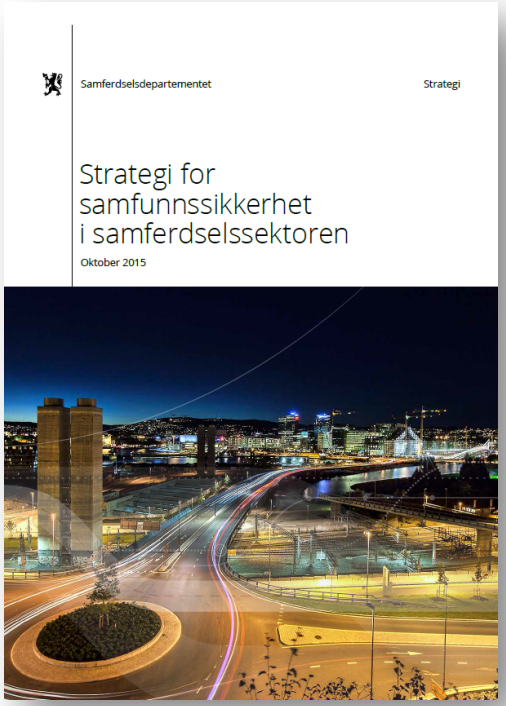
Nasjonal kommunikasjons-myndighet

EkomROS 2016

Alexander Iversen
sjefingeniør

CIO Forum Sikkerhet 28. april 2016

Risiko og sårbarheit i ekomsektoren

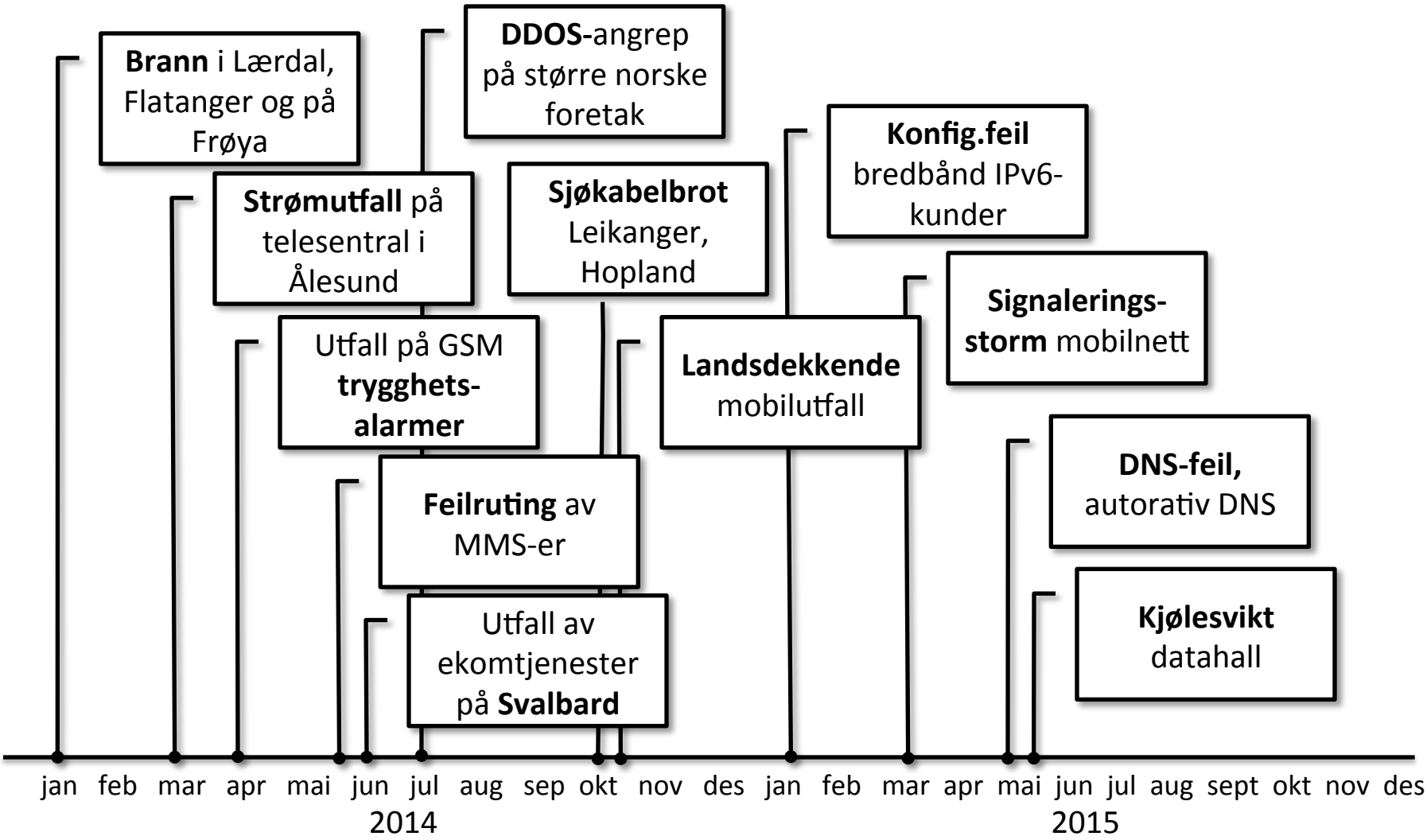


- Arbeide systematisk, målretta og sporbart med samfunnssikkerheit
