

# Sikkerhetskultur - nei, det har vi sluttet med

Hanne Tangen Nilsen,  
Sikkerhetsdirektør, Telenor Norge



# Samfunnets krav: Beskytt Norges digitale infrastruktur



5922.56 BUY +00.69 FUT  
8684.86 BUY +04.49 STK  
4283.23 BUY +01.58 FUT  
4121.06 BUY +07.02 STK  
8471.45 BUY +03.70 STK  
7518.78 BUY +05.26 STK  
1240.92 BUY +05.98 FUT  
6444.84 BUY +01.35 FUT  
3315.50 BUY +09.35 FUT

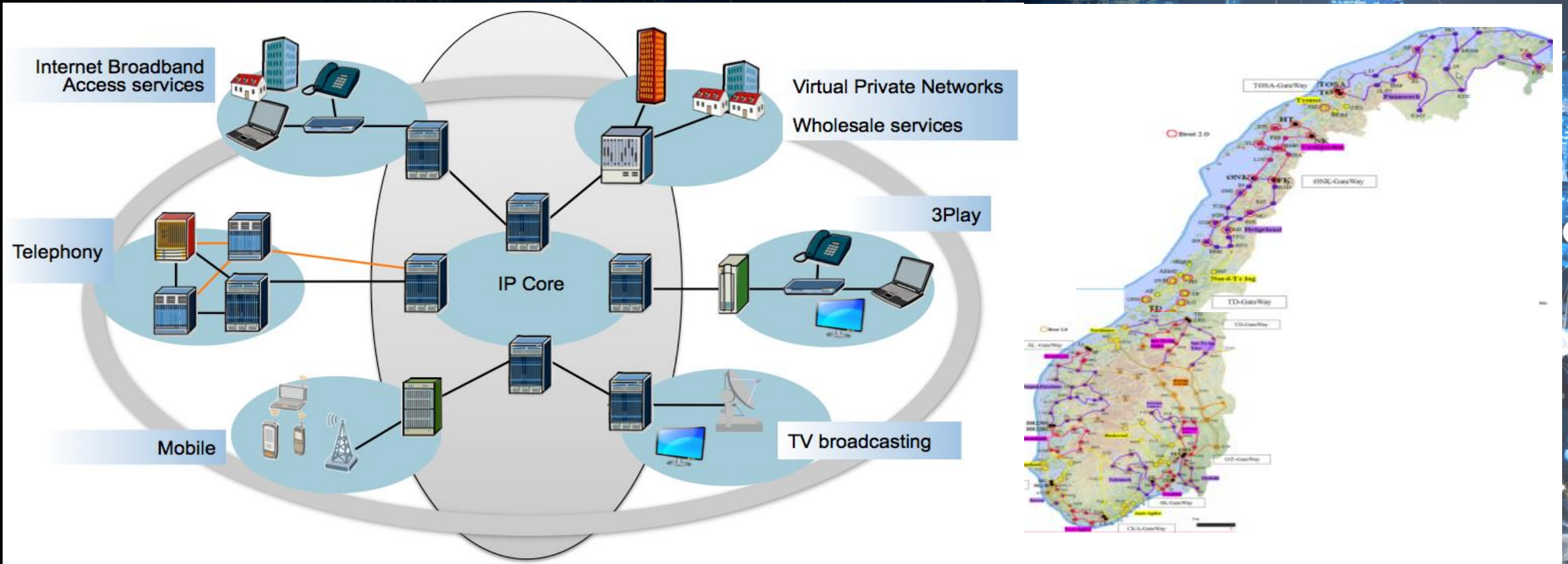


HOUSTON  
WE'VE  
HAD A  
PROBLEM  
HERE

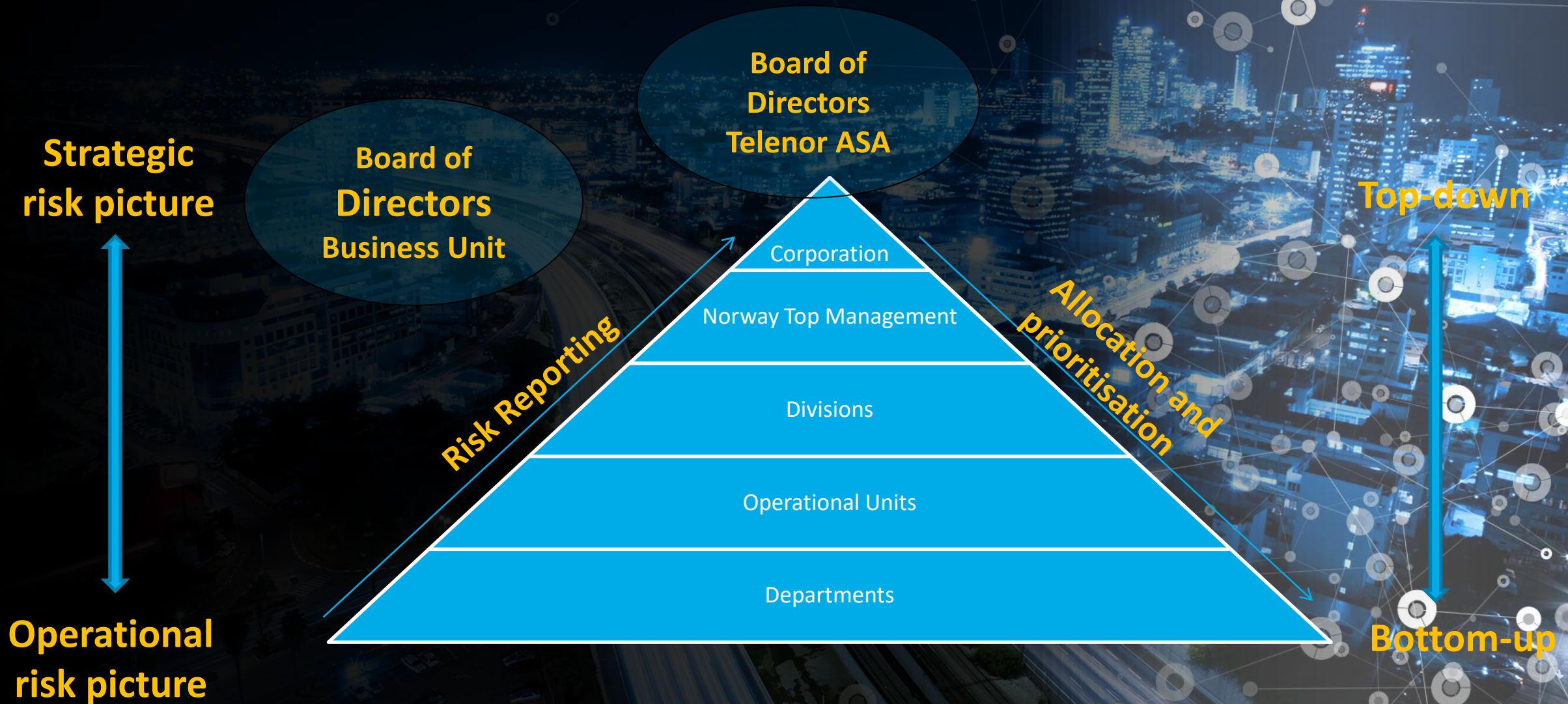
# En verden der alt er koblet på krever mer av oss



