«Security» i prosjektering

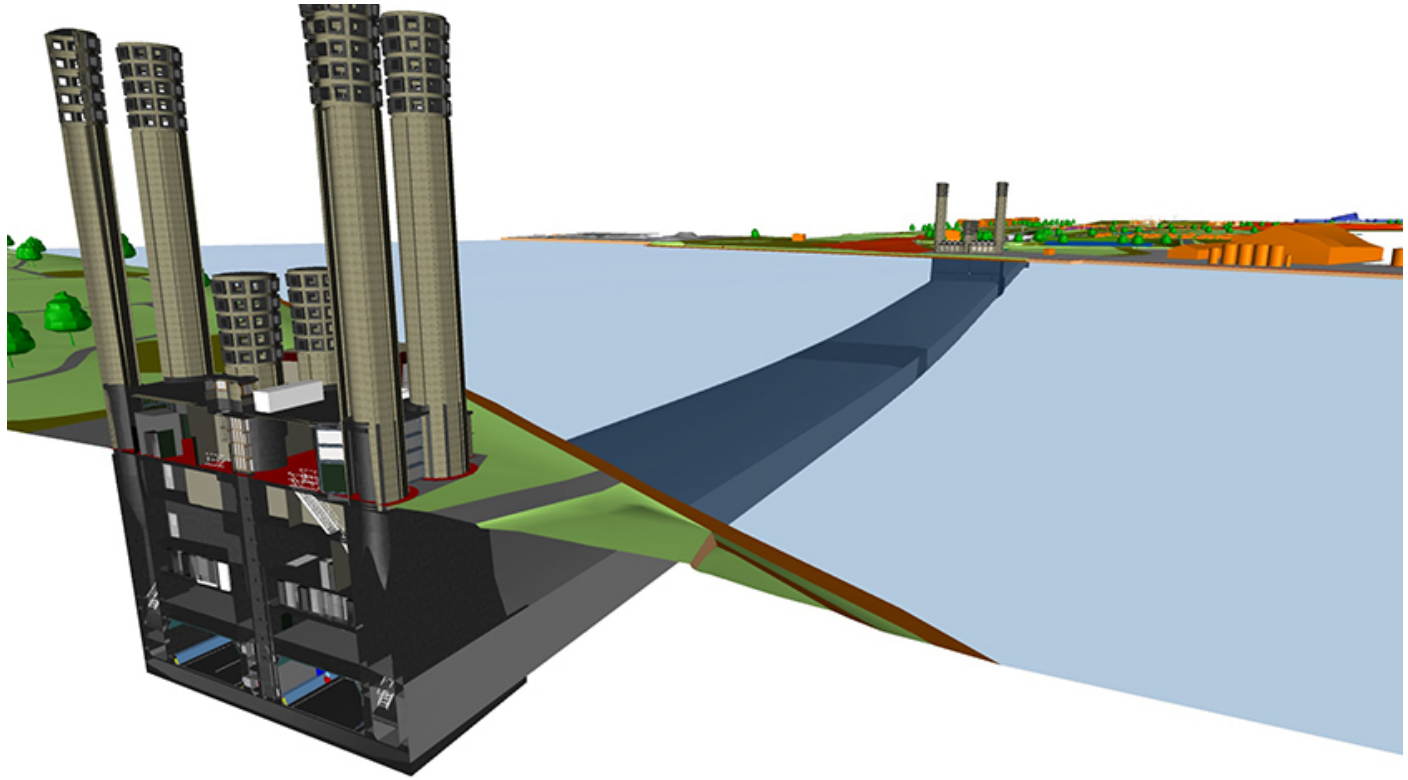
- 22 000 dataangrep mot norske bedrifter og offentlige etater (2016)

- Norge, et av verdens mest digitale land

  -> mer sårbare for angrep.

BIM - 3D

- Økende detaljnivå
- Bedre sammenstilling
- Bedre til å synliggjøre risiko
    - Identifisere svakheter
- Skytjenester
- Én modell- mange involverte