- Oversikt over risiko og sårbarheit innan eiget ansvarsområde
- Sett i verk førebyggande tiltak og beredskapstiltak på bakgrunn av eit godt utgreia kunnskapsgrunnlag

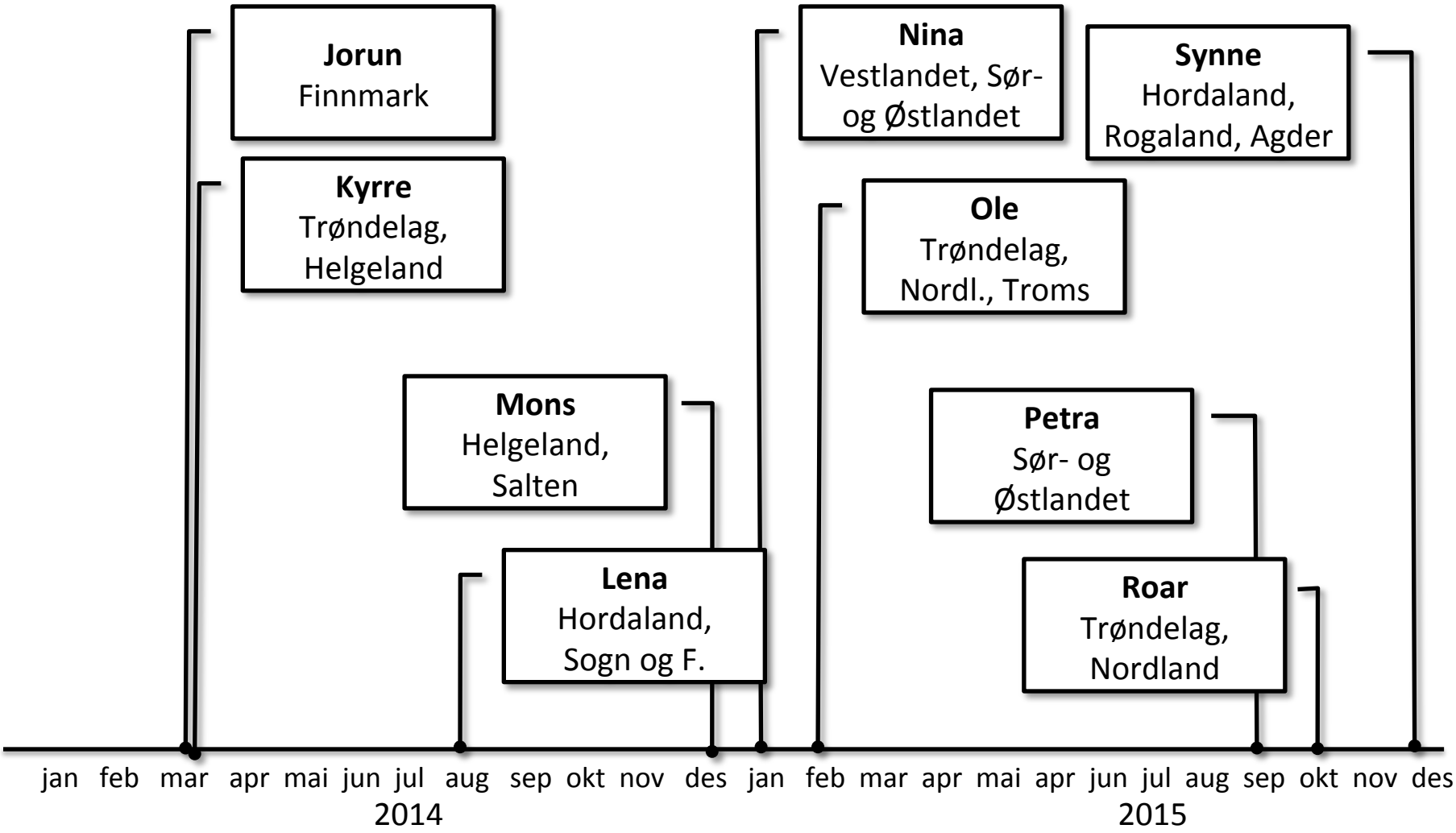
EkomROS:
Overordna risikoanalyse av sektoren

