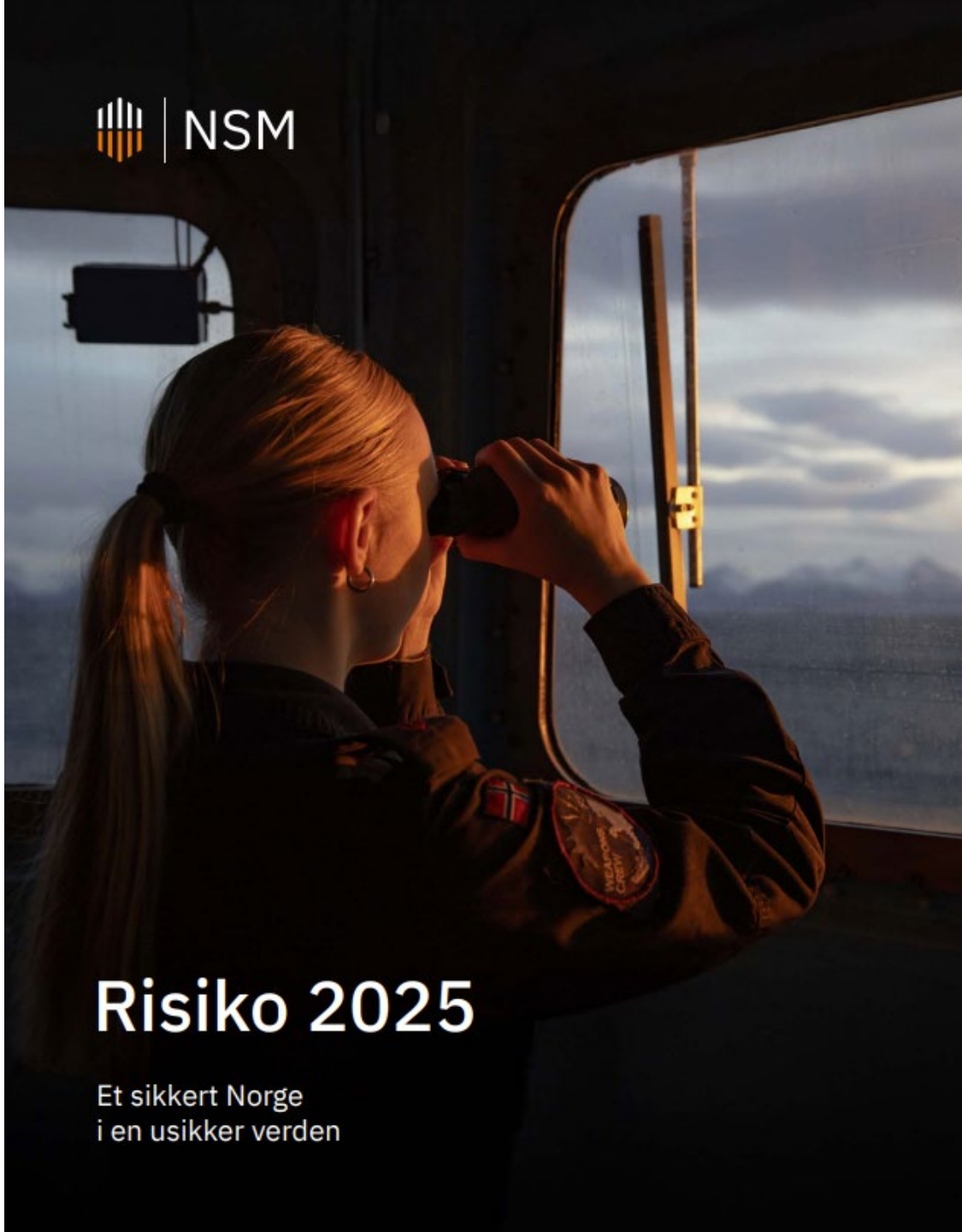


Statlige

Sikkerhetsutfordringer

- Sabotasjeforsøk i Norge er sannsynlig
- Vi blir utsatt for cyberangrep fra andre stater
- Infrastruktur og sårbarheter blir kartlagt av fremmede stater