Cyberkrim - en gigantindustri

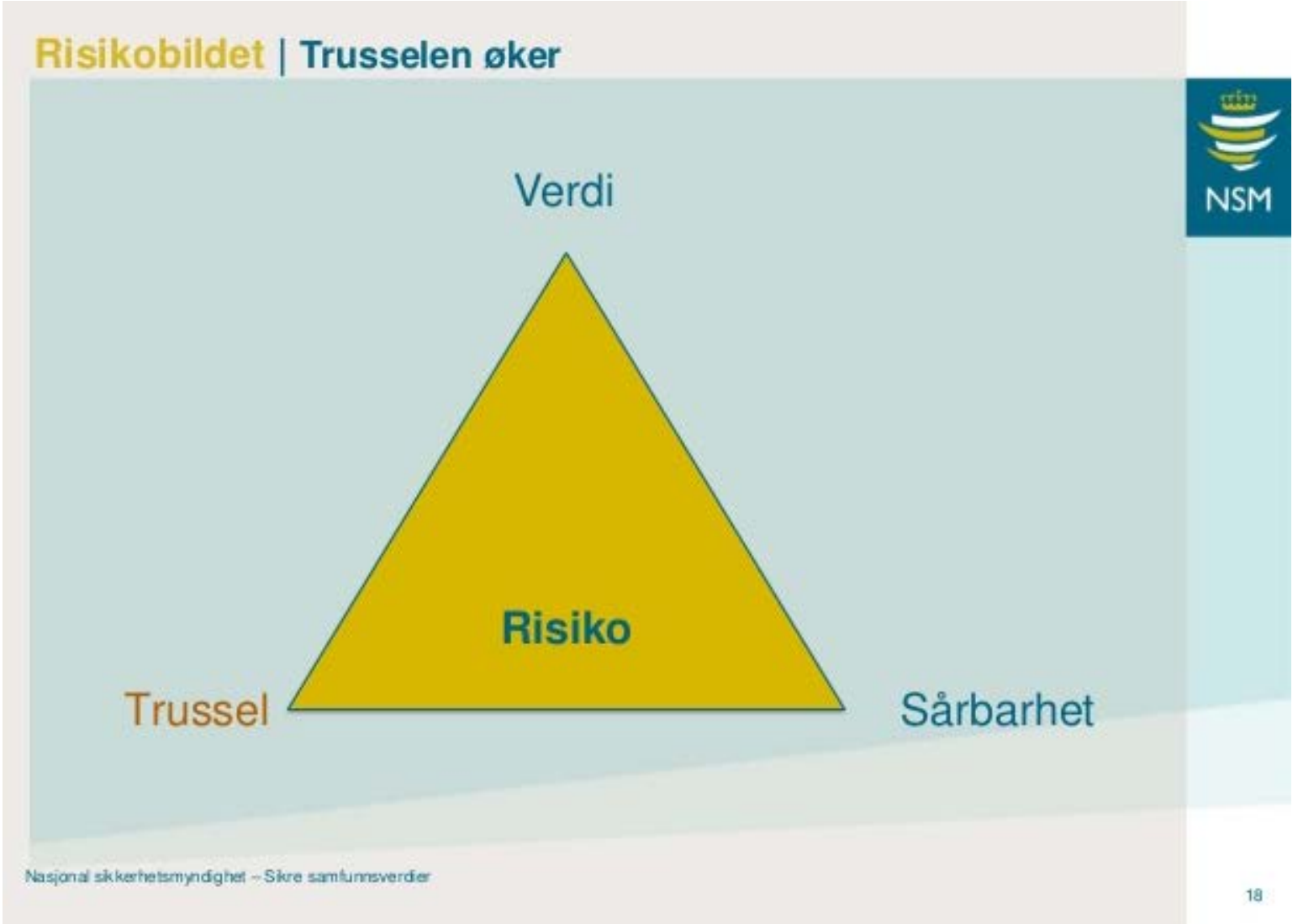
- EUROPOL beregner årlig tap til €290 milliarder i 2012
- Mer profitabel enn narkotikaindustrien

Utfordring med økende digitalisering, og bruk av BIM på ugradert nett.

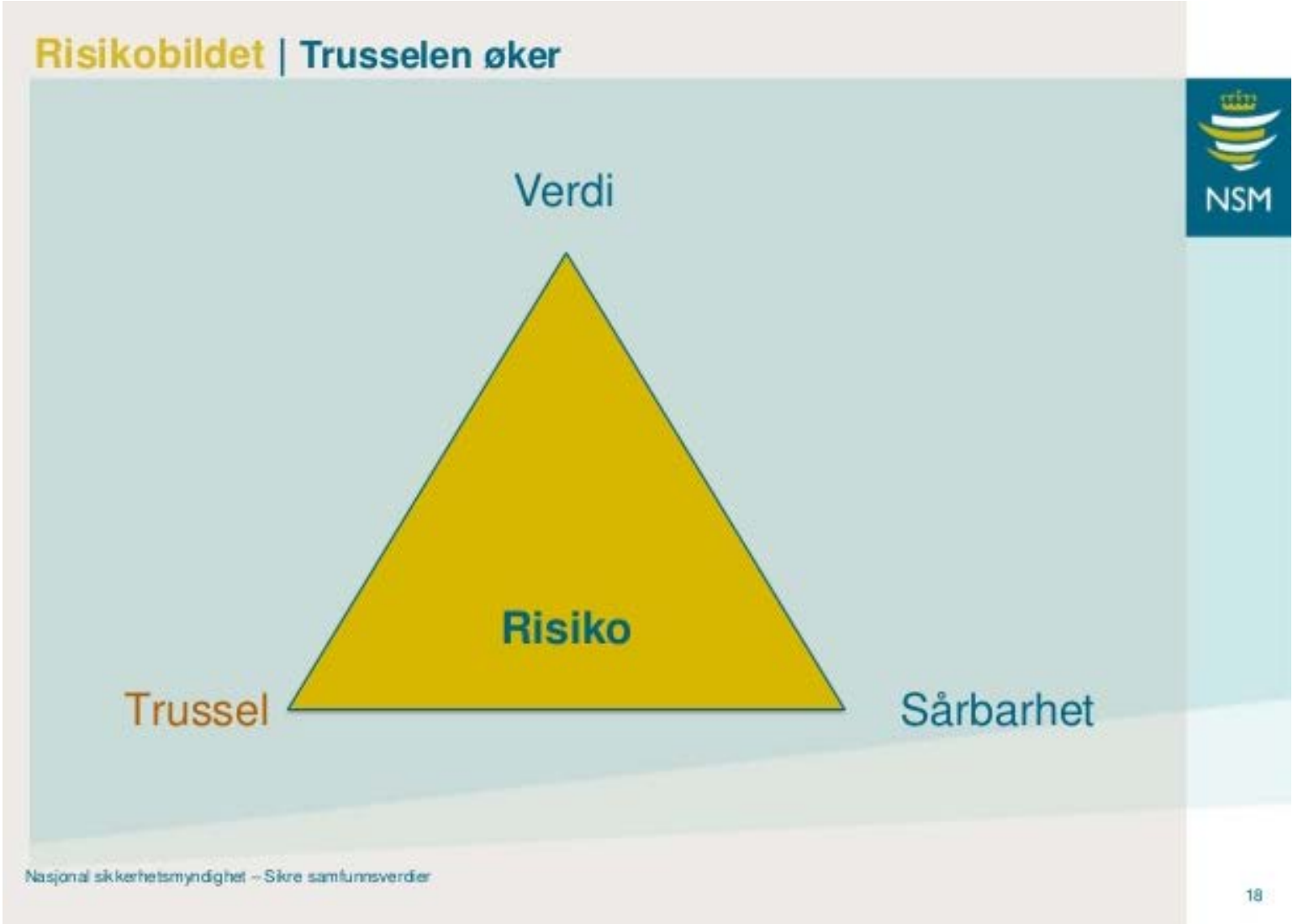
- Kan prosjektplaner brukes av konkurrenter?
- Vil kopier kunne selges?
- Vil noen ønske å manipulere dem?
- Vil noen kunne angripe modellene for så å kreve penger- Løspengevirus
- Relevant å frykte angrep og terror for å lamme infrastrukturen?