2014 og 2015

2014 og 2015 – utvalg av hendingar i Noreg



2014 og 2015 – ekstremvêr



2014 og 2015 – «bugged, tracked, hacked»

PÅ SPORET AV DN. Den tyske hackeren Karsten Nohl kunne følge DNs bevegelser i Oslo med utgangspunkt i mobilnummeret. DN testet ut overvåkningsmetoden som nå selges kommersielt, i en måned.

Magasinet Teknologi

Sirklet inn fra utlandet

Nå kan hackere finne ut eksakt hvor du er til enhver tid, fra et hvilket som helst sted i verden, bare ved å kjenne mobilnummeret. Og du kan ikke gjøre noe med det. DN testet ut den nye overvåkningsmetoden – som allerede er til salgss

Gemalto ble trolig hacket i 2010 og 2011 av NSA og britiske Government Communications Headquarters (GCHQ), men ifølge selskapet klarte ikke de to statlige etterretningsorganisasjonene å hente ut verdifull informasjon. (Ill.: Simon Yeo/Flickr)

Gemalto: – NSA klarte ikke å stjele SIM-nøklene

Av Trond Bie, 25. februar 2015 kl 08:59

Hevder at de uansett ikke kan spionere på 3G og 4G-nett.

SIKKERHETSHULL: Det er avdekket sikkerhetshull i det svenske og danske telenettet til Telenor og Telia.

Lekker ditt mobilnummer når du surfer

Stortinget og statsministeren

OVERVÅKES

Utenfor Stortinget, regjeringskontorene og boligen til statsminister Erna Solberg befinner det seg avansert spionutstyr som kan overvåke alle mobiltelefoner i området. Spørsmålet er: Hvem står bak?

2016-2020?