- Utfordrer vår motstandsdyktighet
- Vi må sikre verdier og redusere sårbarheter
- Risikobildet krever handling



Kina

- Langsiktig

Russland

- Økende risikovilje

Kina jobber langsiktig

Kina jobber langsiktig

Ukraine's airport, metro system hit by new cyber attacks

BY | KIEV | OCT 24, 2017 - 12:00 AM GMT+3 |

|Reuters Photo

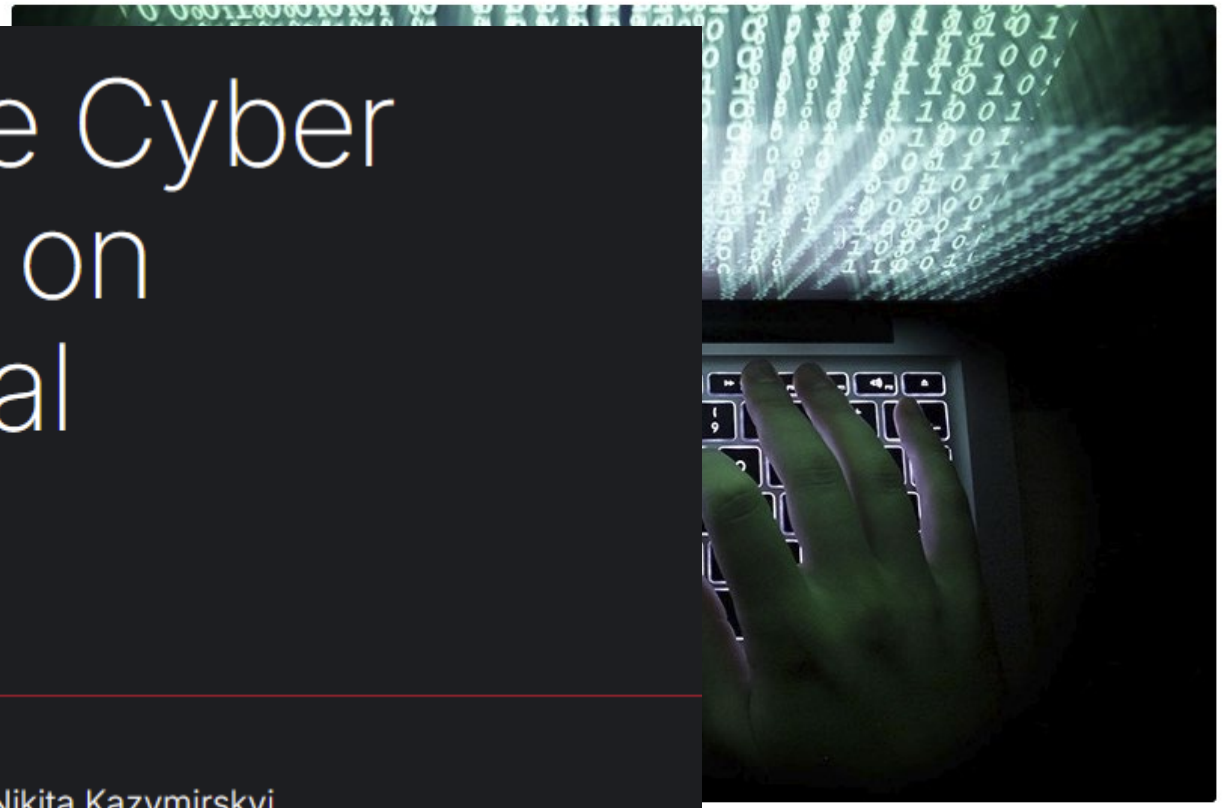
Cyber attacks hit Ukraine's Odessa airport and the metro system in Kiev on Tuesday, with the state-run Computer Emergency Response Team (CERT) saying a new wave of hacks was hitting the country and asking transport networks to be on particular alert.