f.Eks store totalentrepriser

- Mange virksomheter undervurderer sine verdier
- Verdi er subjektivt
- Hva vil en hacker oppnå?

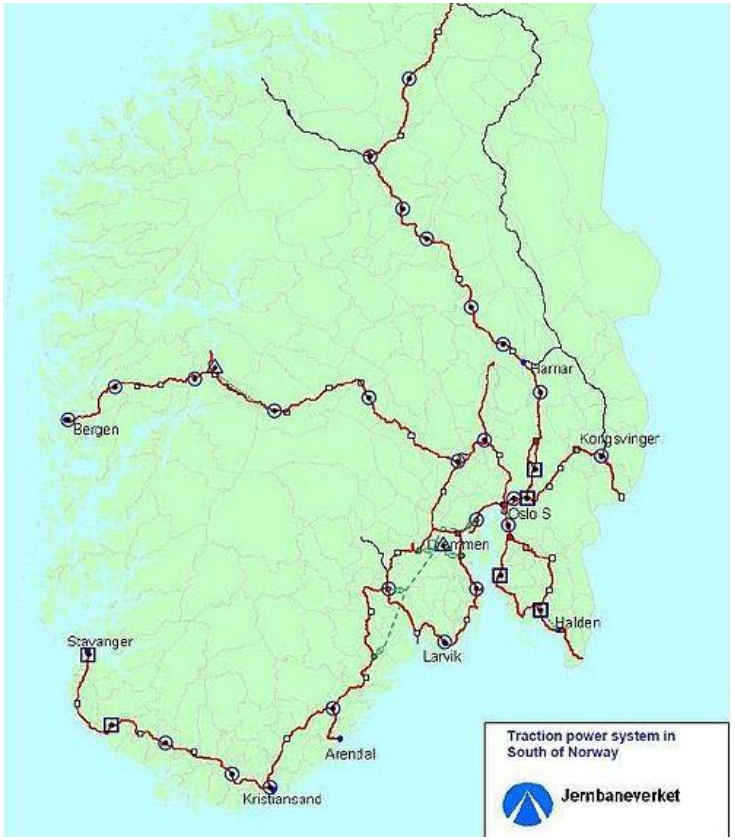


- Kost-nytte, hva er akseptabelt nivå for sårbarhet.



Jernbanen: en kritisk infrastruktur

- Stor utbredelse, distribuert kontroll
- Vanskelig å sikre fysisk
- Store konsekvenser ved bortfall
- Tap av menneskeliv, farlig gods
- Næringsliv kan rammes



Kraft: en kritisk infrastruktur

- Fundamentalt for alle andre systemer
- Norsk vannkraft viktig for Europa
- Økende global trussel fra hackere

Årsrapport Nasjonal sikkerhetsmyndighet

NSM registrerer et jevnt trykk av målrettede digitale spionasjeoperasjoner fra fremmede stater mot norske virksomheter.

Trusselaktørenes metoder er i stadig endring. Det utfordrer vår evne til å forebygge, oppdage og håndtere hendelser. Informasjonsoperasjonene i forbindelse med det amerikanske presidentvalget i 2016 viste at digital spionasje og nettverksoperasjoner kan sette demokratiske prosesser under press.

Større løsepengeviruskampanjer har fått store konsekvenser på verdensbasis i 2017, både for virksomheter og samfunnsfunksjoner. Vi forventer at slike angrepskampanjer vil fortsette og i enda større grad kunne treffe Norge, også med nye metoder som utnytter andre sårbarheter.