Viktige utviklingstrekk (1)

Teknologi

- Felles IP-basert sambandsinfrastruktur
- VoLTE
- Network function virtualization
- Over-the-top (OTT) tenester

Organisasjon

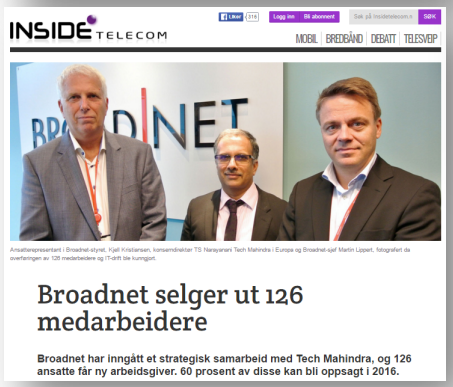
- Utkontraktering
- Internasjonalisering
- Managed services


INSIDE TELECOM

MOBIL | BREDBÅND | DEBATT | TELESVEIP

Ice bygger telenett med vanlige servere

Da mobiloperatøren Ice måtte øke kapasiteten i nettet valgte de standardservere heller enn tradisjonelle teleservere – til halve prisen.


INSIDE TELECOM

MOBIL | BREDBÅND | DEBATT | TELESVEIP

Broadnet selger ut 126 medarbeidere

Broadnet har inngått et strategisk samarbeid med Tech Mahindra, og 126 ansatte får ny arbeidsgiver. 60 prosent av disse kan bli oppsagt i 2016.

Viktige utviklingstrekk (2)

Brukarane

- Mobile tenester
- Samfunnskritiske brukarar
- Internet of Things

Analysen

Datagrunnlag

.....

Resultat frå tilsyn

Nkoms utgreiingar om falske basestasjonar, SS7, nasjonal autonomi,…

Nordisk NIS-samarbeidet

ENISA trendrapportar

Hendingsrapportar, ENISA, NSM, ekomtilbydarane

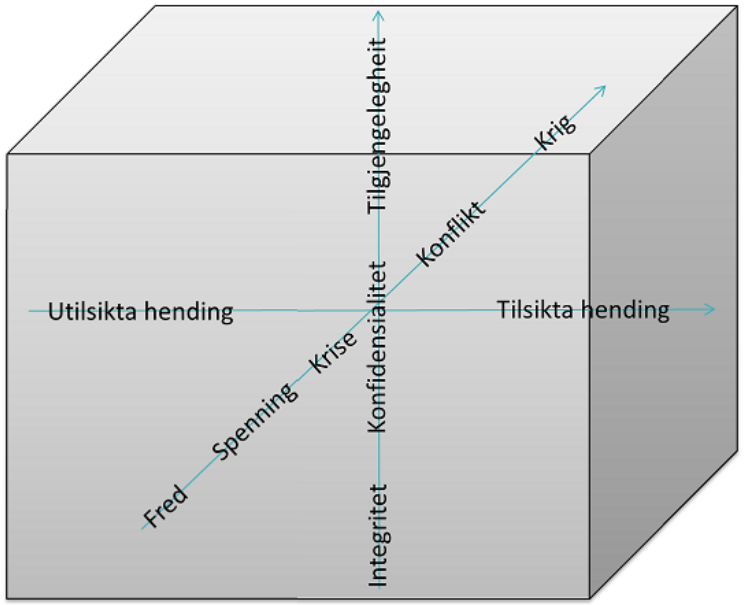
Trusselvurderingar NSM, PST, E-tenesten

Nkoms topologi-kartlegging

Nasjonalt risikobilete, DSB

Metodisk tilnærming

- Definere mulegheitsrommet
- Grovanalyse (identifisere risikoområder)
- Analyse av potensielle uønskte hendingar
- Identifisere tiltak



Grovanalyse: Identifiserte risikoområde

Den nasjonal sambandsinfrastrukturen og sentraliseringa av tenesteproduksjon fører til at enkeltfeil kan få store konsekvensar

Kompleks verdikjede og omfattande utstyrsportefølje gjer det vanskeleg å kjenne heile sårbarheitsbiletet, aukar avhenga til leverandørane

Utkontraktering og internasjonalisering utfordrar kompetanse, ansvar, læring, og kontroll på nye måtar