The Russia-Ukraine Cyber War Part 3: Attacks on Telecom and Critical Infrastructure

March 05, 2025 | 8 Minute Read | by Pawel Knapczyk and Nikita Kazymirskyi

Ukraine's airport, metro system hit by new cyber attacks

BY | KIEV | OCT 24, 2017 - 12:00 AM GMT+3 |



Cyber attacks hit Ukraine's Odessa airport and the metro system in Kiev on Tuesday, with the state-run Computer Emergency Response Team (CERT) saying a new wave of hacks was hitting the country and asking transport networks to be on particular alert.

Kina

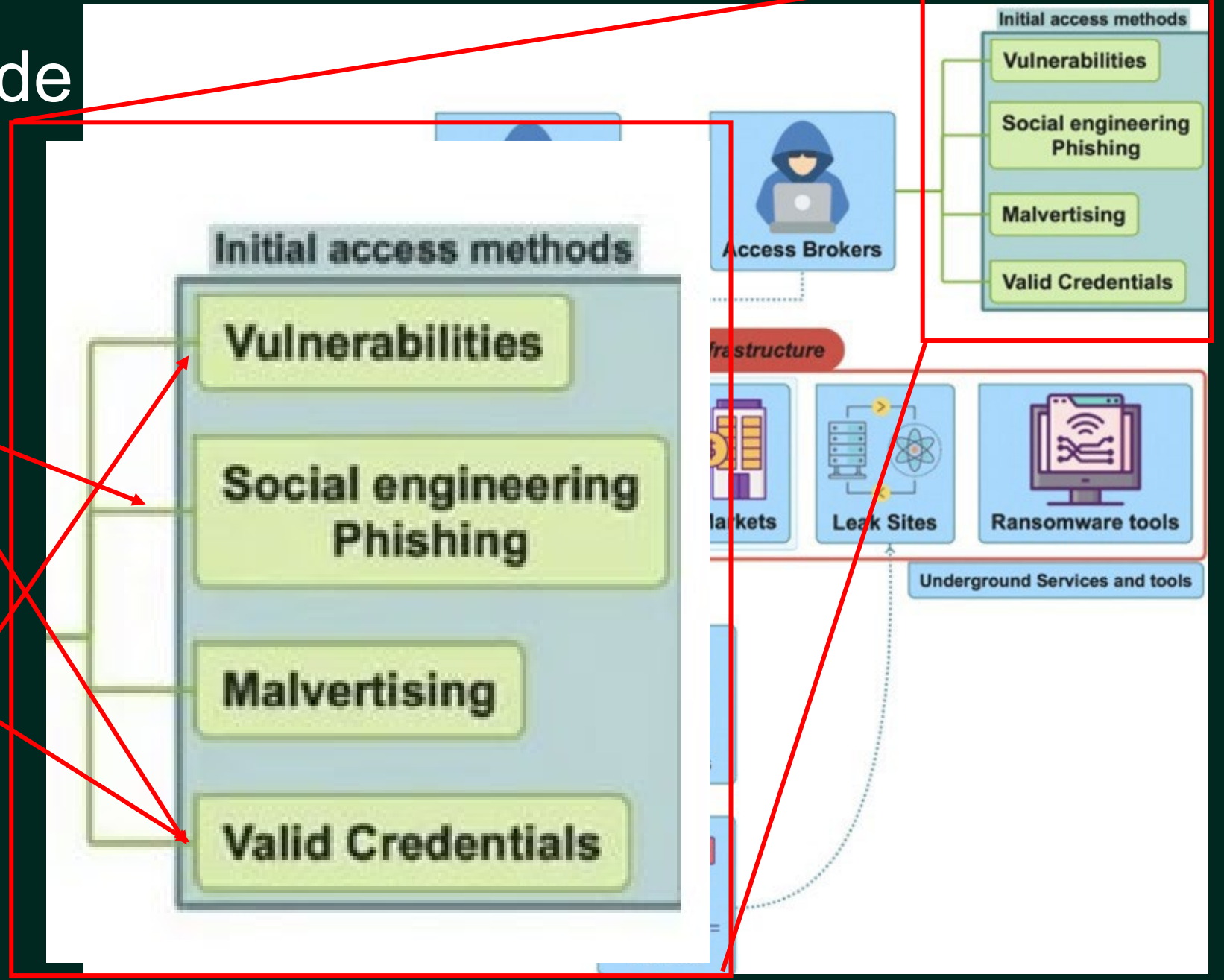
- Langsiktig
  - Strategisk posisjonering
  - Teknologi som interesserer Kina
  - Jobber målrettet etter sårbarheter som inngangsvektor