Årsrapport Nasjonal sikkerhetsmyndighet

NSM registrerer et jevnt trykk av målrettede digitale spionasjeoperasjoner fra fremmede stater mot norske virksomheter.

Trusselaktørenes metoder er i stadig endring. Det utfordrer vår evne til å forebygge, oppdage og håndtere hendelser. Informasjonsoperasjonene i forbindelse med det amerikanske presidentvalget i 2016 viste at digital spionasje og nettverksoperasjoner kan sette demokratiske prosesser under press.

Større løsepengeviruskampanjer har fått store konsekvenser på verdensbasis i 2017, både for virksomheter og samfunnsfunksjoner. Vi forventer at slike angrepskampanjer vil fortsette og i enda større grad kunne treffe Norge, også med nye metoder som utnytter andre sårbarheter.

Nettverksoperasjoner med formål å forstyrre eller gjøre informasjon og tjenester utilgjengelig, er forventet å vedvare i tiden fremover.

Årsrapport Nasjonal sikkerhetsmyndighet

NSM registrerer et jevnt trykk av målrettede digitale spionasjeoperasjoner fra fremmede stater mot norske virksomheter.

Trusselaktørenes metoder er i stadig endring. Det utfordrer vår evne til å forebygge, oppdage og håndtere hendelser. Informasjonsoperasjonene i forbindelse med det amerikanske presidentvalget i 2016 viste at digital spionasje og nettverksopera-sjoner kan sette demokratiske prosesser under press.

Nettverksoperasjoner med formål å forstyrre eller gjøre informasjon og tjenester utilgjengelig, er forventet å vedvare i tiden fremover.

– Når det gjelder dataangrep spenner aktørene fra fremmed etterretning, kriminelle organisasjoner, til vanlige hackere. Det er ingen tvil om at fremmed etterretning utgjør den største og mest alvorlige trusseler

Årsrapport Nasjonal sikkerhetsmyndighet

NSM registrerer et jevnt trykk av målrettede digitale spionasjeoperasjoner fra fremmede stater mot norske virksomheter.

Trusselaktørenes metoder er i stadig endring. Det utfordrer vår evne til å forebygge, oppdage og håndtere hendelser. Informasjonsoperasjonene i forbindelse med det amerikanske presidentvalget i 2016 viste at digital spionasje og nettverksoperasjoner kan sette demokratiske prosesser under press.

Større løsepengeviruskampanjer har fått store konsekvenser på verdensbasis i 2017, både for virksomheter og samfunnsfunksjoner. Vi forventer at slike angrepskampanjer vil fortsette og i enda større grad kunne treffe Norge, også med nye metoder som utnytter andre sårbarheter.

Nettverksoperasjoner med formål å forstyrre eller gjøre informasjon og tjenester utilgjengelig, er forventet å vedvare i tiden fremover.

– Når det gjelder dataangrep spenner aktørene fra fremmed etterretning, kriminelle organisasjoner, til vanlige hackere. Det er ingen tvil om at fremmed etterretning utgjør den største og mest alvorlige trusseler

Vi erfarer et jevnt trykk av målrettede digitale spionasjeoperasjoner fra statlige aktører mot norske offentlige og private virksomheter. Spionasje mot høyteknologi, forsvarsinteresser, virksomheter knyttet til kritisk infrastruktur så vel som nettverksoperasjoner mot politiske, økonomiske og militære mål, vedvarer også i 2017.[2]

Årsrapport Nasjonal sikkerhetsmyndighet

NSM registrerer et jevnt trykk av målrettede digitale spionasjeoperasjoner fra fremmede stater mot norske virksomheter.

Trusselaktørenes metoder er i stadig endring. Det utfordrer vår evne til å forebygge, oppdage og håndtere hendelser. Informasjonsoperasjonene i forbindelse med det amerikanske presidentvalget i 2016 viste at digital spionasje og nettverksoperasjoner kan sette demokratiske prosesser under press.

Større løsepengeviruskampanjer har fått store konsekvenser på verdensbasis i 2017, både for virksomheter og samfunnsfunksjoner. Vi forventer at slike angrepskampanjer vil fortsette og i enda større grad kunne treffe Norge, også med nye metoder som utnytter andre sårbarheter.

Nettverksoperasjoner med formål å forstyrre eller gjøre informasjon og tjenester utilgjengelig, er forventet å vedvare i tiden fremover.