Risiko for potensielle uønskte hendingar

ID	Uønsket hendelse	Risiko	Usikkerhet
H2	Konfigurasjonsfeil i landsdekkende IP-nett	Moderat/høy	Høy
H3	Utpressing av nøkkelressurs – sabotasje transportnett	Moderat/høy	Høy
H8	Utpressingsforsøk mot ISP - skadevare	Moderat/høy	Høy
H12	Kartlegging av norsk kritisk infrastruktur	Moderat/høy	Høy
H1	Multippel transmisjonsfeil i transportnett	Moderat	Høy
H4	Fiberbrudd Svalbard og Finnmark	Moderat	Moderat
H5	Strømsvikt på kritiske anlegg i Oslo	Moderat	Moderat
H6	Signaleringsstorm i landsdekkende mobilnett	Moderat	Lav
H7	Sikkerhetshull i VoLTE	Moderat	Høy
H13	Ressursproblemer - entreprenør	Moderat	Høy
H14	Ressursproblemer - leverandør	Moderat	Moderat
H15	Overvåkning via nett i utlandet	Moderat	Høy
H9	DNS-angrep	Lav/moderat	Lav
H10	Kompromittering av sertifikatutsteder	Lav/moderat	Lav
H11	Bortfall av GPS	Lav/moderat	Lav

Høgst risiko: Kartlegging av/etterretning mot kritisk ekominfrastruktur (H12)

Mål

- Kartlegging av/etterretning mot kritisk personell
- Kartlegging av/etterretning mot kritisk ekominfrastruktur

Dette bidrar til risikoen

- Kritisk infrastruktur: høgverdig mål for utanlandsk etterretning
- Aktørar har evne og vilje til (avansert) kartlegging
- Vanskeleg å oppdage, m.a. p.g.a. utkontraktering og internasjonalisering
- Vanskeleg å oppdage; får lett mindre merksemd
- Kan utnyttast til å «lamme» samfunnet i ein konflikt-/ krigssituasjon


– For lett å hente ut informasjon fra Norge

NTB

OPPDATERT: 10.FEB. 2016 06:23 | PUBLISERT: 10.FEB. 2016 06:23

FOTO: Berntsen, Terje

Justisminister Anders Anundsen mener at nordmenn, norske bedrifter og offentlige organer er ekstremt dårlige til å beskytte seg mot utenlandsk spionasje. – Vi må skjerpe oss, sier han.

Høgst risiko: Logiske feil i transportnett og kjernenett (H2, H3, H8)

Dette kan utløyse feilen

- Utilsikta hending (konfigurasjonsfeil, programvarefeil etc.)
- Tilsikta hending (utpressing, sabotasje, etc.)

Dette bidrar til risikoen

- Systemkompleksitet skjuler logiske sårbarheiter
- Logiske feil går «på tvers» av den fysiske redundansen
- Kan løysast ut av ein enkelt programvarefeil, eller enkeltperson
- Avhengig av mange ressursar (interne/eksterne) for feilsøking
- Berar av store samfunnsverdiar

Tiltak

Risikoreduserende tiltak

	Tiltak	Risikoreduserende effekt														
		H 2	H 3	H 8	H 12	H 1	H 4	H 5	H 6	H 7	H 9	H 14	H 15	H 10	H 11	H 13
T1	Redundans og swapping					X	X									X
T2	Risikovurderinger og tiltak - planlagt arbeid i nett	X				X			X							X
T3	Utveksling av trusselbilde		X	X	X		X			X	X		X	X		
T4	Awareness - etterretning				X		X						X			
T5	Vedlikehold av reservestrøm							X								
T6	Risikovurderinger og tiltak – teknologiske/ organisatoriske endringer								X	X						
T7	Sikringstiltak mot logiske sårbarheter og skadevare	X	X	X	X				X	X	X		X	X		
T8	DNSSEC og BCP										X					
T9	Implementering av forordning (EU) 910/2014													X		
T10	Øke operativ krisehåndteringsevne	X	X	X		X	X	X	X		X	X		X	X	X
T11	Risikovurderinger og tiltak – avhengighet til underleverandører											X	X			X
T12	Videreutvikle regelverk – utkontraktering/ internasjonalisering											X	X			X

Tabell 5. Forslag til tiltak sammen med en angivelse av hvilke hendelser tiltakene har risikoreduserende effekt på.