# Beskyttelse av alt som er sårbart via IKT



# Risikostyring og lederforankring



# Alt henger sammen med alt



Sårbarheter

Nye  
forretningsmodeller

Vårt digitale  
levesett

Trusselbildet

Telenor Norges  
sikkerhetsnivå

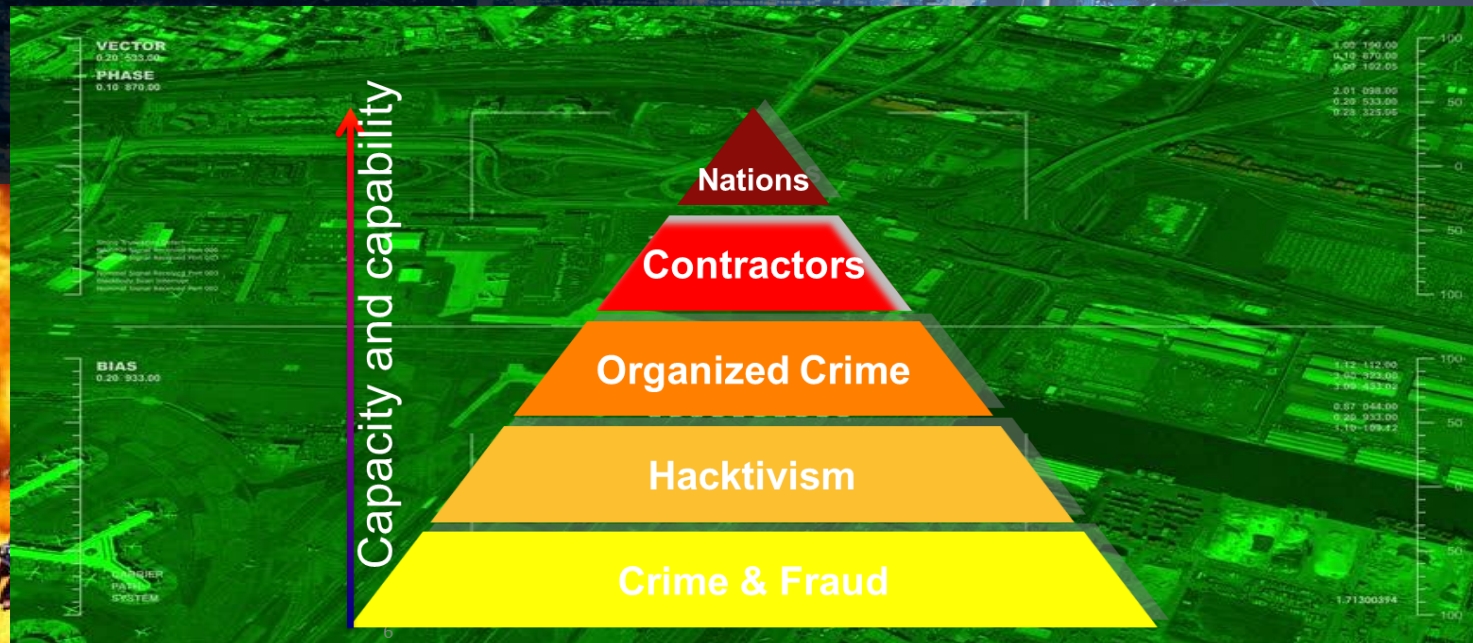
Regulering



# Vi måtte begynne å tenke det utenkelige



Tradisjonell sikkerhet



INTEL metodeverk for å forstå trusselaktører

# Generelt om trusselnivå

Telenor Norge er et mål for avanserte aktører, basert på myndighetenes trusselvurderinger og egen arbeid med trusselbildet erkjenner vi at:

- Cyberkrigføring pågår, og privat infrastruktur brukes til å utføre cyberkrigføring
- Telenor Norge vil bli forsøkt utnyttet av fremmed etterretning og utsatt for målrettet innhenting og offensive digitale operasjoner
- Avanserte aktører vil ønske å drive både fysisk og logisk innhenting av informasjon
- Forsøk på sosial manipulering og påvirkning av nøkkelpersonell vil fortsette
- Fremmed etterretning vil forsøke å misbruke tjenester
- Fremmed etterretning ønsker meget sannsynlig å benytte statssponsede organisasjoner og organiserte kriminelle miljøer, i tillegg til egen kapasitet, for å drive cyberoperasjoner mot Telenor Norge og enkelte av Telenor Norges kunder
- Det er sannsynlig at Telenor Norge kan bli utsatt for aktører som benytter løsepengevirus («ransomware»)

Trusselforståelse bruker vi som del av vårt arbeid med risk management for å beskytte totalforsvaret, nasjonale interesser, samfunnsinteresser og kunder.



# Ting som angriper Ting

- Vi har sett mennesker angripe ting og vi har sett ting angripe IT
- «Botnett mot botnett-krigen» viser hva som kan komme
- Det er svært sannsynlig at vi vil se ting-på-ting-angrep begått av nasjonalstater så vel som kriminelle
- Konsekvensene av cyberkriminalitet og cyberkonflikt vil bli annerledes, avhengig av om vi gjør ting rett eller bare «snubler inn» i online-samfunnet