Russland

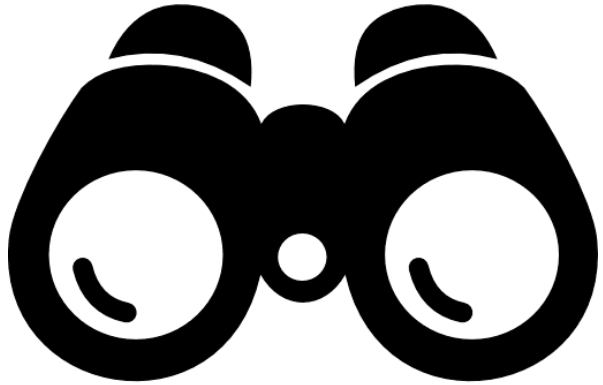
- Cyberangrep som politisk pressmiddel
- Økt risikovilje
- Destruktive angrep
  - (så langt fokusert mot Ukraina)

Hvordan kommer de

- Vi ser noen få vanlige inngangsvektorer
  - Phishing som omgår multifaktorautentisering
  - Kompromitterte brukernavn og passord (og manglende MFA)
  - Sårbarheter eller dårlig/manglende passord i internetteksponert utstyr



Hvordan er tilstanden "der ute"?

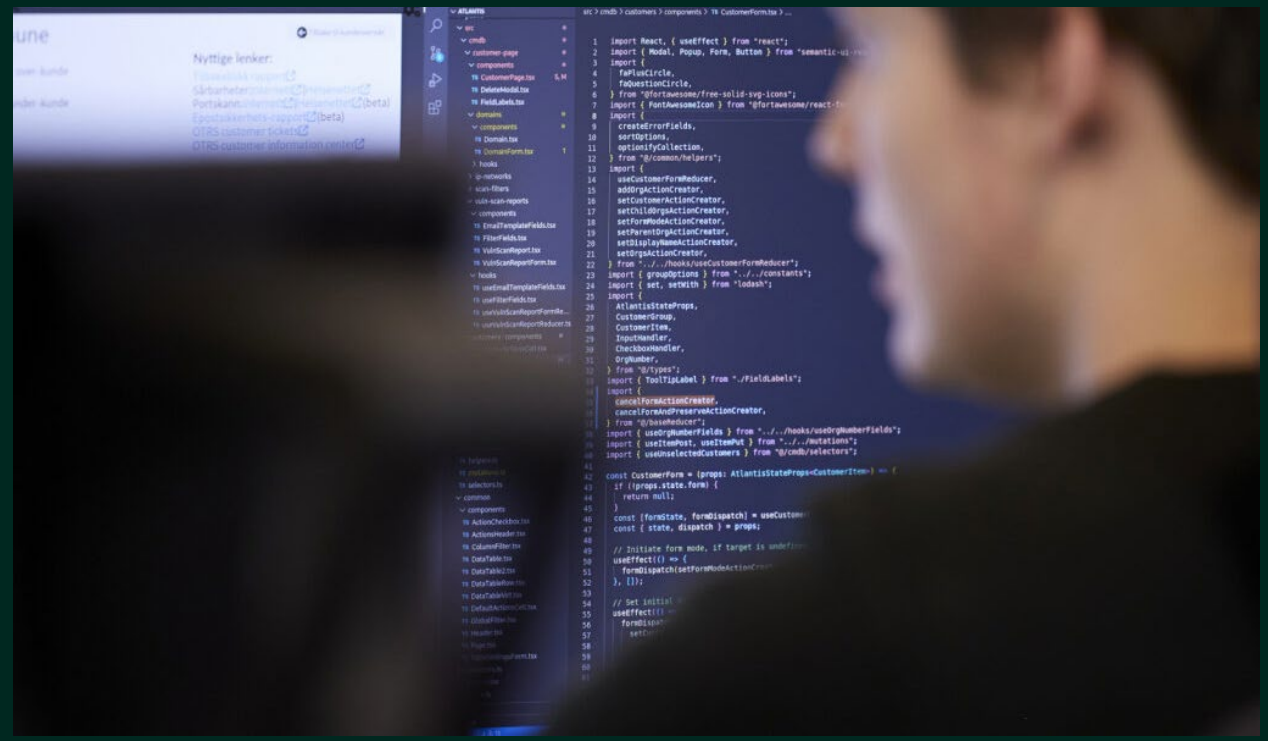


Resultater fra våre kommunetester

- Testet over 115 virksomheter så langt
  - Kommuner, fylkeskommuner, helseforetak, helseregioner
- Erfaringer
  - Stor forskjell på modenhet
  - Person- og ressursavhengig
  - Enkle tiltak er ikke gjennomført
  - Mye teknisk gjeld
- En test ender i mange tilfeller med full kompromittering