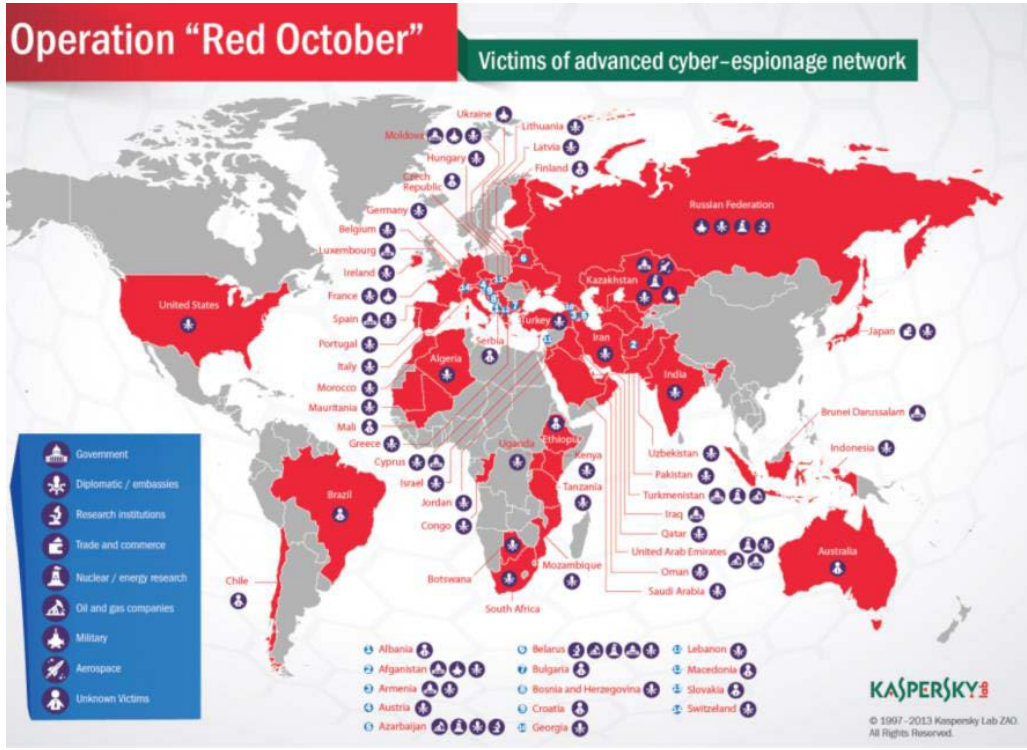
– Når det gjelder dataangrep spenner aktørene fra fremmed etterretning, kriminelle organisasjoner, til vanlige hackere. Det er ingen tvil om at fremmed etterretning utgjør den største og mest alvorlige trusseler

Vi erfarer et jevnt trykk av målrettede digitale spionasjeoperasjoner fra statlige aktører mot norske offentlige og private virksomheter. Spionasje mot høyteknologi, forsvarsinteresser, virksomheter knyttet til kritisk infrastruktur så vel som nettverksoperasjoner mot politiske, økonomiske og militære mål, vedvarer også i 2017.[2]

Når vi i tillegg ser at trusselaktørene utvikler sine metoder raskere enn vi utvikler og tar i bruk mottiltak, vurderer NSM at risikobildet forverres og forventer at samfunnskonsekvensene av IKT-hendelser vil øke.

PST sin sikkerhetsvurdering

- Norge og norske interesser vil i 2017 utsettes for fremmed etterretningsvirksomhet som kan ha et stort skadepotensial. Aktiviteter vil blant annet rettes mot mål innenfor kritisk infrastruktur. Fremmede tjenester bruker både avanserte datanettverksoperasjoner og tradisjonelle metoder mot norske mål.



PST sin sikkerhetsvurdering

- Norge og norske interesser vil i 2017 utsettes for fremmed etterretningsvirksomhet som kan ha et stort skadepotensial. Aktiviteter vil blant annet rettes mot mål innenfor kritisk infrastruktur. Fremmede tjenester bruker både avanserte datanettverksoperasjoner og tradisjonelle metoder mot norske mål.

- Russiske og kinesiske aktører har forsøkt å kompromittere datasystemer hos virksomheter som forvalter grunnleggende nasjonale verdier og store kommersielle interesser. Det vil bli gjennomført avanserte datanettverksoperasjoner mot aktører med ansvar for kritisk infrastruktur også i 2017.

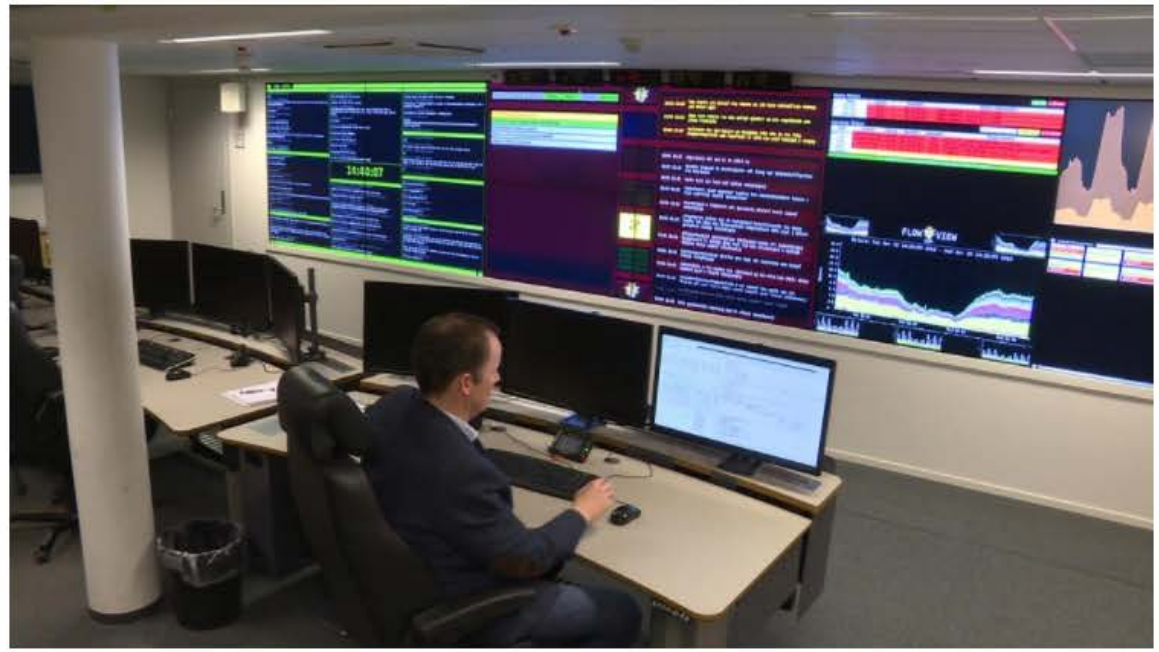
- Flere stater har etterretningspersonell i Norge. Mange opererer under diplomatisk dekke ved ambassader og konsulater.