# Forpliktelse ende til ende



# Kontinuitetssikring

Problem Management

Crisis Management

Incident Management

Driftsovervåkning

Reserve- / beredskapsutstyr

Ressursstyring

Design av nett og løsninger

Innovasjon +++

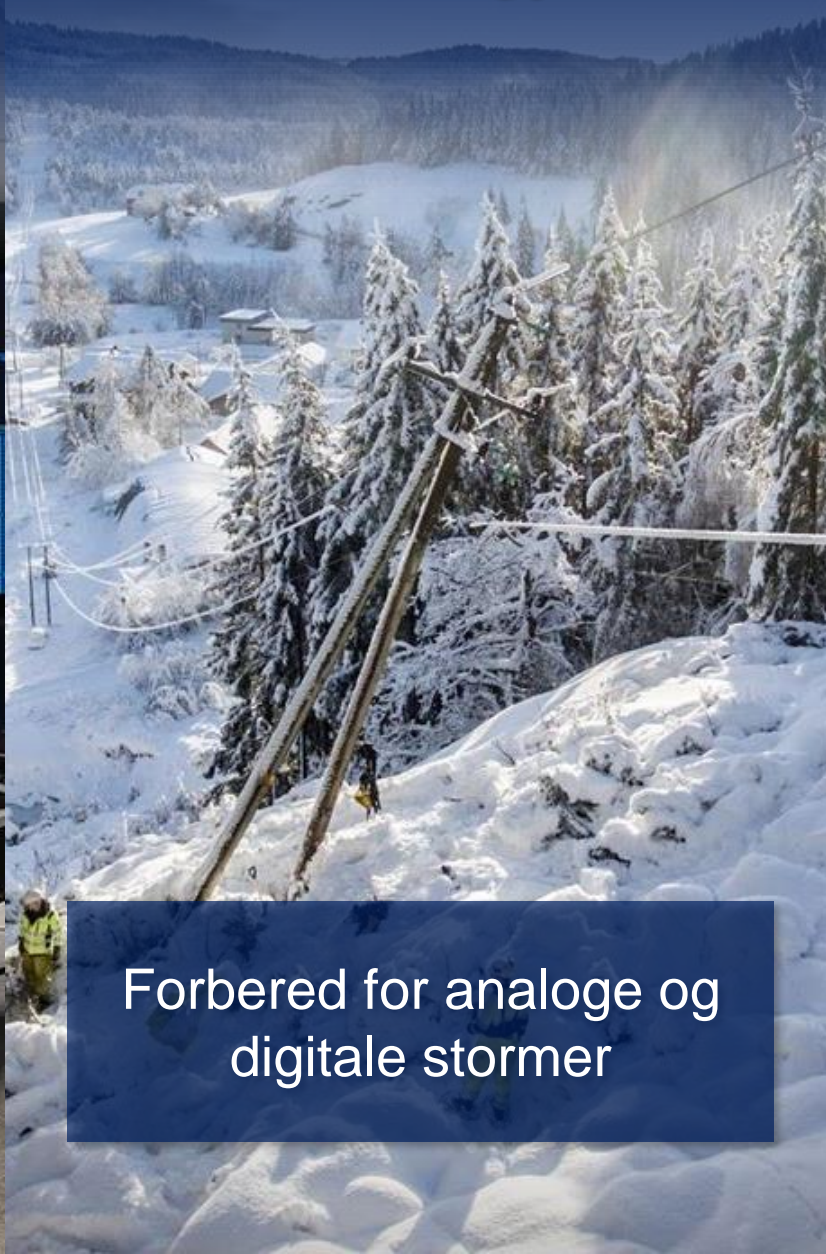
## Business Continuity:

«The ability of Telenor to Ensure continuity and availability of service and support for customers, partners and the general public interest before, during and after a Crisis.»