Men hva skjer etter en inntrengingstest?

- **Operativ bistand**
  - Et eget team bistår våre medlemmer etter endt test
  - Krever forankring i ledelsen og en forpliktelse ovenfor oss i Helse- og KommuneCERT
- **Hjelpe å utbedre funn, men også å utveksle kompetanse**
- **Vi ønsker at medlemmene skal sitte igjen med kunnskapen**



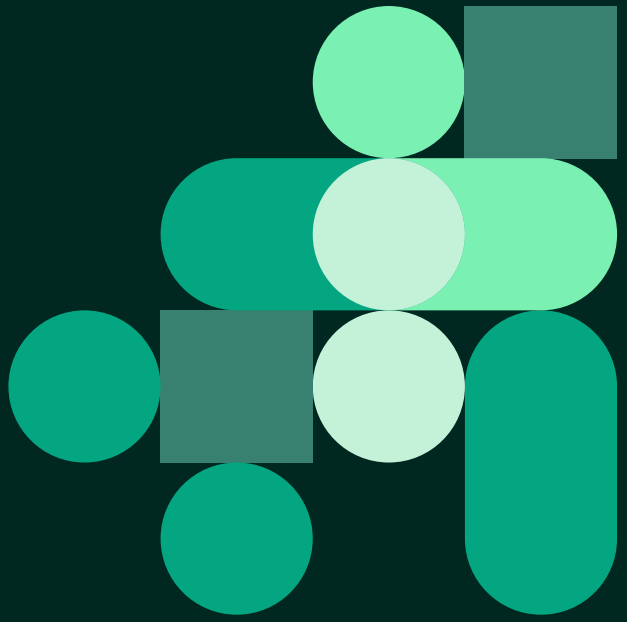
Positiv utvikling etter endt Kommunetest hos flere virksomheter

Positiv utvikling vedrørende herding

- Flere av de mest kritiske sårbarhetene blir tettet innen kort tid
- Angrepsflaten blir redusert

Kompetanseheving og bevisstgjøring

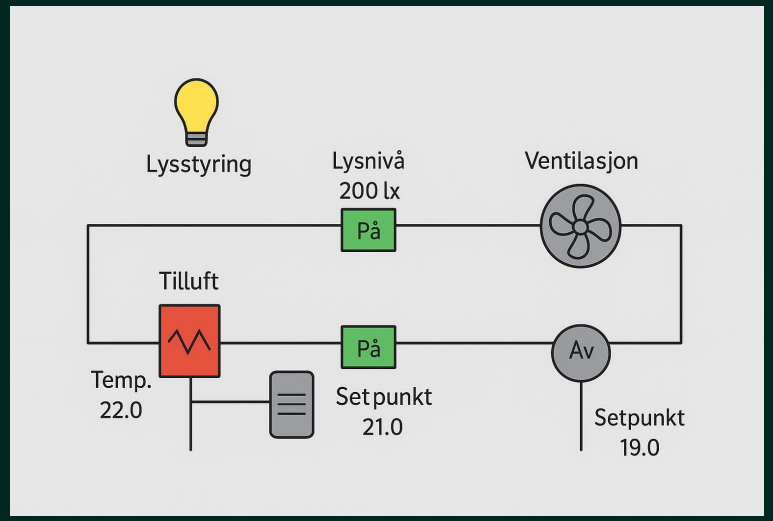
- Flere virksomheter lærer hvordan en angriper tenker
- Fremtidig sikkerhetsarbeid blir justert basert på testresultatene