Etterretning

- Informasjon og kunnskap tilegnet gjennom
    - Observasjon,
    - Innsamling
    - Analyse
    - Evaluering

Dataangrep er lederes største bekymring

Norske ledere frykter dataangrep mer enn konjunkturnedgang eller finanskrise, ifølge en ny undersøkelse.



Fra operasjonsrommet hos Nasjonal Sikkerhestmyndighet, NSM, overvåkes dataangrepene mot Norge.
FOTO: TORMOD STRAND / NRK

Kilde: **NTB**

Publisert i dag, for 11 timer siden

Samtidig som at frykten for dataangrep er størst, oppgir hver fjerde virksomhet at de ikke er godt nok sikret mot dette, skriver Finansavisen. Det er revisjons- og rådgivningsselskapet BDO som har gjennomført en undersøkelse blant 1.500 norske ledere i offentlig og privat sektor.

Løsepengeviruset i juli: Danske Moller-Maersk kan ha tapt milliarder på dataangrep

NTB
OPPDATERT: 16.AUG.2017 14:59 | PUBLISERT: 16.AUG.2017 14:59

FOTO: KACPER PEMPEL / X02307

Vann- og avløpssystemet i Oslo var dårlig beskyttet mot et terrorangrep, ifølge VG. Her fra Oslos største renseanlegg Oset. FOTO: MORTEN HOLM/SCANPIX
FOTO: Holm, Morten

Passordet 0-0-0-0 kunne fram til i vår ha gitt terrorister full kontroll over vann- og avløpssystemet i Oslo kommune. En rapport fant så mange sikkerhetshull at den ble hemmeligstemplet.

I rapporten avsløres det at terrorister med en vanlig mobil og det lette passordet kunne overta kontrollen over vannforsyningen i Oslo og fysisk ha kommet seg inn på vannrenseanleggene for å forgifte, stoppe og sabotere drikkevannet til 600.000 mennesker,

Tilsynet varslet Bane Nor: – Al-Qaida oppfordrer til terror mot tog og T-bane

NTB

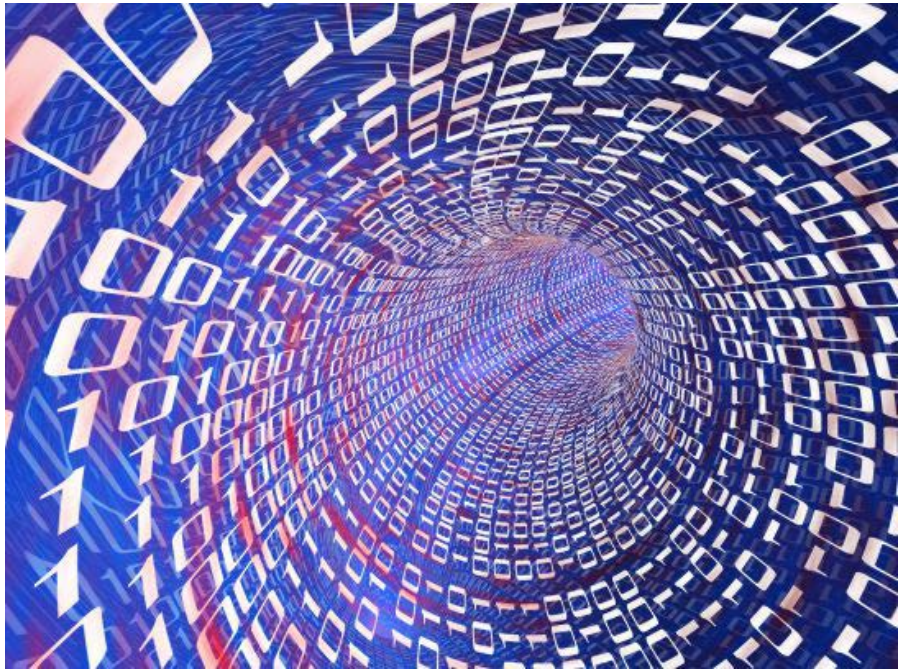
OPPDATERT: 20.AUG.2017 21:23 | PUBLISERT: 20.AUG.2017 21:23

Cyberangrep er komplisert og ressurskrevende. Enklere med fysiske angrep.