Tiltak med brei risikoreduserande effekt

Utveksling av trusselbilete

- Informasjonsutveksling i Ekomsikkerheitsforum (sikkerheitsmyndigheitene, Nkom, tilbydarane)
- Informasjonsutveksling mellom NorCERT, NkomCSIRT og tilbydarane sine CERT/sikkerheitsmiljø

Sikringstiltak mot logiske sårbarheiter og skadevare

- Autorisasjon og logisk tilgangskontroll
- Logging og sporing

Auka operativ krisehandteringsevne

- Vidareutvikle den proaktiv beredskapen hos tilbydarane og myndigheitene
- Samhandlingsløysingar for krisehandtering
- Myndigheitsfinansiert beredskapsutstyr

Tiltak for å styrke tilbydarane sine eigne risikovurderingar

Planlagt arbeid i nett

- Dokumenterte prosessar for risikovurderingar før planlagt arbeid i nett
- Sette i verk tilpassa skadeførebyggande tiltak
- Kontroll, verifikasjon og beredskap

Teknologiske og organisatoriske endringar

- Identifisere *nye* sårbarheiter som vil følgje av endringane
- Sette i verk proaktive risikoreduserande tiltak (jf. krav i ekomregelverket)

Avhenge av underleverandørar

- Identifisere sårbarheiter knytt til avhenga til underleverandørar (leverandørar, entreprenørar,…)
- Sette i verk risikoreduserande tiltak; førebyggande tiltak og beredskapstiltak

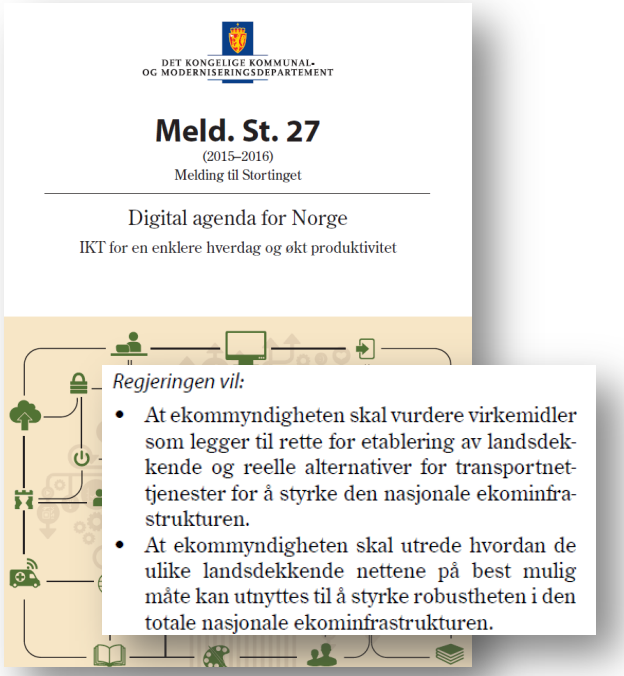
Tiltak retta mot den fysiske infrastrukturen

Halde fram arbeidet med bevisstgjering om etterretningstrusselen i organisasjonane

- Opne kjelder, publisering på nett, konferansar, sosiale medier,…
- Underleverandørar, konsulentar, etc.
- Informasjonssikkerheit/objektsikkerheit/ personellsikkerheit

Redundans i transport- og regionalnett

- Auka diversitet i transportnett (jf. også ekomplanen)
- Styrking av redundans i regionalnett, m.a. gjennom «Forsterket ekom»-programmet.



Takk for merksemda