Operasjonell Teknologi (OT)

Hovedforskjellene mellom IT og OT

- OT styrer fysiske enheter
  - Eksempler er motorer/pumper, dører, ventilasjon, varme...
  - Små fabrikker til kritisk infrastruktur (vann/avløp/strøm)

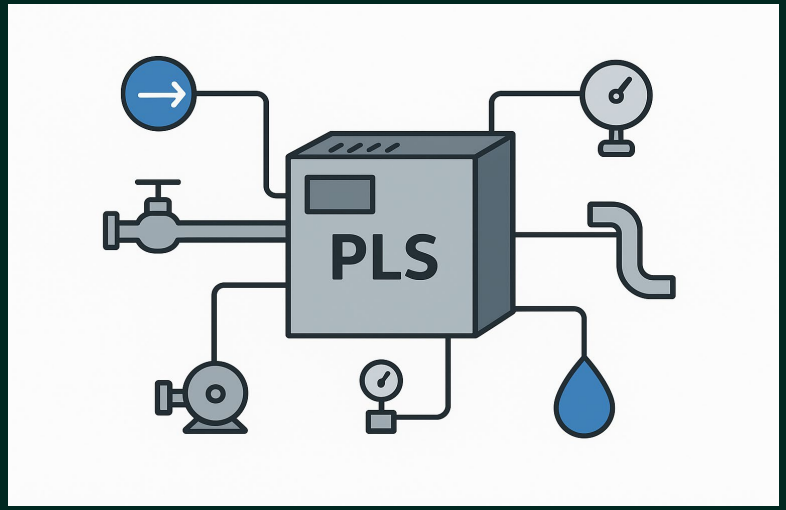


- Stort fokus på "Availability". Oppetid er alltid kritisk

- Ofte nøkkelferdige løsninger med begrenset kompetanse hos eier
  - I mange tilfeller tungt avhengig av leverandør(er)
- Standard sikkerhetsoppdateringer kan knekke anleggene
  - skreddersydde løsninger og programvare

Helse- og KommuneCERTs arbeid rundt OT/VA

- Sommeren 2025 jaktet vi etter eksponerte OT-systemer på internett
- Avdekket mange hundre OT-enheter, noen av disse tilhørende VA, men også kraftverk
- Noen var uten passord og andre benyttet seg av fabrikkpassord
- Ofte var ikke systemeier klar over eksponeringen da vi varslet
- Besøk på vannverk: Kritiske sårbarheter internt, og på internett.
- Kommunene er ofte ikke klar over tilstanden på anleggene, da leverandørene drifter og vedlikeholder det meste selv



Hvor involvert er du angående tredjepartsleverandører og deres sikkerhetsrutiner i ditt OT-anlegg?

Vaksinasjon – tiltak og forebyggende aktivitet

HVORDAN ØKE VÅR MOTSTANDSDYKTIGHET?

Anbefalinger

- Implementer phishingresistent autentisering på eksponerte tjenester
  - Spesielt viktig på M365
- Ha kontroll på angrepsflate. Hvilke systemer har du på internett?
- Ha oversikt over egne systemer og sørg for at de blir driftet.
- Gjennomfør grunnleggende sikkerhetsherding.
- Still krav til leverandører.

Norsk helsenett

Helse- og KommuneCERT

for helse- og kommunesektoren

post@helsecert.no