# Uansett; beredskapen avgjør når det smeller



Forutsi, detektér, håndter,  
normaliser, lær, repetér

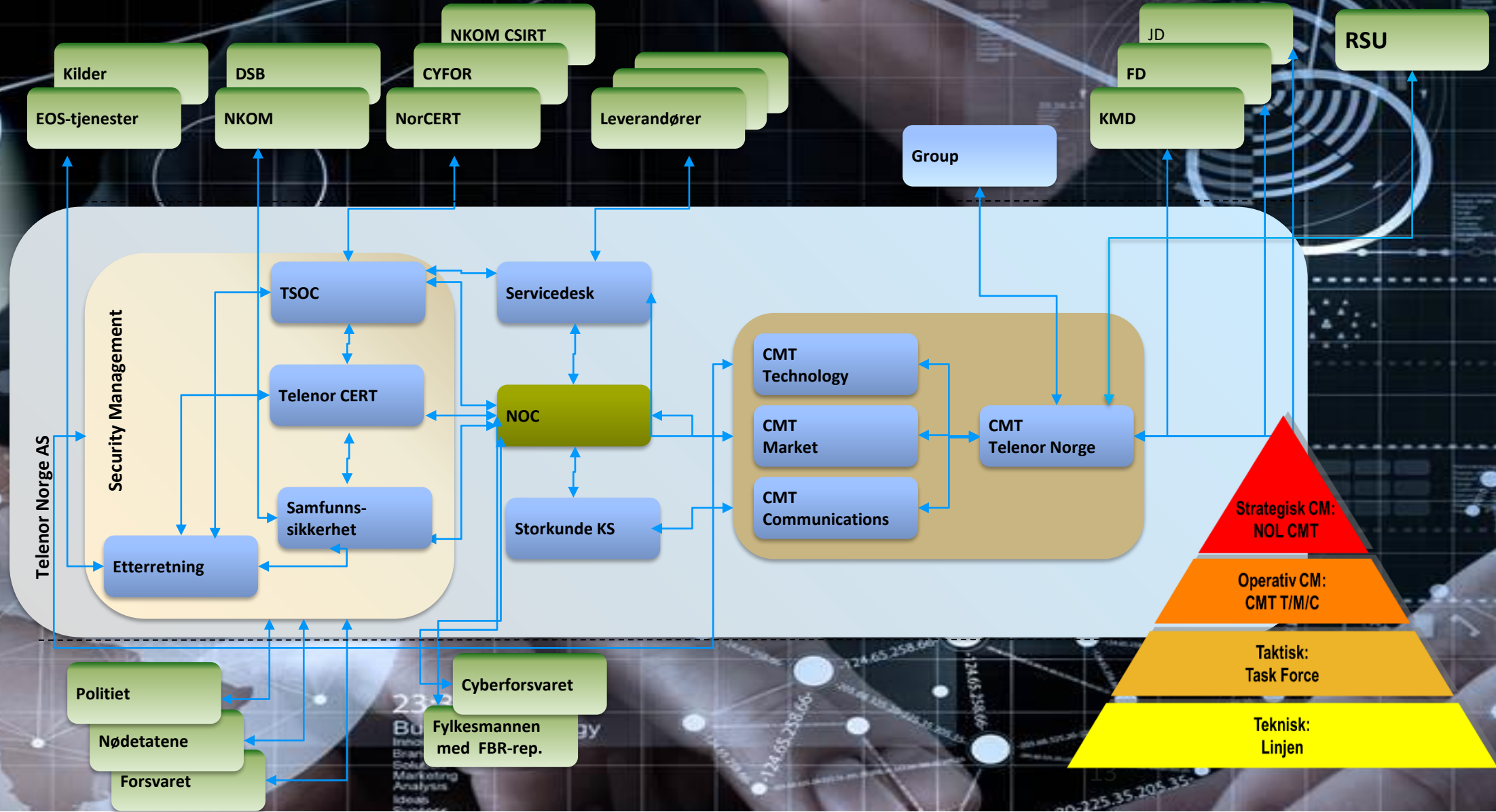


Forbered for analoge og  
digitale stormer



Tren organisasjonen på  
sosial manipulering

# Krise- og beredskapsorganisasjonen



# Øvelse for å teste organisasjonen



Utpressing og kidnapping

Teknisk hendelsehåndtering

Samfunnsrollen og  
Totalforsvaret

# Telenors minstekrav til alle ansatte

1. Forstå innholdet i [Taushets- og lojalitetserklæringen](#) og at den er en varig forpliktelse
2. Kunne benytte [Regler for beskyttelse av informasjon](#) riktig
3. Vær kjent med hvilke eiendeler som er underlagt ditt og din avdelings ansvarsområde
4. Forstå hvilke særskilte sikkerhetsbestemmelser som er knyttet til dine arbeidsoppgaver og inneha kompetanse til å etterleve disse
5. Vit at du finner Telenors sikkerhetskrav og hva som er relevant for din funksjon i [Sikkerhetshåndboken](#) og på [Security Sharepoint](#), og i eventuelle lokale bestemmelser utarbeidet for din funksjon
6. Vit at du melder brudd på sikkerhetsbestemmelser, sikkerhetshendelser eller sikkerhetsrelaterte tips og bekymringer til [security@telenor.no](mailto:security@telenor.no) - og er du i tvil spør du din nærmeste leder

## Utdrag fra Sikkerhetshåndboken:

Krav 3: «Du skal være kjent med hvilke eiendeler (informasjon inkludert) som er underlagt ditt og din avdelings ansvarsområde.» Eiendeler kan være informasjon, kunnskap, penger, systemer, hw/sw, arealer/bygg, kabler osv.

Krav 4: «Du skal forstå hvilke særskilte sikkerhetsbestemmelser som er knyttet til dine arbeidsoppgaver og inneha kompetanse til å etterleve disse.»

An aerial night view of a city, likely Dubai, featuring a complex highway interchange in the foreground. The city lights are visible in the background. A network of white lines and circular nodes is overlaid on the image, suggesting a digital or technological theme.

Takk for oppmerksomheten