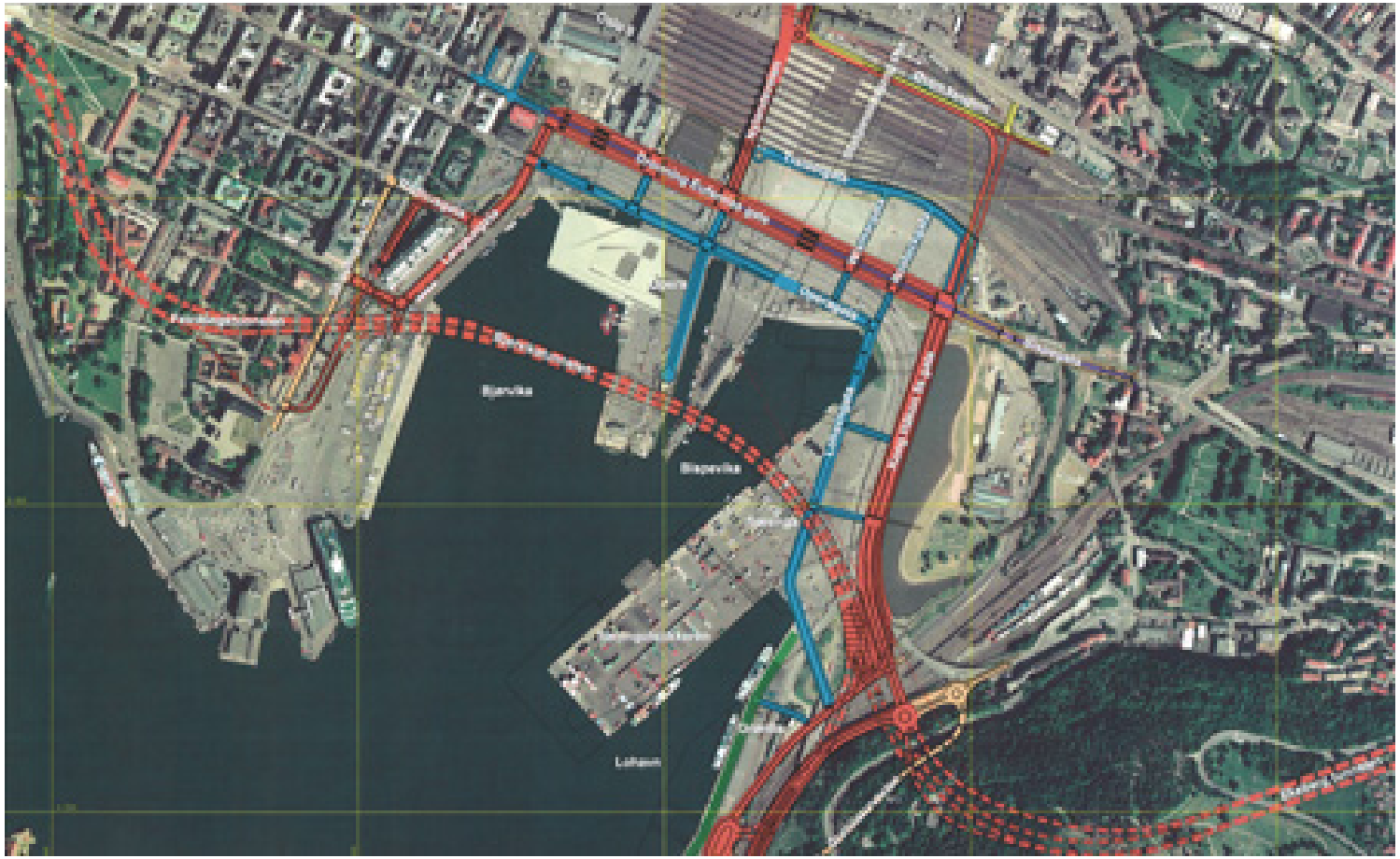
Niklas Vilhelm, NSM

Ifølge finske Etlatieto har Norge nå passert Finland og er det mest digitaliserte landet i verden. Digi-

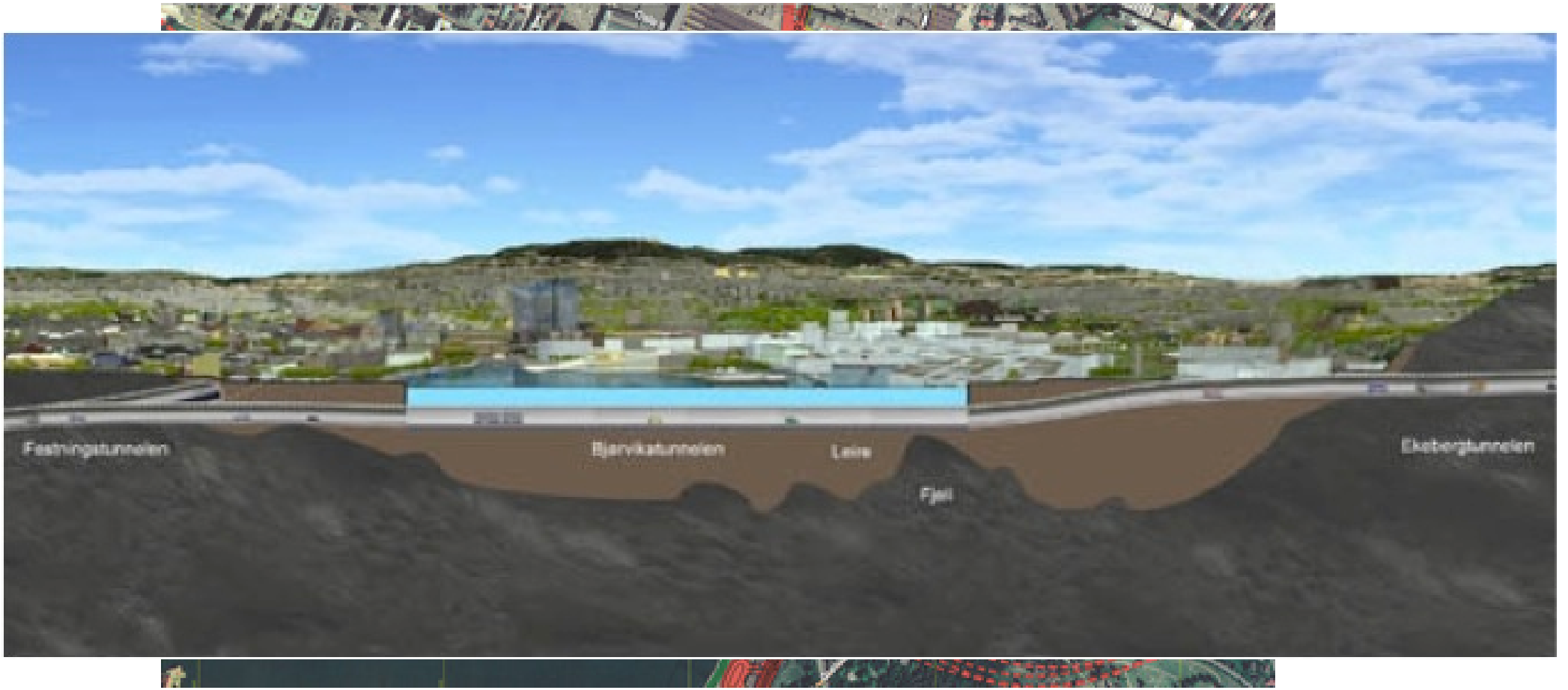
Papirarkiv sikrere enn datarkiv?



Kan en BIM modell av Operatunnelen i feil hender gjøre stor skade?



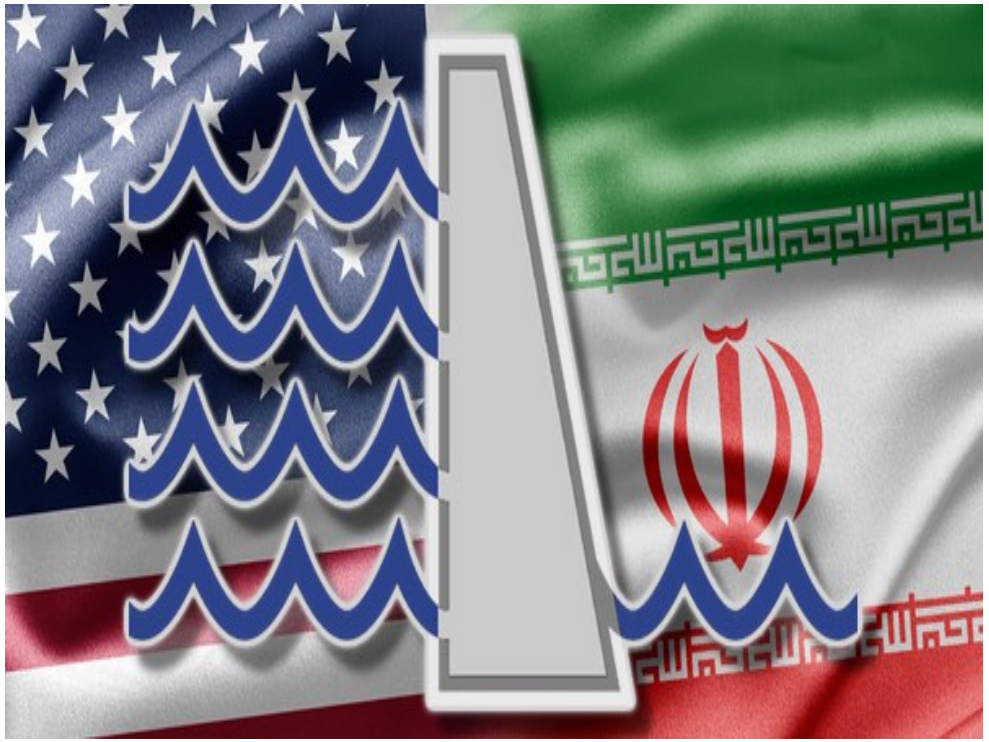
Kan en BIM modell av Operatunnelen i feil hender gjøre stor skade?



Svakhet i konstruksjoner

USA:

Iranske hackere trodde de hadde hacket et stort dam-anlegg i USA. Det viste seg at dammen var knøttliten, men hadde et lignende navn. De kunne sikkert hatt bruk for litt bedre arbeidstegninger, dammen de trodde de hacket har ikke et digitalt styringssystem



Takk for meg


Q:
WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?
YO! DUDE... BACK HERE
CYBER SECURITY